DARKNETS, CYBERCRIME & THE ONION ROUTER:

ANONYMITY & SECURITY IN CYBERSPACE

by

Richard B. Yetter

A Capstone Project Submitted to the Faculty of

Utica College

May 2015

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Cybersecurity

Abstract

Anonymizing Internet technologies present unique challenges to law enforcement and intelligence organizations. Tor is an anonymity technology that has received extensive media coverage after a virtual black market hidden by its network was seized by the FBI in 2013. Anonymizing technologies have legitimate purposes, and as states increasingly employ sophisticated Internet censorship and surveillance techniques, they are becoming increasingly relevant. This study examines the creation of the modern Internet, explores the drastic changes that have taken place, and takes an in-depth look at intended and unintended uses of anonymizing technologies.

Keywords: Cybersecurity, Tor, cyberspace, cyber warfare, hacking, defense, attribution, darknet, espionage, security, privacy, encryption, free speech, cybersecurity, Professor Albert Orbinati.

Acknowledgements

For the past two and a half years I have been balancing my life between spending time with my beautiful wife Kate, the demands associated with this cybersecurity program at Utica College, and my commitment to the United States Air Force. Thank you to my wife for your patience and support, to Chad Miller for the effort you put in as a second reader, to the faculty at Utica College for your mentorship, and to the men and women I work with everyday who supported my goal to complete this program.

Table of Contents

STATEMENT OF THE PROBLEM

Introduction

Authoritarian states are not alone in their efforts to implement Internet controls. Over the past decade, a global trend has emerged where nations brazenly attempted to exert influence and control over cyberspace. Physical internet infrastructure has been centralized and consolidated, and the result is a system of choke points where network traffic is subject to exploitation and filtering (Roberts & Palfrey, 2010). Citing terrorism, cybercrime, or the threat of large-scale cyberattacks, nations' law enforcement and intelligence organizations have justified the implementation of sophisticated surveillance technologies that can target specific individuals or identify online behavior (Deibert & Rohozinski, 2010). In response, an online movement that resists Internet controls and surveillance has emerged, and this community has developed circumvention technologies that enable users to bypass state-sanctioned Internet controls.

One such circumvention technology is The Onion Router (Tor). Tor works by cocooning network traffic inside layers of encryption and then weaving the data through a maze of constantly shifting virtual tunnels (Crenshaw, 2011; Greenwald, Ball, & Schneier, 2013). Tor provides privacy by anonymizing a user's identity, and its advocates state that Tor is a force for good that can help protect journalists, promote free speech, enable access to censored content, and prevent intrusion into private communications (Lawrence, 2014; The Tor Project, n.d.). Tor's proven ability to defeat state-sanctioned Internet controls received coverage in the media, and this publicity attracted the attention of undesired audiences.

Cybercriminals have taken to using anonymizing technologies – including Tor – to evade traditional law enforcement surveillance techniques (Ablon, Libicki & Golay, 2014). Tor has been used to by cybercriminals to setup anonymous virtual black markets, conceal

communications, and obscure the connection between compromised machines and remotely controlled malware (McKim, 2012; Grossman, 2013; Lozhkin, 2014). Tor's critics have accused the network of being riddled with criminal activity, and some have called for it to be dismantled and shutdown entirely.

Justification of the Problem

Anonymity technologies inhibit attribution, and without attribution, there is no fear of consequence or possibility for deterrence (Lewis, 2010). In the context of cybercrime, anonymity technology prevents law enforcement from associating individuals with criminal behavior, and it enables cybercriminal enterprise to operate in the open without the fear of apprehension or prosecution (EC3, 2014; UNODC, 2014; EUROPOL, 2014). However, anonymity by itself is not inherently criminal in nature, and anonymity technologies have legitimate functions.

From the perspective of a person living in a repressive totalitarian society, a technology like Tor might be the only their means of communication with the outside world; and conversely, the only source of information about activities taking place behind closed borders (McKim, 2012). Dismantling anonymity technologies like Tor would further isolate already disenfranchised populations, and it would enhance a totalitarian state's ability to mold public perception through propaganda and misinformation (Lawrence, 2014; Deibert, 2012).

Nations are increasingly attempting to control cyberspace, and privacy technologies like Tor play a critical role in keeping the Internet open and global. However, anonymity technologies should not become the catalyst for an upsurge in organized criminal activity. It is therefore essential that law enforcement and intelligence organizations develop strategies to counter cybercriminals that make use of anonymizing technologies like Tor.

Gaps in Research

Very little is known about Tor's user base. Tor is a privacy and anonymity tool, and by design, it protects the identities of its users – even from the project's operators. Tor's website lists potential legitimate target audiences, but it does not identify known users (The Tor Project, n.d.). More information on Tor's users could help substantiate or refute allegations that the network is primarily used for criminal purposes.

Aside from the OpenNet Initiative and Citizen Lab information, there is insufficient publically available reporting on specific instances and details of Internet censorship. Internet controls are often talked about in broad terms versus naming specific manufactures, countries, installed systems, and specific surveillance or censorship techniques. This reporting would be useful in justifying the need for circumvention technologies such as Tor.

With regard to the virtual black markets that are operating on Tor, there is a lack of quantifiable data measuring the amount of money being generated and the volume of goods and services being traded (UNODC, 2014; EC3, 2014; EUROPOL, 2014). Dollar estimates of virtual black market cybercrime vary substantially, and experts cite this variance as an indication that the pervasiveness of cybercrime as a whole is not fully understood by law enforcement and regulatory organizations (Deibert, 2013; UNODC, 2014). If data existed on the revenue being generated by Tor virtual black markets, researchers would be able to assess the threat in terms of what the income could fund or sponsor.

Few reports on Tor cybercrime take into consideration other anonymizing technologies employed by cybercriminals. If Tor were to cease operations today, cybercriminals currently have at their disposal a variety of other anonymization tools; however, information about these alternatives is often absent from reporting on Tor cybercrime (Ablon, Libicki & Golay, 2014;

Lawrence, 2014). Research comparing Tor to alternative anonymity technologies would provide a more comprehensive understanding of the challenges faced by law enforcement, and it would be useful in developing new strategies that specifically target cybercrime on Tor.

Defining the Audience

Over the past half-century, the user base, physical structure, and ways in which people interact with the Internet have radically shifted. Critical interdependencies between the physical and cyber domains have developed, and these relationships will continue to intertwine and evolve in the years to come (Deibert & Rohozinski, 2010). For these reasons, individuals working with intelligence agencies, defense-related cyber units, and law enforcement organizations can benefit from this examination of anonymizing technologies, the emergent situations that necessitated Tor's creation, and the consequences of online anonymity.

The purpose of this study was to examine the evolution of Tor in order to develop counter cybercrime strategies that take into consideration the online freedoms anonymity technologies provide. This study attempted to answer the following questions: How does the Tor anonymizing network enable criminal activities? Does the Tor network represent a threat to U.S. national security? Is it possible for law enforcement and intelligence organizations to identify and apprehend individuals hiding their identities utilizing Tor? Should access to anonymizing technologies, like Tor, be regulated; restricting access to particular groups or individuals?

The Evolution of the Internet

In 1957 the Soviet Union launched the first manmade satellite, Sputnik, into orbit. This development shocked Americans who, for the first time, found themselves technologically outpaced by a rival nation. In response, U.S. President Dwight D. Eisenhower established the Advanced Research Projects Agency (ARPA) and charged the organization with regaining and

maintaining America's technological preeminence in the areas of space, missile defense, and nuclear-test detection (VanAtta, 2008).

One of ARPA's first efforts was the creation of an entirely new early-warning network that could monitor the air space for incoming threats (Waldrop, 2008). To accomplish this, developers collocated state-of-the-art computers at multiple radar and tracking sites, and they connected the machines through a redundant series of links that communicated across the existing telecommunications infrastructure. This first-ever real-time exchange of data between computers at multiple locations resulted in the desired comprehensive picture of the air space, and the technological innovations and developments that arose as a result of this endeavor set a precedent for the modern computer networks of the future.

By the 1980s, computers had evolved from simple real-time calculators to supercomputers capable of solving complex predictive models at a speed that was not humanly possible (Rogers, 1998). As a result, scientists working on advanced projects came to rely on supercomputing technology as an integral part of their research. At the time, many of the supercomputers were federally owned and operated by the United States Department of Energy (DOE), and only scientists working on defense related projects were allowed access to the systems and to the network that connected them – the Advanced Research Projects Agency Network (ARPANET). This arrangement led to advanced research being conducted by an elite few and excluded a majority of state universities and private research organizations.

In contrast to the American model of supercomputer access, Japanese universities routinely purchased supercomputers and made them available to their scientists. In 1981 the Japanese government announced their plan to launch a national program to develop an advanced form of artificial intelligence that would be made possible by domestically produced

supercomputers, and in 1983 several Japanese companies appeared to be in the verge of creating systems that would surpass the fastest machine of the time – the American-made CRAY 1 supercomputer. In response to these developments, the National Science Foundation (NSF), the U.S. Department of Defense (DOD), the National Aeronautical and Science Association (NASA), and the U.S. DOE produced a report that presented the situation as, "…a 'new Sputnik' that required immediate concerted action and succeeded in attracting the attention of Congress, which held two hearings on the matter in 1983…" (Rogers, 1998, p. 217). As a result of these Congressional hearings, federal funding was secured and a plan was developed by the National Science Foundation to create regional supercomputing centers connected by a wideband telecommunications network to be known as NSFNET.

Prior to the issue of supercomputing attracting the attention of Congress, the NSF had begun working a parallel effort to connect the Computer Science departments of non-ARPANET schools through another network known as the Computer Science Network (CSNET) (Rogers, 1998). One of key technologies utilized by CSNET and later adopted by NSFNET was the implementation of the DARPA developed TCP/IP protocol suite. These protocols worked by encapsulating large amounts of data into small packets of information that could be electronically routed to a destination Internet Protocol (IP) address, and unlike other protocols that existed at the time, TCP/IP also enabled multiple users to share a single communication line (Microsoft, 2003; Rogers, 1998). The proven success of TCP/IP within CSNET led to its implementation into NSFNET, and TCP/IP remains one of the core Internet technologies in use today (Rogers, 1998; Asadullah, Ahmed, Palet, Popoviciu & Savola, 2007).

From 1987 to 1995, the NSF worked to expand and upgrade the NSFNET National Backbone Service that interconnected the once disenfranchised universities and research

organizations (Harris, 1996; Frazer, 1996). The process involved a three-tiered approach that integrated campus and regional networks into a national network connected through a central backbone. In this configuration, the NSFNET maintained the backbone, and regional networks could plug-in as they were brought online (Frazer, 1996).

Over time, CSNET was essentially absorbed into NSFNET, and the success of the program led to consensus in Congress that the federally funded NSFNET should be transitioned to a commercially developed and maintained Internet (Frazer, 1996; Harris, 1996). The commercial model relied on private Internet Service Providers (ISPs) selling bandwidth to an information infrastructure where the components were owned and operated by telecommunication companies (Harris, 1996; Rogers, 1998).

In 1988 the NSF contracted with IBM, MCI, and Merit Inc. to manage the NSFNET backbone, and after the 1992 decision to transition the network to a commercial enterprise, these same companies (along with AT&T, Sprint, CISCO Systems, and Digital Equipment Corporation) became key players in the privatized network's development and operations (Rogers, 1998; Frazer, 1996). After nearly a decade of work, on May 8, 1995, the last of the regional networks were transitioned onto to the new network operated by American telecom companies, and the NSFNET backbone was officially decommissioned (Harris, 1996; Frazer, 1996). NSFNET's retirement represented the end of a federally funded network dedicated exclusively to scientific research communication and the beginning of a transition to a privatized, modern Internet.

The NSFNET represented a revolutionary new technology. When the project began in 1987, its goal was to connect regions of universities in America. By the time the project was completed, NSFNET had become the principle link between not only

American universities, but also between similar networks in 93 other countries (Frazer, 1996). The network's architecture and abundant bandwidth meant that at some point virtually all Internet communications traversed American infrastructure, and elements of this legacy configuration are still in place today (Frazer, 1996; Roberts & Palfrey, 2010). Just as the NSFNET backbone originally connected regions of America, the global Internet remains largely glued together through American infrastructure (Roberts & Palfrey, 2010).

In 1984, Tim Berners-Lee, a British scientist, started a fellowship at the European Organization for Nuclear Research (CERN) (Poole, 2005). To manage the massive amount of data that accompanies nuclear physics research, Berners-Lee created a system he referred to as a "…'memory substitute' to help him recall who worked where and on what project" (Poole, 2005, p. 12). In March of 1989, Berners-Lee submitted *Information Management: A Proposal* that "…discusses the problem of information access at CERN… introduces the idea of linked information systems, and compares them with less flexible ways of finding information" (Berners-Lee, 1989, para. 2).

At the time, CERN physicists routinely dealt with incompatibilities between computer systems that prevented them from electronically collaborating and sharing research (Berners-Lee, 1989). Additionally, because of the lack of a central repository, individual scientists had to download large personal libraries of material related to their work (Berners-Lee, 1989). Berners-Lee sought to resolve these issues by creating a "…global hypertext system as a way for physicists all over the world to collaborate and pool their information in one single information space" (Poole, 2005, p. 12).

In December of 1990, Berners-Lee authored the world's first hypertext markup language (HTML) documents, placed them on the world's first webserver at CERN, and by doing so, Berners-Lee created the world's first website (O'Luanaigh, 2012). The creation of the CERN website marked the beginning of a system that would evolve into today's sprawling World Wide Web (WWW) – or web for short. While working to organize information associated with nuclear physics research, Berners-Lee had inadvertently created a technology that would revolutionize the Internet make it more accessible to a global audience.

On April 30 1993, CERN declared the source code that powered the three components of WWW technology (e.g. the client, the basic server, and the library of common code) was now open source software and intellectual property that belonged to the public domain. At the time, the legality of free-to-use open source software was relatively unexplored, and the release of the WWW source code to the public marked the beginning of a movement to ensure that the software responsible for powering Internet enabled technologies remained in the public (Flückiger & Smith, n.d.). Additionally, this development meant that anyone in the world was now able to setup webservers, author HTML websites, and develop new applications for the technology without violating any sort of intellectual copyright.

Prior to Berners-Lee's creation of the WWW, in 1984 CERN made the then controversial decision to adopt the TCP/IP protocol in order to connect its facilities scattered across Europe (Flückiger, 2013). This decision led to CERN unintentionally positioning itself to be the equivalent of the NSFNET backbone for Europe, and it enabled the 1987 connection between the CERN and NSFNET networks (Sagel, 1995; Flückiger, 2013). Berners-Lee's creation of the WWW while employed by CERN coincided with the development of the international CERN

network, and through the CERN-NSFNET connection, the technology that powered the web spread throughout the world.

The NSFNET acceptable use policy implicitly forbade for-profit usage (Werbach, 1997). The only commercial organizations allowed on the network were companies that had a role in NSFNET's development. Because the primary users of NSFNET were academics and scientists who used the network to collaborate and share research, early content on the web was typically in the form of Berners-Lee's static, hyperlinked documents. However, the 1995 redefinition of the Internet as a commercial medium meant that the Internet was now open to everyone, not just scientists, and the content no longer constrained to technical data (Frazer, 1996).

After the privatization of the web in 1995, new users flooded onto the Internet though newly created ISPs – e.g. America Online, CompuServe, and Prodigy…etc. (Frazer, 1996; Vossen & Hagermann, 2007). In the years to come, the Internet's demographic would shift from an academic audience to a wide swath of the general public. These new users would drive the development and innovation of numerous new Internet technologies that would fundamentally alter the web's architecture and functionality. The early web made it possible for people to share digital media by embedding images, videos, and audio recordings into webpages, but it attracted a limited audience because it required users to have an understanding of the HTML programming language in order to publish content (Vossen & Hagermann, 2007).

In 1998 the World Wide Web Consortium (W3C) – an organization Berners-Lee established to standardize emerging web technologies – released RFC2318 that officially announced the acceptance cascading style sheets (CSS) (Lie, Boss & Lilley, 1998). CSS made it possible to separate the human information embedded in webpages from the machine code responsible for formatting and presentation (Vossen & Hagermann, 2007). With the advent of

CSS, webpages could be coded to act like shells for information, and users could manipulate or publish content through web-based interfaces without the need to directly edit HTML code. Users with little technical knowledge could now easily manipulate web content.

Publisher Tim O'Reilly popularized the term Web 2.0 that describes the shift from static HTML documents to interactive websites that function like applications (O'Reilly, 2005). By 2004, server-side scripting languages, CSS, and databases were being used to dynamically create webpages in real time. Web 2.0 technologies made the creation of advanced ecommerce websites like Amazon and eBay possible, and they were instrumental to the development of social media services including Twitter, Facebook, Blogger, and YouTube. The Internet of 2015 was largely made possible by advancements that took place because of Web 2.0 technologies and the success and popularity of social media services.

The blogosphere is the term that refers to the portion of cyberspace where individuals share their ideas, opinions, and experiences and interact with other people through social media services (Deibert, Palfrey, Rohozinski, & Zittrain, 2012). The blogosphere is what made it possible for anyone with an Internet connection to publish online content and communicate with a global audience. This capability has proven to be a force for democratization by enabling individuals to organize into groups moving toward collective action, and these Internet-enabled collectives have influenced political processes in ways that were not previously possible. For example, during the Arab Spring uprisings from 2010 to 2012: "The government tried to ban Facebook, Twitter and video sites such as DailyMotion and YouTube. But within a few days, social media networks were the organizing tool of choice" (Howard, Duffy, Freelon, Hussain, Mari, & Mazaid, 2011, p. 8).

Repressive states have historically relied on state-controlled media outlets to shape their citizens' perception of the world, and they have responded harshly and violently to mass gatherings and protests (Economist Intelligence Unit, 2008). The modern Internet has provided a potential means to bypass these control mechanisms, and for this reason, many authoritarian regimes regard Internet as a threat to their stability (Faris & Villeneuve, 2008; Deibert & Rohozinski, 2012). In a move of self-preservation, many totalitarian states have opted to limit access to the Internet, censored online content deemed politically or socially detrimental, and sought-out and punished individuals who attempted to access or distribute forbidden digital materials. In the context of authoritarian Internet controls, circumvention technologies like Tor became powerful tools that had the ability to enable the types of collective action that could drive democratic change.

LITERATURE REVIEW

The development of the web and the successful commercialization of the Internet infrastructure significantly expanded the Internet's audience and reshaped its content. What was once an elite computer network for scientists has transformed into the domain of cyberspace that connects billions of users around the world in ways the Internet's creators never imagined (Lewis, 2010; Deibert, 2013). As a growing number of objects from our physical world are mirrored or replaced by their digital equivalents in cyberspace, the issue of securing these important virtual items has become increasingly important.

Tor provides security through anonymity and encryption. It is resistant to exploitable weaknesses associated with standard Internet protocols, prevents eavesdropping, and can bypass state-sanctioned Internet controls (The Tor Project, n.d). While legitimate users have relied on Tor for access and anonymity, criminal organizations have also taken advantage of Tor's capabilities. Cybercriminals have used Tor to hide their illicit dealings from law enforcement organizations, and they have gone so far as to setup publically accessible anonymous virtual black markets with the intent of trading illegal goods and criminal services. This study examined the ways in which Tor has been exploited by cybercriminals, the challenges anonymizing technologies like Tor pose to U.S. law enforcement and intelligence organizations, and the difficulty associate with balancing security and anonymity.

Criminal Activity on Tor

When standard communications traverse the Internet, they do so in form of TCP/IP packets. These packets are like envelopes that are stamped with the address of the intended recipient and the return address of the original sender (Microsoft, 2003). If a third party wanted to know the contents of a postal letter, they could intercept the envelope while it was in route,

open it, and read the message inside. The same is true for unencrypted TCP/IP packets. A third party can collect packets as they traverse the Internet, reassemble them, and reveal a message's contents. And, just as in the example with the letter, a third party would also be able to see who is communicating with whom and record information on the nature of their communications such as how often they communicated, when they communicated, and the length of the communications (Ablon & Libicki, 2014).

Tor prevents electronic eavesdropping by encrypting the contents of packet data, and it attempts to resist traffic analysis by routing the data through its constantly shifting network of dedicated relays (The Tor Project, n.d; Lawrence, 2014). Tor seals the packet's ultimate destination inside three layers of encryption that are peeled away one at a time as a message traverses the Tor network. At each relay, a layer of the encryption is removed, and the next relay identified. In this arrangement no single system ever knows the entire path from start to finish.

To further obfuscate who is communicating with whom, the sender and receiver's IP addresses are effectively removed from the TCP/IP packet and replaced with a cryptographic hash that acts as an alternative routing mechanism (The Tor Project, n.d.). In the letter metaphor, the message would be written in a secret code, the envelope would take a constantly changing route as it moved through the postal system, and the sender's and receiver's addresses would be unintelligible to anyone but the mailman.

The Tor architecture was initially developed to provide secure communications and anonymity for people; however, in 2003, Tor released the Hidden Services protocol that extended similar protections to machines (Dingledine, Mathewson & Syverson, 2004). The Hidden Services protocol relies on rendezvous points inside the Tor network to anonymize the circuit between the client and the server. These rendezvous points act as trusted intermediaries

between a hidden service server and a requesting user, and they prevent both the client and the host from seeing the complete path from start to finish. Ultimately, the Hidden Services protocol anonymizes users and conceals the location of servers.

In order to access Tor hidden services, specialized software or a highly customized network configuration is required. By definition, this attribute is what constitutes Tor as a darknet (Crenshaw, 2011; UNODC, 2014). A user who entered an .onion address into a standard version of Microsoft Internet Explorer (MSIE) will never reach a Tor darknet site; because, by default, MSIE is configured to route traffic through the traditional Internet using standard protocols – not through the Tor network using the Hidden Services protocol.

Tor was originally developed by the Naval Research Laboratory to protect military communications; however, as of 2015, it was a publically available resource vehemently supported by online privacy and anti-censorship activists including the Electronic Frontiers Foundation. Tor is managed by the non-profit organization Tor Project Inc., and it receives a majority of funding from three federal agencies: the United States Department of State, the Broadcasting Board of Governors, and National Science Foundation (McKim, 2012; Lawrence, 2014). These organizations view Tor as significant and necessary because it "…provides potentially life-saving online security and privacy in places - such as Iran and Syria – where political dissidents are often dealt with harshly" (McKim, 2012, para. 12).

At the time of this study's writing, The Tor Project was actively developing and freely distributing multiple versions of the software needed to connect to the Tor network. The most popular was a browser bundle designed for everyday users that comes pre-configured, supports several platforms, and is easy to install. In addition to its browser bundle, the Tor Project has also released the standalone operating system Tails (The Amnesic Incognito Live System) that can be

configured to operate entirely from a bootable USB drive (Tails, 2015). Between uses, Tails resets to a default state eliminating any history and traces of activity, it leaves no evidence of usage on a host machine, and it securely routes all traffic through the Tor network. To a user in a contested Internet zone, Tails provides the perfect tool to access the Internet anonymously and destroy any record of doing so on a public or private system.

Current studies by Oxford Internet Institute indicate the Tor network has grown from its initial handful of proof-of-concept relays to over 5000 nodes, and that every day over 750,000 people use Tor (Oxford Internet Institute, 2014). Tor's growing popularity and ease of use have, however, attracted the attention of unintended audiences. Enterprising cybercriminals have used Tor to hide their identity while engaging in illegal online activity, and they have exploited Tor's Hidden Services protocol in order to setup virtual black markets that deal exclusively in illegal goods and services (EC3, 2014, EUROPOL, 2014; Grossman, 2014; Lawrence, 2014).

> Markets are good because they facilitate economic efficiency, but when that efficiency facilitates criminal activity, such "black markets" can be deemed harmful… As with most things, intent is what can make something criminal or legitimate, and there are cases where goods or services can be used for altruistic or malicious purposes... (Ablon, Libicki, Golay, 2014, p iii)

The Silk Road was the first hidden service ecommerce website that specialized entirely in illicit content. The Silk Road was a full-fledged, publically accessible, virtual black market complete with discussion forms, user reviews, and escrow services (McKim, 2012; Grossman, 2013; UNODC, 2014). Patrons could anonymously purchase illegal goods and services from anonymous vendors by conducting the transactions through digital cryptocurrencies, and illegal

merchandise was frequently shipped in disguised packaging through the postal system or commercial delivery companies (Ablon, L., & Libicki, M., 2014).

The Silk Road operated with impunity for two and a half years before the FBI was able to takedown the first inception of the site (Greenberg, 2014; UNODC, 2014). However, the lack of response by law enforcement – even after publicity in the media – helped generate a perception that cybercriminals could operate virtual black markets on Tor with impunity. As a result, many copycat sites emerged to include The Armory and Executive Outcomes that dealt in unregistered firearms, Evolution Marketplace and Dream Market that specialized in narcotics and stolen financial information, and The Hitman Network that offered contract killing as a service. The abundance of Tor darknet sites that catered to illegal goods and criminal services has rapidly expanded from 2010 to 2014, and "…(has) elicited so little prosecution from the world's law enforcement agencies it makes one wonder if a defacto decriminalization has occurred" (Deibert & Rohozinski, 2013, p. 29).

Anonymous virtual black markets are one way Tor's capabilities have been exploited, but innovative cybercriminals have found other ways as well. A study released on March 7, 2014 by the network security firm Kaspersky Labs found that cybercriminals were, "…actively using Tor to host malicious infrastructure…" to command-and-control botnet networks and communicate with remote malware (Lozhkin, 2014, para. 2). Tor has the ability to anonymize servers and conceal two-way communications – including automated machine-to-machine transmissions. This makes Tor an ideal platform for malware that requires two-way communication between a remote operator and a compromised system.

Cryptowall 2.0 ransomware is one form of malware that relies on hidden two-way communication. It is designed to encrypt a user's data and hold it hostage until a payment is

made to the malware's operator (CISCO, 2015). It is typically spread through infected email attachments or misleading Internet ads that trick users into downloading infected executable files. After embedding itself into the Microsoft Windows operating system, Cryptowall 2.0 is programmed to download the client version of Tor from a list of several predesigned sites and install it without detection. Once the Tor client is successfully installed on the compromised system, the malware uses Tor to connect to its command-and-control .onion server and communicate with the ransomware's anonymous operator.

Critics of Tor claim that while the network was designed with legitimate purposes in mind, it is now the preferred network of criminals, terrorists, or both. The Tor Project organization cannot refute these allegations because Tor's design prevents even its creators from knowing the identities of its users or qualifying the content on Hidden Services servers. However, in 2013 scientists Biryukov, Pustogarov, and Weinmann discovered a vulnerability in the Tor protocol that allowed them to analyze the number of Hidden Services websites and categorize their content based on metadata. Their conclusion was that the amount of sites dedicated to illegal activity was roughly equal to the number of legitimate sites associated with human rights, freedom of speech, and privacy. After performing their content analysis, they disclosed their discovery to the Tor's operators who subsequently patched the weakness – meaning that once again, no one is technically capable of categorizing the Tor darknet's content or user base (Biryukov, Pustogarov & Weinmann, 2013).

Anonymizing Technologies & National Security

In June 2013, the Guardian newspaper published the first of several stories about alleged mass surveillance programs being conducted by the American National Security Agency (NSA) and British Government Communication Headquarters (GCHQ) intelligence organizations. The

information featured in the Guardian series was derived from classified material illegally disclosed by the former NSA contractor Edward Snowden (Young, 2014).

In the story *NSA and GCHQ target Tor network that protects anonymity of web users,* author Glen Greenwald asserts the NSA and GCHQ were actively involved in an effort to identify and exploit Tor vulnerabilities (Greenwald, 2013). The article focuses on the different techniques the NSA attempted to apply to this effort, and it evaluates their level of success. One of Tor's creators, Roger Dingledine, was interviewed and quoted in the story as saying, "'The good news is that they went for a browser exploit, meaning there's no indication they can break the Tor protocol or do traffic analysis on the Tor network'"(Greenwald, 201, para. 33). Revelations from the series prompted a political debate in the U.S. and Europe on the lawful extent of government surveillance and Internet privacy, and the stories purportedly affected how U.S. adversaries worldwide conducted their operations (Young, 2014). For example, according to a New York Post staff report:

> 'After the leak, jihadists posted Arabic news articles about it … and recommended fellow jihadists to be very cautious, not to give their real phone number and other such information when registering for a website,' said Adam Raisman of the SITE Intelligence Group, a private analysis firm. 'They also gave out specific advice, recommending jihadists use privacy-protecting email systems like TOR, also called The Onion Router, to hide their computer's IP address, and to use encrypted links to access jihadi forums', Raisman said. While TOR originally was designed to help dissidents communicate in countries where the Internet is censored, it is facing legal difficulties because criminals allegedly have used it as well (Staff Report, 2013, para. 16).

Because of Tor's design, there is no definitive data on how many (if any) jihadists are using Tor to communicate and radicalize new recruits; however, if the information from the Greenwald series is correct, extremist groups could use Tor to communicate through an encrypted means that even the NSA and GCHQ struggle to decipher (Greenwald, 2013).

In the 2013, COMPUTERWORLD magazine article *British man charged with hacking NASA and US military computers,* author Jeremy Kirk reported on the 28 year-old man Lauri Love who was arrested for participating in a hacker organization that illegally accessed systems belonging to NASA, the U.S. Army, the Missile Defense Agency, and the Environmental Protection Agency (EPA) (Kirk, 2013). In order to avoid detection and identification, "…the group allegedly channeled its attacks through proxy servers and used TOR, a network that provides greater privacy by routing encrypted Web traffic through servers around the world" (Kirk, 2013, para. 7).

In the 2009 report *Cyberwarfare and Its Impact on International* Security, author James Lewis from the Center for Strategic and International Studies (CSIS) addresses the threats that exist due to the interdependencies between the physical and cyber domains. Lewis focuses on the idea that weak attribution results in a poor legal grounds for retaliation, and he examines the Internet's historic evolution as it relates to its intended function and design. In reference to the debate of online privacy in the form of anonymity, Lewis writes:

> Anonymity protects privacy and, to some extent, political speech. So there is a value to anonymity, but it also creates immense risks. On the Internet we are currently tilted so far in favour of anonymity that it is going to be very difficult to secure. One of the lines that we had in our (initial) report was that an anonymous Internet can never be secure (Lewis, 2010, p. 9).

Law Enforcement & Intelligence Agencies Attempts to Counter Cybercrime on Tor

According to a 2014 United Nations report, the Silk Road took in approximately $1.2 billion dollars in sales in the two-and-a-half years it was online before it was taken down by the FBI on October 1, 2013 (UNODC, 2014). The details about how the location of the server and the identity of its owner were discovered remain controversial, but the accounts are that the FBI was able to locate the .onion site because of a misconfiguration with the site's CAPTCHA – a security mechanism that requires users to spell out letters generated at random and delivered as an image – that was required in order for visitors to enter the site. Despite the FBI's achievement, a Silk Road 2.0 came online only two weeks after the first iteration had been seized and remained online for over a year until it was taken down during a joint EUROPOL and FBI sting operation in November of 2014 (Greenberg, 2014; Cook, 2014).

The FBI achieved its second success in countering a cybercriminal .onion server in July 2013 when they seized the Freedom Hosting servers in France that had been associated with a known child pornography distribution ring; however, the techniques used by the FBI in the Freedom Hosting case differed significantly from the tactics used in conjunction with the Silk Road takedown (Poulsen, 2013; Poulsen, 2014). The FBI later admitted to seizing the Freedom Hosting servers through international cooperation and reconfiguring them to exploit a zero day weakness in certain versions of the Tor browser. This vulnerability enabled the FBI to clandestinely install a program onto remote machines that communicated the IP address of flagged systems back to a datacenter in the Washington DC area (Greenberg, 2014; Poulsen 2013; Poulsen, 2014). This technique represents the most intrusive of active client-level surveillance measures and the most sophisticated, most aggressive means of defeating circumvention technologies used by the FBI to date.

A 2014 RAND Corporation study entitled *Markets for Cybercrime Tools and Stolen Data Hackers' Bazaar* stated that while law enforcement organizations have struggled to keep pace with cybercrime, law enforcement has increased its number of prosecutions and improved its methods for tracking down culprits (Ablon, Libicki & Golay, 2014). As the principle catalysts for change, the report cites a younger generation that are more comfortable with technology entering the force and an increase in international partnerships that eases extradition proceedings and the prosecution of cybercriminals. The report's prediction was that with the new focus on cybercrime by governments around the world, there would be substantial improvements when it came to fighting cybercrime in the near to immediate future – to include cybercrime on Tor.

On November 7, 2014, predictions in the RAND corporation report seemed to come to fruition when 16 European countries and the United States coordinated an extensive sting operation that took down 414 illicit Tor darknet domains (EUROPOL, 2014; EC3, 2014; Greenberg, 2104). Both FBI and EUROPOL spokespeople remained standoffish when it came to explaining how they managed to locate the servers stating they hoped to repeat their success and could not reveal their methods; however, one of Tor's creators, Andrew Lewman, later announced that law enforcement had simply followed a Bitcoin money trail and that they had come nowhere near cracking Tor's encryption or architecture. Lewman added that while 414 domains may have been removed, this represented less than 27 individual websites, and this much smaller number explained why the removal of 414 domains resulted in a mere 17 arrests by authorities (Lee, 2014).

Assessing the Availability of Anonimizing Technologies

In the 2008 book entitled *Access Denied: The Practice and Policy of Global Internet Filtering*, author and political science professor Robert Deibert examined worldwide patterns of

Internet censorship and surveillance. Deibert's findings drew extensively from data recorded during a four-year investigation conducted by the anti-Internet-censorship organization the OpenNet Initiative (ONI). From 2003 to 2006 the ONI team systematically assessed Internet accessibility from within 41 counties and concluded there was empirical "…evidence of technical filtering in twenty six (countries)" (Deibert, 2008, p. 5). Based on this information, Deibert concluded the Internet's architecture was fundamentally shifting toward a closed information environment subject to exploitation and manipulation by nation-state actors.

While the Internet had its roots in a single open global network meant to facilitate the sharing of ideas and research, a trend had emerged where access to the Internet was being denied along geographic lines in order to protect political interests. Deibert faulted authoritarian states that sought to control the public's perception of social and political issues as the primary perpetrators of Internet censorship, and he made the prediction that additional nations would justify implementing some kind of Internet filtering as a defensive measure in the years to come (Deibert, 2008).

In his 2010 follow-up *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace,* Deibert describes the rapidly changing landscape of the Internet:

> Since our research for 'Access Denied' was conducted, a sea change has occurred in the policies and practices of Internet controls. States no longer fear pariah status by openly declaring their intent to regulate and control cyberspace. The convenient rubric of terrorism, child pornography, and cyber security has contributed to a growing expectation that states should enforce order in cyberspace, including policing unwanted content… No longer is consideration of state-sanctioned Internet censorship confined to authoritarian regimes or hidden

from public view. Internet censorship is becoming a global norm (Deibert, 2010, p. 4)

Since Deibert's publication of *Access Denied: The Practice and Policy of Global Internet Filtering* in 2008 and *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* in *2010*, many of his predictions have come to fruition. Nations have realigned critical Internet infrastructure, installed defensive checkpoints that can monitor and control the information as it passes through them, and become increasingly aggressive in the ways they exert control over cyberspace (Deibert, 2010; Gallagher, 2012).

Numerous unprecedented instances of nations attempting to control access to the Internet have made headlines over the past four years. During the Arab Spring uprisings from 2010 to 2012, the governments of Egypt, Syria, Tunisia, Saudi Arabia, Bahrain, and Libya attempted to restrict Internet access in an effort to disrupt communication and quell protests (Soengas, 2013). In August of 2012 and in the wake of a cyberattack that crippled the Iranian nuclear program, Iran announced plans to replace the "…global Internet with a domestic intranet system" (Tait, 2012, para. 4). The Chinese government has expressed pride in their ability to restrict access to content deemed unsavory through their Great Firewall that currently "…blocks more than 18,000 websites operated across the planet, and is patrolled by tens of thousands of cyber-sentries" (Holden, 2014, para. 2). Most recently, Russia announced legislation reminiscent of the German War Powers Act that enables government cyber organizations to seize control of RUNET domains in the event of an Internet emergency such as a large-scale cyberattack (BBC, 2014). In 2003 the reality and pervasiveness of Internet filtering was unknown. As of 2014, it has been firmly established that "Internet censorship and surveillance are growing global phenomena" (ONI, 2014, para. 1).

ONI classifies Internet control mechanisms into three generational categories that represent the level of sophistication being employed with the first generation being the least technically sophisticated.

> In Chinese-style (first generation) filtering, lists of Internet Protocol (IP) addresses, keywords, and/or domains are programmed into routers or software packages that are situated at key Internet choke points, typically at international gateways or among major Internet service providers (Deibert, 2010, p 4)

This approach blocks specific traffic and is simple and effective, but it can quickly be bypassed by using virtual private networking (VPN) connections or proxy servers. With these systems a user connects to a machine outside the filtered network and creates a secured, dedicated, and encrypted connection back to the original machine. Once the connection is established, the system inside the filtered network uses the machine outside the filtered network to relay requests on its behalf. The filtered network's gateway cannot read the information because it is encrypted, and therefore, the traffic is allowed to pass. State-sanctioned countermeasures employed to prevent this from happening add the IP address of known VPN and proxy relays to the list of blocked addresses, or they simply do not allow any encrypted traffic through international gateways (Ablon & Libicki, 2014).

> Second-generation controls create a legal and normative environment and technical capabilities that enable actors to deny access to information resources as and when needed, while reducing the possibility of blowback or discovery. These controls have an overt and covert track. The overt track aims to legalize content controls by specializing the conditions under which they can be denied… The covert track establishes the procedures and technical capabilities that allow

> content controls to be applied 'just in time'… (e.g. during elections or public demonstrations) (Deibert, 2010, p 10).

This type of Internet control was exercised in Syria in 2012. As rebel groups advanced on the capitol city of Damascus, the country's international Internet Exchange Points (IPXs) – gateway chokepoints that link ISPs on major Internet backbones – suddenly and inexpiably stopped communicating with the rest of the world (Howard, Duffy, Freelon, Hussain, Mari, & Marwa, 2011). For two days there was virtually no Internet traffic coming out of Syria. Once the rebel advance had been stalled, the IPXs reconnected and Internet access was restored. The rebels blamed the Assad regime and the regime insisted that rebel attacks were responsible for the Internet outage.

Although an examination on the website ArsTechnica reveals the Syrian national telecom company had been actively working for over a year to consolidate control of Internet communication infrastructure prior to the blackout, there is no definitive proof to date the Syrian government ordered the IPXs shutdown (Gallagher, 2012). Under the ONI construct, the regime might have ordered the Internet to be cutoff if they feared information leaving the country through the Internet was going to be used against them. Cutting the Internet had the potential to disrupt rebel communications, and it reduced the likelihood of politically unfavorable news such as successful rebel advancements, use of chemical weapons, or ethnic or tribal cleansing from making its way to the international community.

If a nation-state shuts down its international IPXs, the only way for traffic to pass in or out of a country is through a completely different path. Satellite communications (SATCOM) have the ability to provide this type of alternate route. However, to counter the threat of information leaking out through SATCOM links and as a testament to how seriously the regime

regards Internet controls, authoritarian states, including Syria, often times employ signals intelligence equipment that can detect and locate SATCOM systems.

> Third-generation controls take a highly sophisticated, multidimensional approach to enhancing state control over national cyberspace... the focus is less on denying access than on successfully competing with potential threats through effective counter-information campaigns that overwhelm, discredit, or demoralize opponents… (and) also focus on surveillance and data mining… (Deibert, 2012, p. 27)

Third generation control measures include state-sponsored information campaigns in cyberspace. In these operations, state-directed Internet operators are employed to ultimately "…render opaque the role of state actors" (Deibert, 2012, p. 28). Operators accomplish this goal through the strategically calculated "…posting of prepackaged propaganda… mass blogging and participation in Internet polls, harassment of individual users… (and) posting of personal information" (Deibert, 2012, p. 28). Real-time Internet surveillance techniques amplify the effectiveness of these kinds of operations because they allow the state-directed Internet operators to single out dissenting individuals and organizations and respond accordingly to centralized objectives (Deibert, 2012).

The Russian invasion of Georgia in 2008 serves as a prime example of a third generation information operations. One day prior to the Russian military invasion, a "…large number of Georgia's Internet servers were seized and placed under external control… Also, much of Georgia's (Internet) traffic and access was taken under unauthorized external control at the same time..." (Georgia Update, 2008, p. 3). In addition to the kinetic military operations, cyber forces executed a campaign that sought to remotely seize Georgian Internet infrastructure. One day

after the Russian incursion began, the StopGeorgia.ru website came online and served as virtual meeting place for cyber operators to coordinate their efforts. The site distributed hacking tools, contained lists of vulnerable targets, and pinpointed specific application vulnerabilities. The cumulative effect of the cyberattack was that it limited Georgia's communication with the rest of the world and slowed international response (Georgia Update, 2008; Carr, 2011).

Another third generation control measure has been the creation of national cyberzones "…which limit access only to resources found in the national Internet domain" (Deibert, 2012, p. 28). Inside cyberzones, webservers and content that physically resides outside the geographic boundaries of a nation are blocked. Cyberzones make it easier for states to exert control over Internet content, and they allow the domestic Internet to continue to function in the event that the government orders all international Internet traffic to be blocked.

> …with always-on portable devices that are fully connected to the Internet, and much of society's transactions mediated through information and communication technologies… cyberspace is not so much a distant realm as it is the very environment we inhabit (Deibert, 2008, p. 9)

In addition to limiting access to Internet content, nations are also employing sophisticated forms of Internet surveillance. In the book *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace,* contributing authors John Palfrey and Hal Roberts examine the methods that have been used to conduct Internet surveillance. They conclude that because of the Internet's topology, surveillance principally takes place at three distinct levels: the network, the server, and the client (Palfrey & Roberts, 2010).

The network category of Internet surveillance refers to the numerous tactics and techniques that can be employed to monitor traffic as it passes through the Internet. The goal of

network surveillance is to collect personal information or identify targeted individuals. In its broadest sense, network surveillance is similar to a wiretap in cyberspace. Someone other than the intended recipient of a communication – an email, instant message, video conference… etc. – intercepts the message as it passes through the network. Palfrey and Roberts identify three broad areas that are vulnerable to this kind of exploitation: "…routing information, the actual content of the stream, and contextual signatures" (Palfrey & Roberts, 2010, p. 38).

The routing of TCP/IP traffic is made possible by the header portion of Internet Protocol (IP) packets. The TCP/IP packet header contains the unencrypted unique IP address of a message's sender and receiver (Microsoft, 2003). By simply examining a single TCP/IP packet, an observer can deduce who was attempting to communicate with whom. Tor attempts to prevent this from happening by masking the sender and receiver information and encrypting the data inside the TCP/IP packet (Onion Routing, n.d.).

With regard to unencrypted Internet communications, intercepted TCP/IP packets can be reassembled revealing the exact contents of a message. Because Internet traffic flows through public and private networks where any node along a path has the potential to intercept packet data, encryption is oftentimes employed to enhance security and privacy. This may prevent an observer from identifying the exact contents of a message, but by comparing the metadata produced by the communication (e.g. the time of the communication, the duration, the amount of network traffic, the size of the data passed… etc.) to known traffic patterns, observers can deduce the type of communication taking place. This is because different online behaviors produce unique and distinguishable types of TCP/IP streams. For example, packet data from a streaming video will look much different than packet data associated with sending and receiving email – even if it is encrypted. Additionally, in the scenario involving an authoritarian regime

seeking to filter and monitor Internet traffic, the presence of encryption alone could be seen as an attempt to bypass network security measures and prompt further investigation (Luhn, 2014).

"The Internet consists of billions of links between clients, servers, and routers making comprehensive surveillance of the entire network very difficult" (Roberts & Palfrey, 2010, p. 39). However, facilities known as IPXs where major ISPs' networks overlap and machines known as autonomous systems (ASs) that control banks of critical routers make the task of monitoring these billions of links much less difficult. IPXs and ASs are centralized junctions that function as choke points and make it possible to perform traffic analysis or control Internet access on a nation-wide scale. Theoretically, a government could require its ASs and IPXs to monitor or record TCP/IP traffic as it passed through its networks, and because the Internet's architecture consists of a web-like mesh layout, the traffic passing through would likely contain both data from both national and international users. The implication is that any country that acts as an intermediary for international Internet traffic has the ability to monitor the data that traverses its networks (Roberts & Palfrey, 2010).

Servers present the second major category of Internet surveillance. "Google's collection of search terms, IP addresses, and cookies represents one of the largest and most intrusive single collections of personal data online or off-line" (Roberts & Palfrey, 2010, p. 42). Most browsers will, by default, provide a webserver with information about a user's operating system, version, language, time zone, IP address, screen size, fonts installed, browser type, version, and plugins installed (Eckersley, 2010). This information is used by servers to modify webpages sent to a user in real-time so that pages are compatible with the user's system; however, this same information can also be used to associate a particular user with a website – even if a user does not enter a character of information or click a link. For example, there would only be so many

users running Mac OSX 10.1.2.4, using Firefox 13.1, with 37 fonts, a screen resolution and depth of 2128x1330x24, with Java plugin 13.4.1.2 installed, and cookies enabled. Those identifiers create a browser footprint that can be correlated with TCP/IP data to clearly and unmistakably identify a person or system and reveal the content a user sought or viewed (Roberts & Palfrey, 2010; Eckersley, 2010).

When a person connects to a website, it records information about their interaction. Cookies provide a way for servers to chain a series of interactions together by placing a uniquely identifiable file on a user's system. Every time a user enters information or clicks a link, the server has the ability to record that action and associate it with a cookie and a system. This capability creates a mechanism where servers can collect a tremendous amount of information on visitors by simply recording their online behavior and associating it with a unique identifier (Roberts & Palfrey, 2010).

Currently, online advertisers are dissecting this vast amount of data collected by cookies and using server-side analysis to deliver targeted advertisements to individual website visitors in real-time. Roberts and Palfrey cite Google's online advertisement placement system AdWords as an especially good example of how fast and surgical this process has become.

> Google adjusts the placement of ads in real-time according to the current results of an ad auction; content providers watch the profitability of their content in real-time and make adjustments to attract more ad-clicking customers; advertisers adjust their bids and update their ads in real-time to attract more users (Roberts & Palfrey, 2010, p. 43)

The final and most invasive category of network surveillance occurs at the client level. Through this technique, an actor attempts to directly monitor a user by clandestinely installing hidden

software or hardware on the target machine. The installed software or hardware allows a secondary actor to perform a number of collection functions including capturing user names and passwords by recording key strokes, activating webcams or microphones, exfiltrating financial or intellectually copyrighted information, or turning the machine into a zombie controlled by a botnet operator (Roberts & Palfrey, 2010).

The 2009, Citizen Lab report *Tracking GhostNet: Investigating a Cyber Espionage Network* illustrated how intrusive client surveillance techniques can be employed to conduct state-sanctioned espionage. GhostNet – aka GhostRAT (Remote Access Terminal) – was widely believed to have been developed and deployed by the People's Republic of China (PRC). Initially GhostNet targeted computers in the Office of His Holiness the Dali Lama (OHHDL); however, by exploiting the legitimacy of infected machines, GhostNet was able to spread to systems that "…were identified as computers at foreign embassies, diplomatic missions, government ministries, or international organizations" (Citizen Lab, 2009, p. 14). GhostNet gave remote operators virtually complete control of infected systems, and it created a global network of strategically compromised machines. GhostNet was a proof-of-concept command-and-control (C2) model for mass-scale client surveillance. While it was widely suspected the purpose of GhostNet was to augment a larger international intelligence program, GhostNet's capabilities could easily be turned inward on an unsuspecting domestic population. Unrestricted access to webcams and microphones in homes and work centers across an entire country would give Orwellian-like surveillance capabilities to a totalitarian regime.

DISCUSSION OF THE FINDINGS

The Literature Review consisted of four areas of research emphasis: cybercrime on the Tor network, Tor and national security, law enforcement and intelligence organizations attempts to defeat Tor, and an assessment of the need for anonymizing technologies. In order to produce the most complete and unbiased study possible, the referenced material was assembled from a wide variety of sources including: mainstream media, technical journals, research data from the activist groups OpenNet initiative and Electronic Frontier Foundation, official U.S. government, European Police, and United Nations reporting, and numerous dissertations, theses, and academic publications pertaining to cybersecurity. In addition to the second hand reporting, the author of this study personally examined Tor darknet sites in order to confirm the existence of illicit activity and alleged content.

Major Findings

It is very difficult to compare and contrast the good Tor provides with the potential harm it creates. The ability to provide safe, unfiltered access to the Internet in countries like China, Russia, Iran, and Syria does not directly equate to the potential harm created by drugs or firearms coming from anonymous online black markets (McKim, 2012; Lawrence, 2014). Additionally, Tor is one of many anonymizing technologies, and should it cease to exist or be suspected of compromise, the criminal activity on Tor would likely shift to a newer and possibly more complex anonymous platform (Ablon, Libicki & Golay, 2014).

There are instances where authoritarian states have heavily filtered Internet content or oppressed free speech, and it was during these times that anonymity and unfiltered Internet access provided a positive force for change; however, anonymity by itself is not inherently a force for anything. Anonymity is a technological capability that can be used by anyone for any

purpose. If the risk anonymity poses today is so great that it represents a threat to national security and international stability, then it is possible that we have reached a point in time where there is a need to reassess our dependency on the world's information infrastructure and willingness to make cyberspace more transparent (Lewis, 2010).

Cybercrime and cyber warfare represent significant threats to U.S. national security (Lewis, 2010; DHS, 2010). In the 2012 OpenNet Initiative book on Internet controls and censorship, *Access Contested: Security, Identity, and Resistance in Asian Cyberspace information Revolution and Global Politics,* author Ronald Deibert wrote:

> The Internet's infrastructure, relatively trivial at one time, has now become a critical component of society, economics, and politics, and ranked as one of the top security priorities for governments of the world (Deibert, 2012, p. 12).

Most of the material that tied Tor to national security threats tended to focus on what could happen rather than list concrete examples of what has occurred. This is likely because of the tendency to broadly label anything associated with cybercrime and cyber warfare as a direct threat to national security rather than perform a more thorough assessment of the specific dangers posed by a given emerging technology (Deibert, 2013).

Anonymity and security are fundamentally paradoxical concepts (Lewis, 2010). In his 2010 intro to the United Nations report *Cyber Warfare and Impact on International Security*, Lewis wrote in no uncertain terms, "One of the lines that we had in our (draft) report was that an anonymous Internet can never be secure" (Lewis, 2010, p. 9). There is balancing act between online privacy and securing cyberspace. Tor provides near absolute anonymity, and it therefore denies the potential for absolute security.

Comparison of the Findings

The messages conveyed by different sources were diametrically opposed. At one end of the spectrum was the activist belief that online anonymity was a fundamental right and necessary to protect us from an Orwellian surveillance state. At the other end was the view that anonymity created significant security risks and posed threats to national security and global stability. Additionally, reporting in the mainstream media tended to focus on the sensational aspect of a crime-ridden hidden Internet called the darknet and ignored larger international implications associated with anonymity and circumvention technologies.

The foreword in the 2012 OpenNet Initiative book *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* captures the overall sentiment of open Internet advocates. Contributing author Miklos Haraszti wrote:

> Let us be clear. The benefits of the Internet far outweigh the dangers of misuse. In some countries, the Internet is the only source of pluralistic and independent information, even if Internet penetration may still be low. Let us make sure that this unique source of unguided information does not dry out (Haraszti, 2010, p. XVI)

Advocates for a free and uncensored Internet cite the Arab Spring movement as an example of the positive force for democratic change the Internet can provide, and they reference the attempts by authoritarian governments to block Internet access during this period as a justification for technologies that can bypass Internet controls (Soengas, 2013; Howard, Duffy, Freelon, Hussain, Mari, & Mazaid, 2011). Additionally, advocates of anonymity and unrestricted Internet access point out that countries like China, Russia, and Iran are essentially building their own domestic cyberzones that function like the Internet but that are heavily filtered and monitored; and they

express concern that an overzealous approach to cybersecurity could promote Internet isolation and result in decreased global connectivity (Dingledine, Mathewson, Syverson, 2004; Deibert, 2010).

Conversely, U.S. government and United Nations reports frequently stated online anonymity represented a significant threat (UNODC, 2014; EUROPOL, 2014; Lewis, 2010; DHS, 2010). The *EC3 2014 Internet Organized Crime Threat Assessment*, stated that "The use of anonymization tools is ubiquitous amongst the cyber underground…(and recommends) Law enforcement should build technical capabilities in order to support technical investigations into subjects using Darknets" (EC3, 2014, p. 53).

The United Nations *2014 World Drug Report* warns of the potential growth of online anonymous markets and their disruptive potential, and the 2010 U.S. Department of Homeland Security *Information Technology Sector-Specific Plan An Annex to the National Infrastructure Protection Plan 2010* recognizes that, "…(the) anonymity of actors makes identifying threats, assessing vulnerabilities, and estimating consequence at the national-level difficult…" but does not implicitly identify Tor or any other anonymizing technology (DHS, 2010, p. 17).

The issue of online anonymity is controversial and has supporters on either side of the security versus freedom debate. Government reports tend to favor a need for security perspective and view anonymity as a threat to stability. Alternatively, Internet freedom advocates tend to take the stance that excessive security poses a threat to free speech and enables surveillance on a level that violates individuals' right to a reasonable expectation of privacy.

The coverage of Tor in the mainstream media has typically been alarmist and sensational. Stories in magazines and newspapers tended to be superficial and focus on the virtual black markets made possible by the Tor Hidden Services protocol. The magazine Time printed the

story *The secret web: where drugs, porn and murder live online* that – while factually sound – sensationalized a hidden Internet where thriving anonymous marketplaces sold drugs, weapons, counterfeit goods, and contract murder; however, the article spent very little time on topic of the U.S. State Department's goal to promote uncensored Internet access to people living in oppressive states (Grossman & Netwon-Small, 2013).

The U.K. newspaper The Telegraph printed an article, *Click here for crime; Ten years ago, the US Navy invented an anonymous internet network. Today the 'dark web' is used to trade guns, drugs and child pornography. Why do they insist it's a force for good?* which also highlighted the virtual black markets, ransomware, and enciphered botnet communications Tor provided criminals (Simons, 2014). The Australian newspaper The Age's article *Bright ideas lurk in the internet's dark places* echoed the theme of a hidden Internet rife with narcotics and child pornography (Thompson, 2014).

Few stories in mainstream media took a more holistic approach to the subject. The Boston Globe's article *Privacy software, criminal use* was one of the rare pieces that focused more on the history of Tor than illegal virtual marketplaces. Author Jenifer McKim correctly identified the U.S. State Department as one of Tor's primary financers, and she presented their public statement for doing so. Additionally, she interviewed one of Tor's founders, Andrew Lewman, as well as the spokesperson for the National Science Foundation, Lisa-Joy Zgorski, in order to ascertain Tor's official intended uses (McKim, 2012).

Bloomberg's Business Week's author Dune Lawrence published one of the most comprehensive reports on Tor: *The Inside Story of Tor, the Best Internet Anonymity Tool the Government Ever Built* (Lawrence, 2014). The piece detailed the Tor Project from its inception to its current state, and like McKim, Lawrence interviewed Tor's developers and highlighted its

ability to protect legitimate users such as victims of domestic abuse, political dissidents, and journalists. Lawrence also presented a level of technical explanation that was rarely found in mainstream media coverage, and he connected the controversies surrounding NSA and GCHQ surveillance programs to Tor demonstrating the complexity of the online anonymity issue.

The technology magazine Wired provided the most accurate, detailed, and unbiased coverage of Tor cybercrime issues. Wired's articles tended to dissect very specific, significant developments, and they examined events from a technical, legal, and social perspectives. For example, their coverage of the recent FBI takedown of several darknet servers in *FBI's Story of Finding Silk Road's Server Sounds a Lot Like Hacking*, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, and *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack* correctly questioned the legality and legitimacy of the intrusive methods employed by the FBI during this operation (Greenberg 2014; Poulsen, 2014; Poulsen, 2013).

Limitations of the Study

The nature of the Tor network makes it very difficult to study. A majority of the research done on Tor is performed by scientists or other researchers who are directly involved with the project or similar technologies. In *Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries The study Content and popularity analysis of Tor hidden services*, five research scientists – including one of Tor's founders, Paul Syverson – from the U.S. Naval Research Laboratory claim to have found a way to identify Tor users through traffic pattern analysis, but this report also represents the closest anyone has come in recent years to identifying Tor users (Johnson, Wacek, Jansen, Shen, Syverson, 2013). In *Content and popularity analysis of Tor hidden services* three University of Luxembourg researchers identified a technical weakness that allowed them to view metadata related to Hidden Services servers that suggested their content,

but it did not identify the Tor users, the locations of Hidden Services servers, or the actual encrypted traffic (Biryukov, Pustogarov & Weinmann, 2013).

The takedown of the infamous Silk Road marketplace attracted people's attention because it presented the possibility – albeit potentially nothing more than that – of a vast hidden layer of the Internet where unscrupulous site operators were free to peddle unspeakable contraband (Ablon, Libicki & Golay, 2014). On the contrary, the research indicates that drugs are the primary goods being sold on darknet sites, and that other more serious contraband is emerging but not yet prevalent (UNODC, 2014). Regardless, unless the anonymizing capability of Tor is disabled, it is impossible for anyone to know to know the truth.

RECOMMENDATIONS

Many authors have cited the dangers associated with online anonymity (Lewis, 2010; Roberts, 2010; Deibert, Palfrey, Rohozinski, & Zittrain, 2012; McKim, 2012; Thompson, 2014; UNODC, 2014; EUROPOL, 2014). Governments and organizations acknowledge that anonymizing technologies like Tor are being used by cybercriminals; however, they lack critical information detailing the pervasiveness of darknet cybercrime and the impact it has on particular populations (UNODC, 2014; EUROPOL, 2014). Detailed research on the economics of darknet cybercrime should be accomplished in order to understand the scope and magnitude of the issue.

Future research should focus on the need for law enforcement organizations to develop comprehensive technical counter-anonymity cybercrime strategies (Ablon, Libicki & Golay, 2014; EUROPOL, 2014; EC3, 2014). In the 2014 joint EUROPOL and FBI Operation Onymous sting, the law enforcement organizations were able to takedown 27 Hidden Services websites associated with cybercrime (Lee, 2014; EUROPOL, 2014; UNODC, 2014). In response to the raid, one of Tor's original creators, Roger Dingledine, speculated that law enforcement had likely exploited misconfigured web servers, taken advantage of poor operational security, or leveraged some kind of Bitcoin deanonymization technique (Dingledine, 2014; Greenberg, 2014) [1]. These are examples of traditional law enforcement investigation techniques that were modified to work against cybercriminals, and additional research into further developing non-invasive counter-anonymity methods will certainly aid future counter-cybercrime efforts while providing minimum pushback with regard to the legality of such operations.

[1] Note: Dr. Dingledine also theorized law enforcement could have attacked or compromised a Tor relay, but that method of operation would constitute an aggressive, invasive client surveillance technique rather than passive observation that exploited poor operational security. Additionally, such an attack raises legal questions pertaining to search and seizure and the international authority of domestic law enforcement organizations in cyberspace.

Tor does not operate in the vacuum of cyberspace. There are human operators behind the anonymous black markets, and the contraband they solicit often times takes a physical form (McKim, 2012; Grossman, 2013). Narcotics, firearms, and forgeries, for example, require a logistics component in order to be transported and distributed. Law enforcement would benefit from research that examined the methods in which Tor black market operators are moving and distributing illegal goods (Ablon, Libicki & Golay, 2014).

In order to justify the need for anonymizing technologies like Tor, it is critical to understand the extent to which governments are implementing Internet controls (Talbot, 2009; McKim, 2012). Additional research should focus on state-sanctioned tactics and techniques governments have used to exert control over the physical components of cyberspace, and it should examine the specific means by which affected users are attempting to defeat the imposed Internet controls. The advocacy groups OpenNet Initiative and Electronic Frontier Foundation monitor Internet censorship and publish regular reports on their findings, but their work could be bolstered by additional research that clearly demonstrates how Tor and the Hidden Services protocol benefit people inside totalitarian states.

This study was limited by the fact that it was difficult to categorize the activity taking place on Tor or identify the user base because the network's primary function is privacy. Tor achieves privacy through system-wide anonymity; and therefore, no central authority exists that can answer questions nor refute accusations about its users. A majority of the media attention Tor has received has been sensationalized reporting focused on virtual black markets, and it has ignored Tor's potential legitimate uses. Media coverage typically did not address the social implications of nations increasingly employing sophisticated Internet surveillance and content filtering technologies or even acknowledge the emerging trend (Deibert, 2012; Dingledine, 2014;

The Tor Project, n.d). There is a need for balanced research that considers the legitimate functions of anonymity and examines the consequences anonymity being centrally controlled or entirely unavailable.

Additional research into cyber black market economics and logistics, state-sanctioned Internet controls, and counter-anonymity techniques will enable law enforcement and national security organizations to develop more effective and comprehensive counter-cybercrime strategies. By better defining, characterizing, and assessing cyber-threat vectors, researchers can begin to more accurately delineate between cybercrime as a whole, on Tor, and other darknets.

CONCLUSIONS

The issue of non-attribution has led to governments consistently being unable to clearly delineate between acts of cybercrime, espionage, and cyber warfare. This is because, depending on the actors involved, all anonymizing and circumvention technologies could be correctly categorized as cybercrime, espionage, or cyber warfare tools (Lewis, 2010; Deibert, 2013). A cyberattack against critical national infrastructure orchestrated by a teenager in California would be classified as a cybercrime whereas the same act committed by military cyber unit in another nation would constitute an act of war. Antiquated protocols developed to connect scientists 40 years ago were never designed to account for privacy or provide absolute attribution, and, with or without Tor, these outdated Internet protocols can be exploited in ways that make absolute identification virtually impossible (Citizen Lab, 2009; Lewis, 2010; Deibert, 2013).

Tor is no more a tool for cyber warfare or criminal enterprise than are encrypted email services, virtual private networks, and proxy servers. If Tor is to be labeled a criminal tool, then so too should any social media platform, Internet chat program, or Internet service associated with a cyber-incident. By extending this guilt by association mindset to the extreme, one could come to the absurd conclusion that the Internet itself is criminal in nature because it has enabled the phenomenon of cybercrime. Tor is a privacy service, and rather than condemning its capabilities, it would be more productive to answer the question: what is the correct balance of anonymity and security in cyberspace that our society is prepared to accept (Lewis, 2010, McKim, 2012; Deibert, Palfrey, Rohozinski, & Zittrain, 2012)?

When debating the legitimacy of Tor, it is important to remember that Internet censorship is a real and increasingly common global phenomenon (Deibert, Palfrey, Rohozinski, & Zittrain, 2012; Deibert, 2013). Although Tor has been exploited by cybercriminals and presents new

challenges to law enforcement, it remains a relevant and necessary technology that has the potential to open otherwise closed nations (Holden, 2013; Deibert, 2013). Law enforcement and intelligence organizations must develop comprehensive counter-anonymity cybercrime strategies that are effective without attacking the integrity of the underlying privacy system itself. If Tor can be exploited by domestic actors, then so too could it be compromised by security services in oppressive states and repurposed as a tool that enabled retaliation against users who would dare to attempt to bypass state-sanctioned Internet controls. Counter-anonymity cybercrime strategies should concentrate on financial system analysis – including cryptocurrencies such as Bitcoin, common failures in operational security practices, and exploitable misconfigurations that make it possible to passively observe criminal behavior.

The trend where states continue to consolidate Internet architecture within their borders and implement sophisticated Internet controls could lead to the end of the global Internet. As technology progresses and states tighten their grip on cyberspace, it remains to be seen what is in store for Tor's future. However, at the time this study was authored, Tor was still able to circumvent the Great Firewall of China, provide a level anonymity that frustrated U.S. and British national intelligence organizations, and act as a tool that had the power to reconnect isolated users with the rest of the world through the open, global Internet.

REFERENCES

Ablon, L., & Libicki, M. (2014). *Markets for cybercrime tools and stolen data: Hackers' bazaar*. Washington DC: RAND Corporation.

Asadullah, S., Ahmed, A., Palet, J., Popoviciu, C., & Savola, P. (2007, January) ISP IPv6 deployment scenarios in broadband access networks. Retrieved March 24, 2015, from http://tools.ietf.org/html/rfc4779.

Berners-Lee, T. (1989, March 1). Information management: A proposal. Retrieved November 2, 2014, from http://www.w3.org/History/1989/proposal.html

Biryukov, A., Pustogarov, I., Thil, F., & Weinmann, R. (2013). *Content and popularity analysis of Tor hidden services*. Cornell University.

Brenner, S. (2010). *Cybercrime: Criminal threats from cyberspace*. Santa Barbara, Calif.: Praeger.

Bergman, M.. (2013, March 12). Understanding the Deep Web in 10 minutes. Retrieved September 28, 2014, from http://www.Bergman.com/2013/03/whitepaper-understanding-the-deep-web-in-10-minutes/

CISCO. (2015, January 6). Ransomware on steroids: Cryptowall 2.0. Retrieved March 4, 2015, from http://blogs.cisco.com/security/talos/cryptowall-2

Citizen Lab. (2009). Tracking GhostNet: Investigating a cyber espionage network. Retrieved November 17, 2014, from https://citizenlab.org/publications/

Carr, J., & Shepherd, L. (2010). *Inside cyber warfare*. Sebastopol, Calif.: O'Reilly Media.

Chapman, C. (2009, November 15). The History of the Internet in a nutshell - Six revisions. Retrieved September 26, 2014, from http://sixrevisions.com/resources/the-history-of-the-internet-in-a-nutshell/

Cook, J. (2014, November 7). FBI arrests SpaceX employee, alleging he ran the 'Deep Web' drug marketplace Silk Road 2.0. Retrieved November 8, 2014, from http://www.businessinsider.com.au/fbi-silk-road-seized-arrests-2014-11/

Crenshaw, A. (2011, August 4). Cipherspaces/Darknets: An overview of attacks (Hacking illustrated series InfoSec tutorial videos). Retrieved October 26, 2014, from http://www.irongeek.com/i.php?page=videos/cipherspaces-darknets-an-overview-of-attack-strategies

DHS. (2010). *Information technology critical infrastructure and key resources sector-specific plan as input to the National Infrastructure Protection Plan.* Retrieved September 27, 2014, from http://www.dhs.gov/information-technology-sector.

DHS. (2013). *National Infrastructure Protection Plan: 2013.* Retrieved September 27, 2014, from http://www.dhs.gov/national-infrastructure-protection-plan.

Deibert, R., Faris, R., Murdoch, S., Palfrey, J., Rohozinski, R., & Zittrain, J. (2008). *Access denied the practice and policy of global Internet filtering*. Cambridge, MA.: MIT Press.

Deibert, R., Rohozinski, R., Robert, H., Palfrey, J., Villeneuve, N., Zuckerman, E., Zittrain, J. (2010). *Access Controlled The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA.: MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2012). *Access Contested Security, Identity, and Resistance in Asian Cyberspace information Revolution and Global Politics*. Cambridge, MA: MIT Press.

Deibert, R. (2013). *Black code: Surveillance, Privacy, and the Dark Side of the Internet.* Toronto, Ontario: McClelland & Stewart.

Deitz, B. (2008, August 13). Olympics: Jing Jing, Cha Cha, and other online cops. Retrieved

September 27, 2014, from https://www.cpj.org/blog/2008/08/olympics-jing-jing-cha-cha-and-other-online-cops.php

Dingledine, R., Mathewson & Syverson, P. (2004). Tor: The second generation onion router. Retrieved March 27, 2015, from http://dl.acm.org/citation.cfm?id=1251396

Dingledine, R. (2013, October 3). Tor and the Silk Road takedown. Retrieved October 28, 2014, from https://blog.torproject.org/blog/tor-and-silk-road-takedown

Dingledine, R. (2014, November 9). Thoughts and concerns about Operation Onymous. Retrieved December 10, 2014, from https://blog.torproject.org/blog/thoughts-and-concerns-about-operation-onymous

EC3 (2014, February 9). European Cybercrime Center (EC3) - First year report. Retrieved March 3, 2015, from https://www.europol.europa.eu/content/european-cybercrime-center-ec3-first-year-report

Eckersley, P. (2010, January 26). A primer on information theory and privacy. Retrieved March 26, 2015, from https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy

EUROPOL (2014 September 29). *2014 Internet Organised Crime Threat Assessment (iOCTA)*. Hague, Netherlands: EUROPOL.

Flückiger, F., & Smith, T. (n.d.). CERN accelerating science. Retrieved November 2, 2014, from http://home.web.cern.ch/topics/birth-web/licensing-web

Flückiger, F. (n.d.). CERN accelerating science. Retrieved October 2, 2014, from http://home.web.cern.ch/cern-people/opinion/2013/06/how-internet-came-cern

Frazer, K. (n.d.). Merit's history. Retrieved October 2, 2014, from http://www.livinginternet.com/doc/merit.edu/transition.html

Frazer, K. (1996). *NSFNET: A partnership for high-speed networking : Final report, 1987-1995*. Ann Arbor, MI: Merit Network.

Gallagher, S. (2012, December 1). Updated: Paint it black - How Syria methodically erased itself from the 'Net. Retrieved September 27, 2014, from http://arstechnica.com/information-technology/2012/12/paint-it-black-how-syria-methodically-erased-itself-from-the-net/

Greenberg, A. (2014, November 4). Feds seize Silk Road 2 in major Dark Web drug bust. Retrieved December 10, 2014, from http://www.wired.com/2014/11/feds-seize-silk-road-2/

Greenberg, A. (2014, November 5). Global web crackdown arrests 17, seizes hundreds of Dark Net domains. Retrieved November 8, 2014, from http://www.wired.com/2014/11/operation-onymous-dark-web-arrests/

Greenberg, A. (2014, September 14). The FBI finally says how it ‘legally’ pinpointed Silk Road’s server. Retrieved September 9, 2014, from http://www.wired.com/2014/09/the-fbi-finally-says-how-it-legally-pinpointed-silk-roads-server/

Greenwald, G., Ball, J., & Schneier, B. (2013, October 4). NSA and GCHQ target Tor network that protects anonymity of web users. Retrieved October 26, 2014, from http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption

Grossman, L. (2013, November 13). The secret web: where drugs, porn and murder live online. Retrieved September 9, 2014, from http://time.com/630/the-secret-web-where-drugs-porn-and-murder-live-online/

Harris, S. (1996, April 4). Retiring the NSFNET Backbone Service: Chronicling the End of an Era. Retrieved October 2, 2014, from http://www.merit.edu/research/nsfnet_article.php

Holden, K. (2014, July 30). Breaking Through China's Great Firewall. Retrieved September 27,

2014, from http://thediplomat.com/2014/07/breaking-through-chinas-great-firewall/

Howard, P., Duffy, A., Freelon, D., Hussain, M., Mari, W., & Marwa, M. (2011). *Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring?* Washington D.C.: Project on Information Technology & Political Islam.

Kahin, B., & Keller, J. (1995). *Public access to the Internet*. Cambridge, Mass.: MIT Press.

Kirk, J. (2013, January 1). British man charged with hacking NASA and US military computers. Retrieved October 28, 2015, from http://www.computerworld.com/article/2485370/cybercrime-hacking/british-man-charged-with-hacking-nasa-and-us-military-computers.html

Lawrence, D. (2014, January 23). The inside story of Tor, the best Internet anonymity tool the government ever built. Retrieved September 18, 2014, from http://www.bloomberg.com/bw/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-agency.

Lee, D. (2014, November 10). Dark net raids 'overblown' - Tor. Retrieved December 10, 2014, from http://www.bbc.com/news/technology-29987379

Lewis, J. (2010). *Cyberwarfare and its impact on international security*. New York, NY: United Nations.

Lie, H., Boss, B., & Lilley, C. (1998, March 1). Request for Comments: 2318. Retrieved November 3, 2014, from http://tools.ietf.org/html/rfc2318

Lozhkin, S. (2014, March 3). Tor hidden services – A safe haven for cybercriminals. Retrieved March 4, 2015, from http://securelist.com/blog/incidents/58542/tor-hidden-services-a-safe-haven-for-cybercriminals/

Luhn, A. (2014, July 25). Russia offers 3.9m roubles for 'research to identify users of Tor.

Retrieved February 28, 2015, from http://www.theguardian.com/world/2014/jul/25/russia-research-identify-users-tor

McKim, J. (2012, March 8). Walpole company's anonymity software aids illicit deals. Retrieved September 14, 2014, from http://www.boston.com/business/technology/articles/2012/03/08/walpole_companys_anonymity_software_aids_elicit_deals/?page=1

Microsoft. (2003) *How TCP/IP works*. Retrieved November 2, 2014, from http://technet.microsoft.com/en-us/library/cc786128(v=WS.10).aspx

Murphy, M. (2010, July 3). War in the fifth domain. Retrieved September 28, 2014, from http://www.economist.com/node/16478792

O'Luanaigh, C. (2012, January 12). CERN accelerating science. Retrieved November 2, 2014, from http://home.web.cern.ch/about/updates/2012/12/month-1991-web-spreads-beyond-cern

O'Luanaigh, C. (2014, March 12). CERN accelerating science. Retrieved November 2, 2014, from http://home.web.cern.ch/about/updates/2014/03/world-wide-web-born-cern-25-years-ago

O'Reilly, T. (2005, September 30). What Is Web 2.0. Retrieved October 25, 2014, from http://www.webcitation.org/getfile?fileid=52c8d8126b62672683a3a555a63939d9b58cd767

Onion Routing. (n.d.). The history of Onion Routing. Retrieved September 14, 2014, from http://www.onion-router.net/History.html

OpenNet Initiative. (n.d.). The OpenNet Initiative. Retrieved September 28, 2014, from https://opennet.net/

Petroleum Economist. (2012, June 1). US fights cyber-attacks on gas pipelines. Retrieved March 4, 2015, from http://www.petroleum-economist.com/Article/3029489/Technology/US-fights-cyber-attacks-on-gas-pipelines.html

Poole, H. (2005). *The Internet a historical encyclopedia*. Santa Barbara, Calif.: ABC-CLIO.

Post Report. (2013, June 26). Terrorists to ditch Skype and YouTube after leaks reveal NSA surveillance tactics. Retrieved March 4, 2015, from http://nypost.com/2013/06/26/terrorists-to-ditch-skype-and-youtube-after-leaks-reveal-nsa-surveillance-tactics/

Poulsen, K. (2013, September 13). FBI admits it controlled Tor servers behind mass malware attack. Retrieved September 9, 2014, from http://www.wired.com/2013/09/freedom-hosting-fbi/

Poulsen, K. (2014, August 14). Visit the wrong website, and the FBI could end up in your computer. Retrieved August 22, 2014, from http://www.wired.com/2014/08/operation_torpedo/

Rogers, J. (1998). Internetworking and the politics of science: NSFNET in Internet history. *The Information Society, 14*(3), 213-228.

Schneier, B. (2013, October 4). Attacking Tor: How the NSA targets users' online anonymity. Retrieved September 14, 2014, from http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

Segal, B. (1995, April 1). A short history of Internet protocols at CERN. Retrieved November 2, 2014, from http://ben.home.cern.ch/ben/TCPHIST.html

Soengas-Pérez, X. (2013). The role of the Internet and social networks in the Arab uprisings: An alternative to official press censorship. *Comunicar, 21*(41), 147-155.

Tails. (2015, March 16). About Tails. Retrieved March 26, 2015, from https://tails.boum.org/about/index.en.html

Tait, R. (2012, August 5). Iranian state goes offline to dodge cyber-attacks. Retrieved September 27, 2014, from http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9453905/Iranian-state-goes-offline-to-dodge-cyber-attacks.html

Talbot, D. (2009, May 1). Dissent made safer. Retrieved September 7, 2014, from http://www.technologyreview.com/featuredstory/413091/dissent-made-safer/

Thompson, C. (2006, April 22). Google's China problem (and China's Google problem). Retrieved September 27, 2014, from http://www.nytimes.com/2006/04/23/magazine/23google.html?pagewanted=4&_r=1&_r=0

Tor. (n.d.). About the Tor project. Retrieved September 14, 2014, from https://www.torproject.org/about/overview.html.en

United Nations Office on Drugs and Crime (UNODC). (2014, June 1). World drug report 2014. Retrieved September 9, 2014, from http://www.unodc.org/wdr2014/

Van Atta, R. (2008, January 1). 50 Years of innovation and discovery. Retrieved January 22, 2015, from http://www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2553

Vossen, G., & Hagemann, S. (2007). *Unleashing Web 2.0 from concepts to creativity*. Amsterdam, Netherlands: Elsevier/Morgan Kaufmann.

Wakefield, J. (2014, November 7). Huge raid shuts 400 'dark net' sites. Retrieved November 8, 2014, from http://www.bbc.com/news/technology-29950946

Waldrop, M. (2008, January 1). DARPA and the Internet revolution. Retrieved January 22, 2015,

from http://www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2554

Watson, K. (2012). *The Tor Network: A Global Inquiry into the Legal Status of Anonymity Networks*. Washington D.C.: Washington University Global Studies Law Review.

Werbach, K. (1997, March 1). Internet history :: NSFNET. Retrieved October 2, 2014, from http://www.cybertelecom.org/notes/nsfnet.htm#aup

Young, M. (2014). The impacts of illegal disclosures of classified information. *A Journal of Law and Policy for the Information Society, 10*(367).

Zakon, R. (n.d.). Hobbes' Internet timeline - the definitive ARPAnet & Internet history. Retrieved October 25, 2014, from http://www.zakon.org/robert/internet/timeline/

Appendix 1: Tor .onion Hidden Services Websites

.Onion Directories

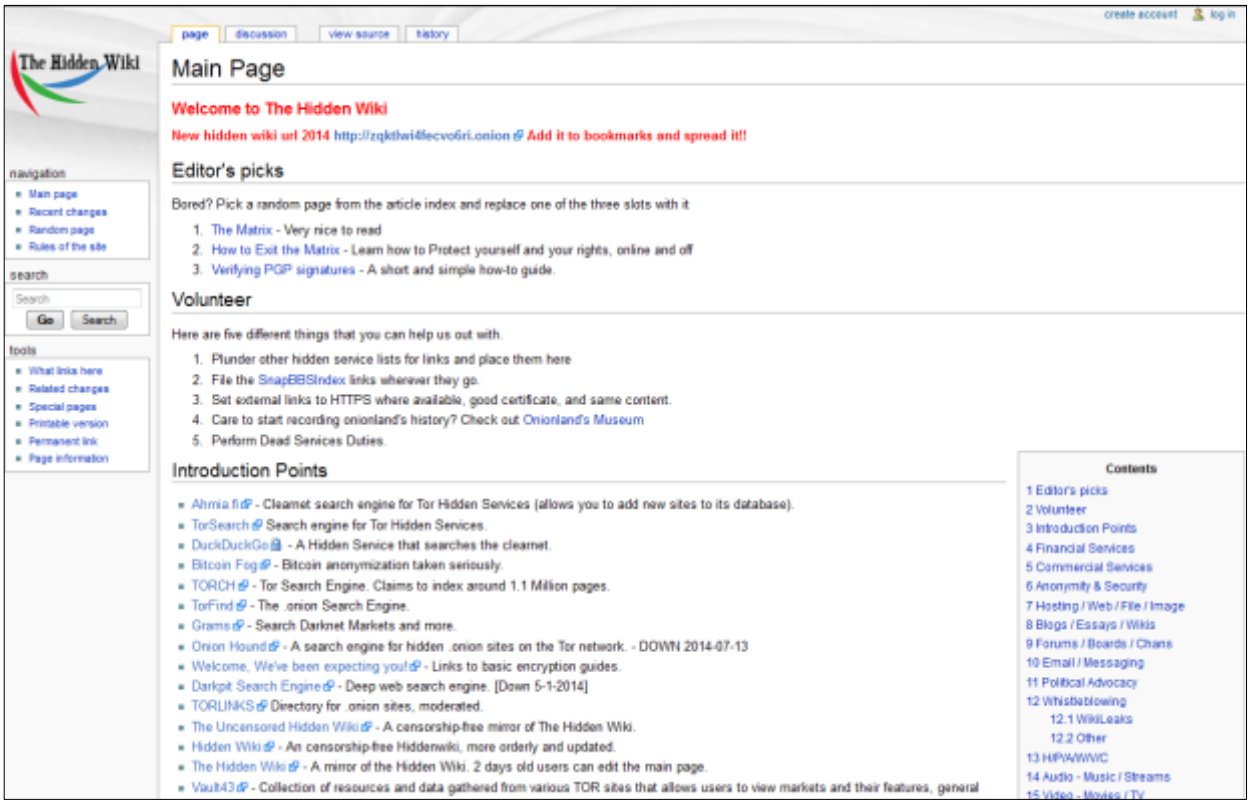


Figure 1: The Hidden Wiki
URL: http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page
Description: Primary listing of Tor Hidden Services .onion sites
Date Accessed: September 17, 2014

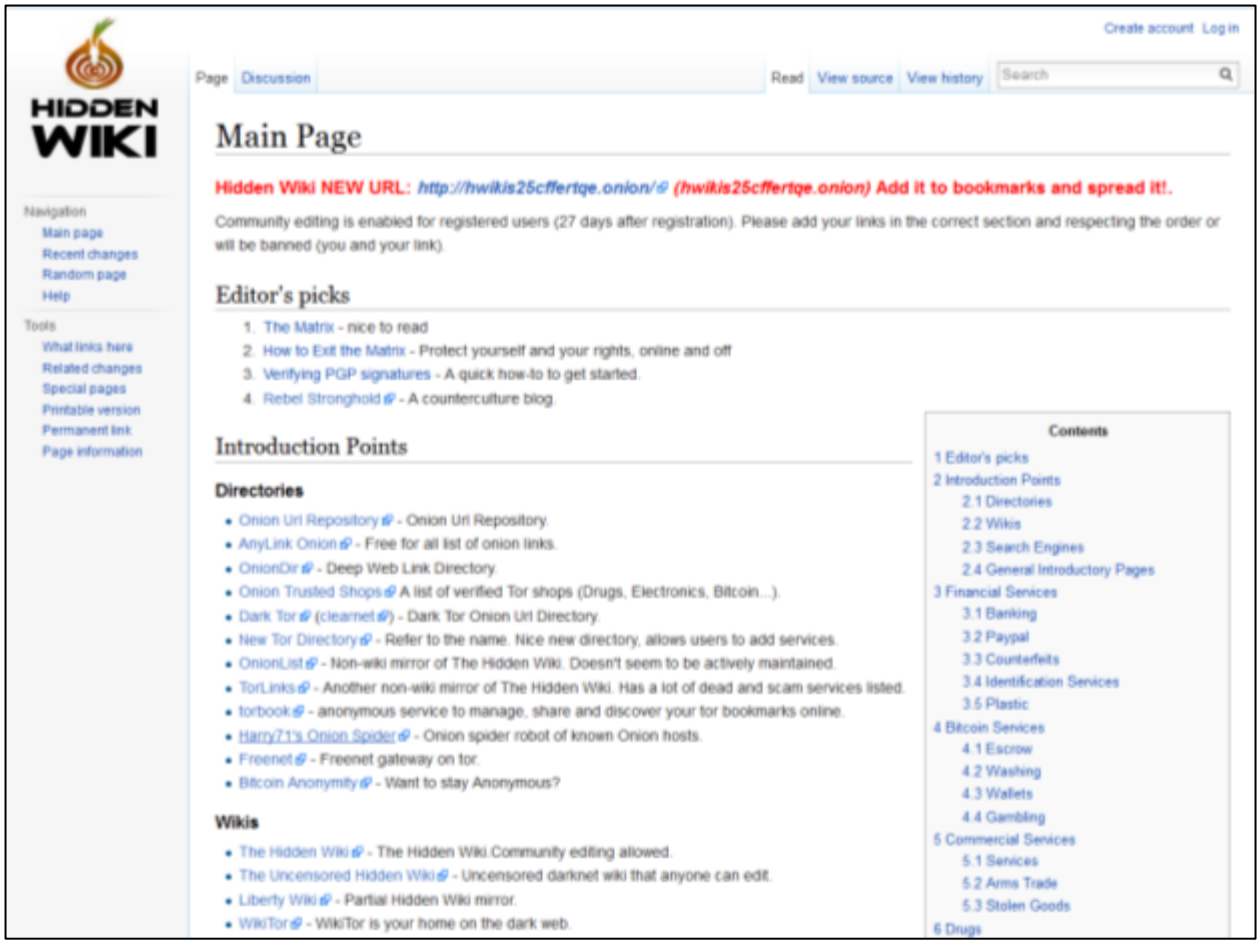


Figure 2: The Updated Hidden Wiki
URL: http://hwikis25cffertqe.onion/index.php?title=Main_Page
Description: A more current and better organized version of the Hidden Wiki
Date Accessed: March 27, 2015

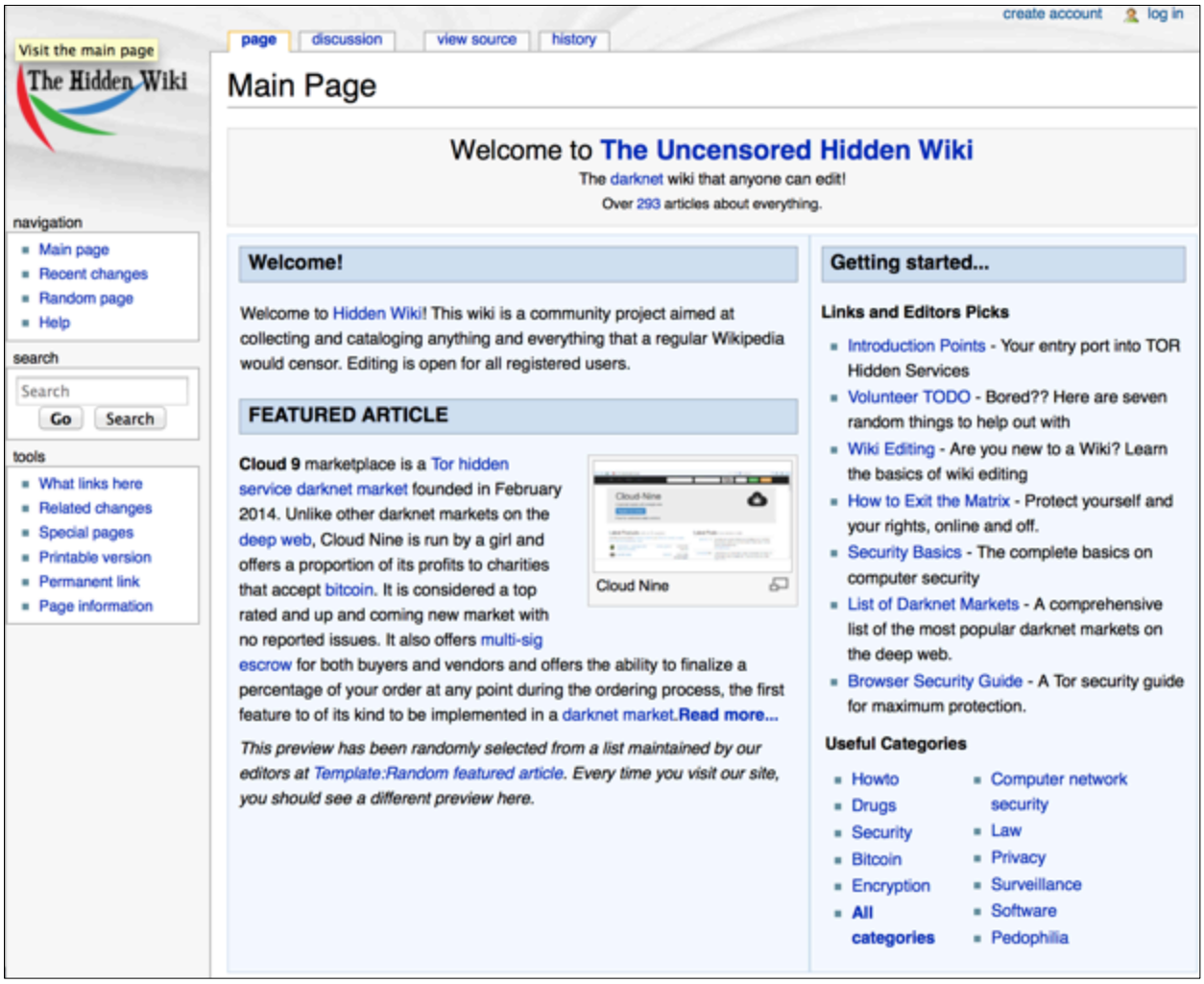


Figure 3: The Uncensored Hidden Wiki
URL: http://kpvz7kpmcmne52qf.onion/wiki/index.php/Main_Page
Description: Uncensored wiki containing Tor .onion links and beginner information
Date Accessed: September 17, 2014

Darknet eCommerce Solutions

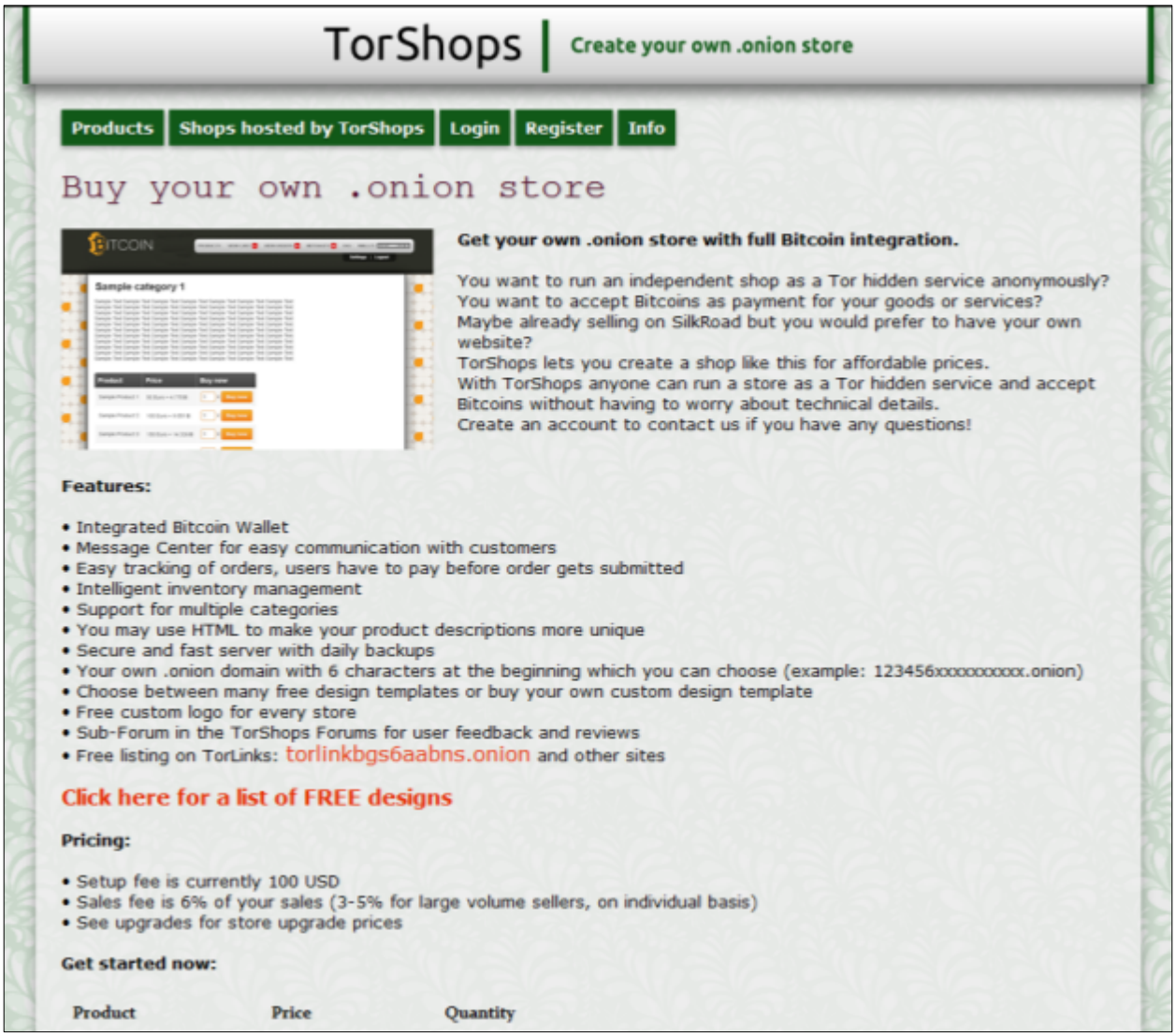


Figure 4: TorShops
URL: http://shopsat2dotfotbs.onion/
Description: Develops custom marketplace websites compatible with Bitcoin transaction tools
Date Accessed: September 17, 2014

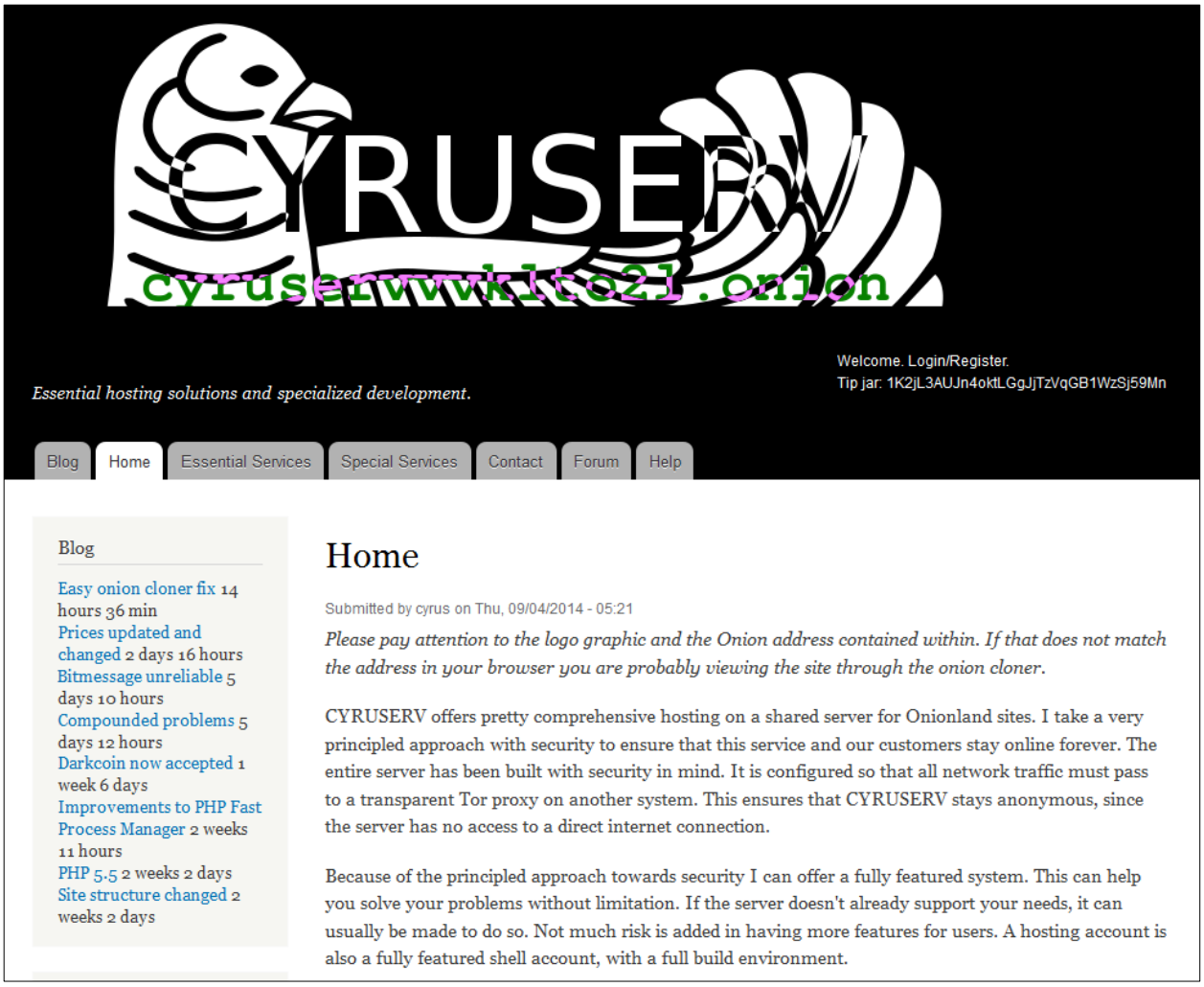


Figure 5: CYRUSERV
URL: http://cyruservvvklto2l.onion/
Description: Tor .onion hosting
Date Accessed: September 17, 2014

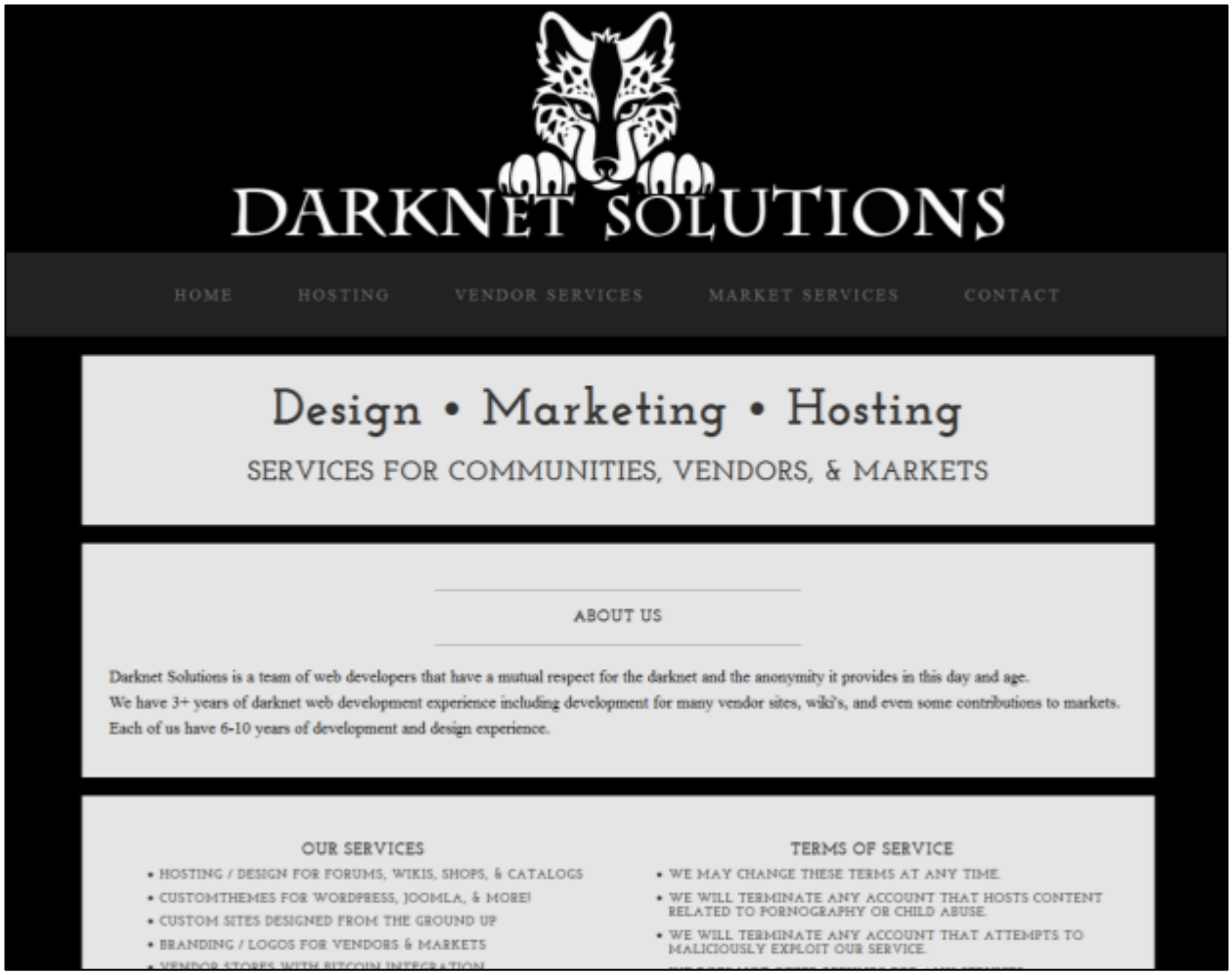


Figure 6: Darknet Solutions
URL: http://darknet47je5xwm6.onion/
Description: Website development and graphic design
Date Accessed: March 27, 2015

Hacking

Figure 7: Rent-a-Hacker
URL: http://2ogmrlfzdthnwkez.onion/index.php
Description: Hackers for hire
Date Accessed: September 17, 2014

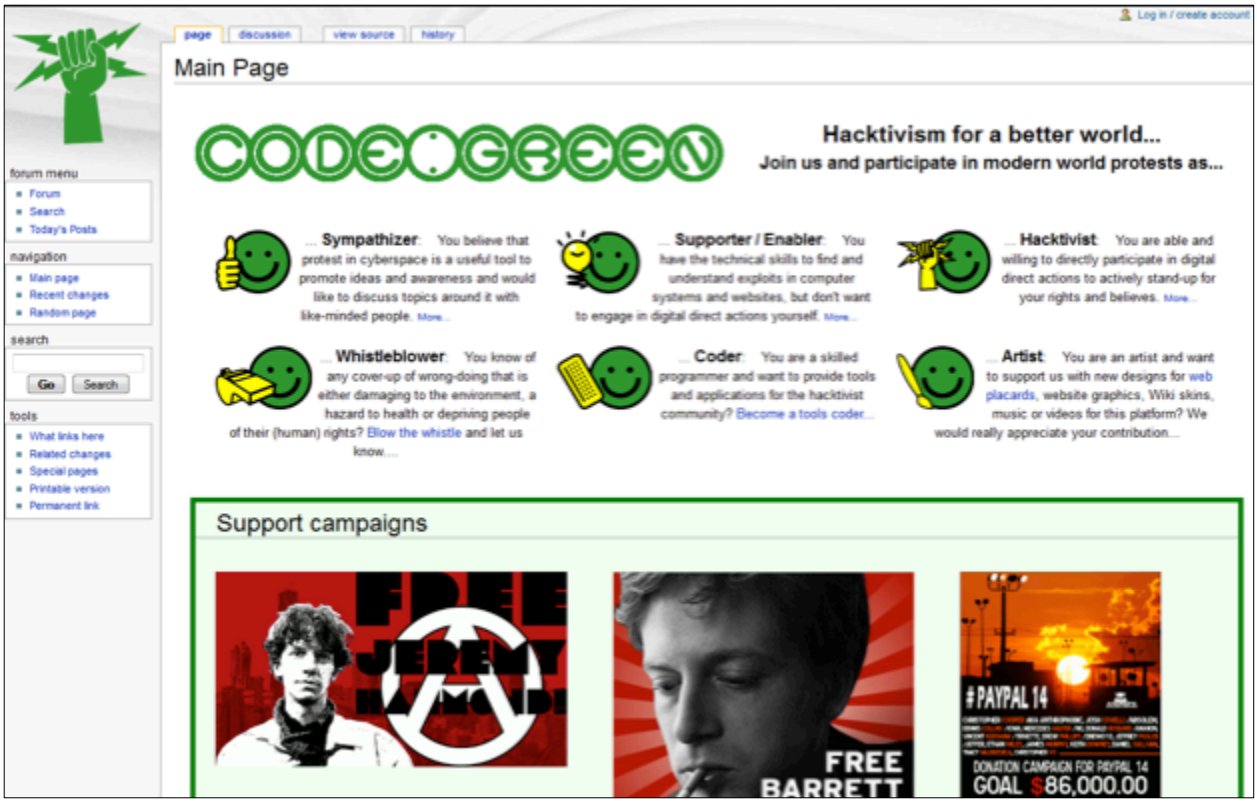


Figure 8: Code Green
URL: http://pyl7a4ccwgpxm6rd.onion/w/index.php/Main_Page
Description: Hacktivism coordination, recruiting, and support
Date Accessed: September 17, 2014

Islamic Extremism

Figure 9: Fund the Islamic Struggle Anonymously
URL: http://teir4baj5mpvkg5n.onion/
Description: Possible Islamic radical recruiting & funding
Date Accessed: September 17, 2014

Seized .onion Joint Law Enforcement Notice

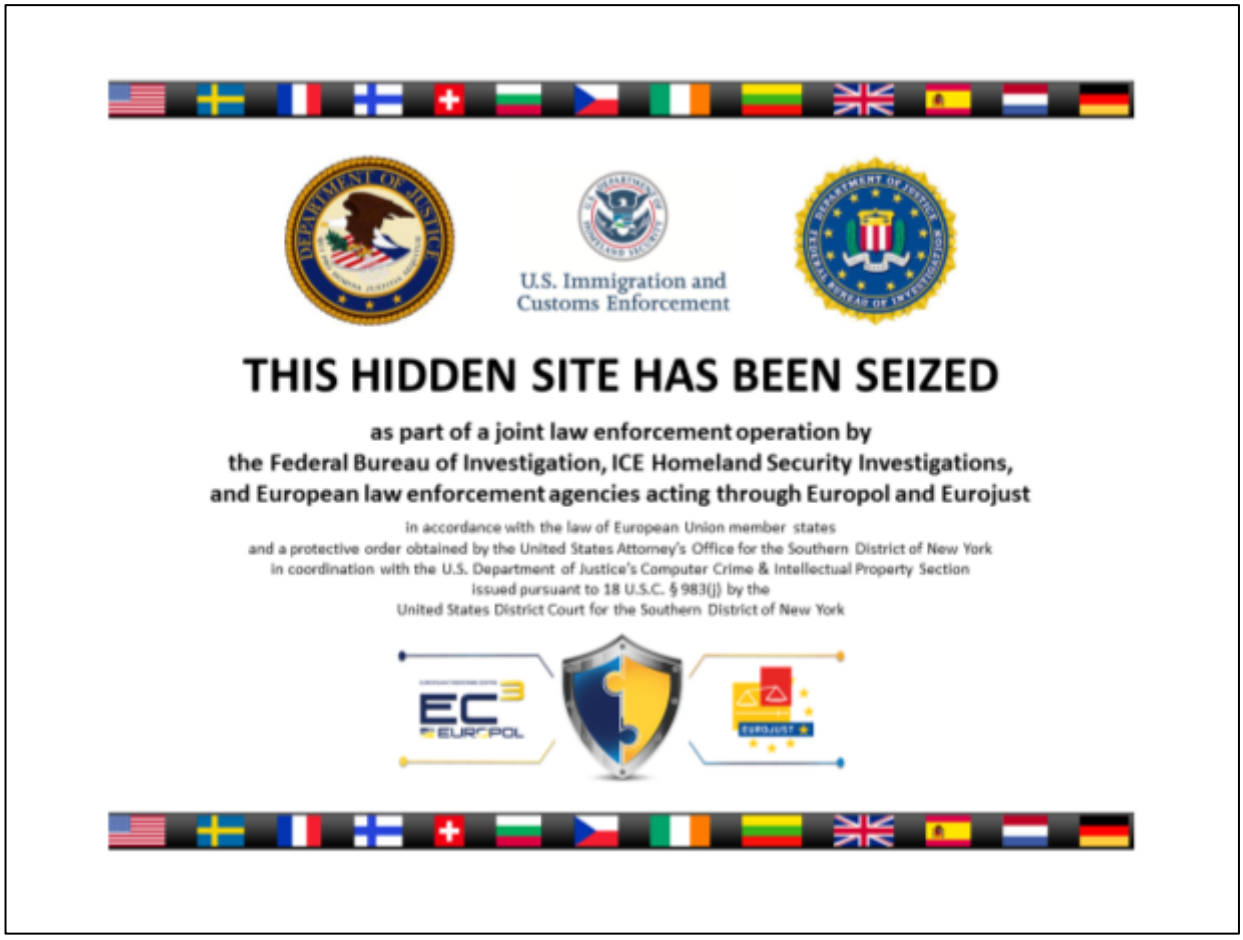


Figure 10: Law Enforcement Seized Server Banner
URL: http://3admlcgsahtchgwj.onion/
Description: Banner displayed after law enforcement seized a .onion site
Date Accessed: March 27, 2015

Uncategorizable

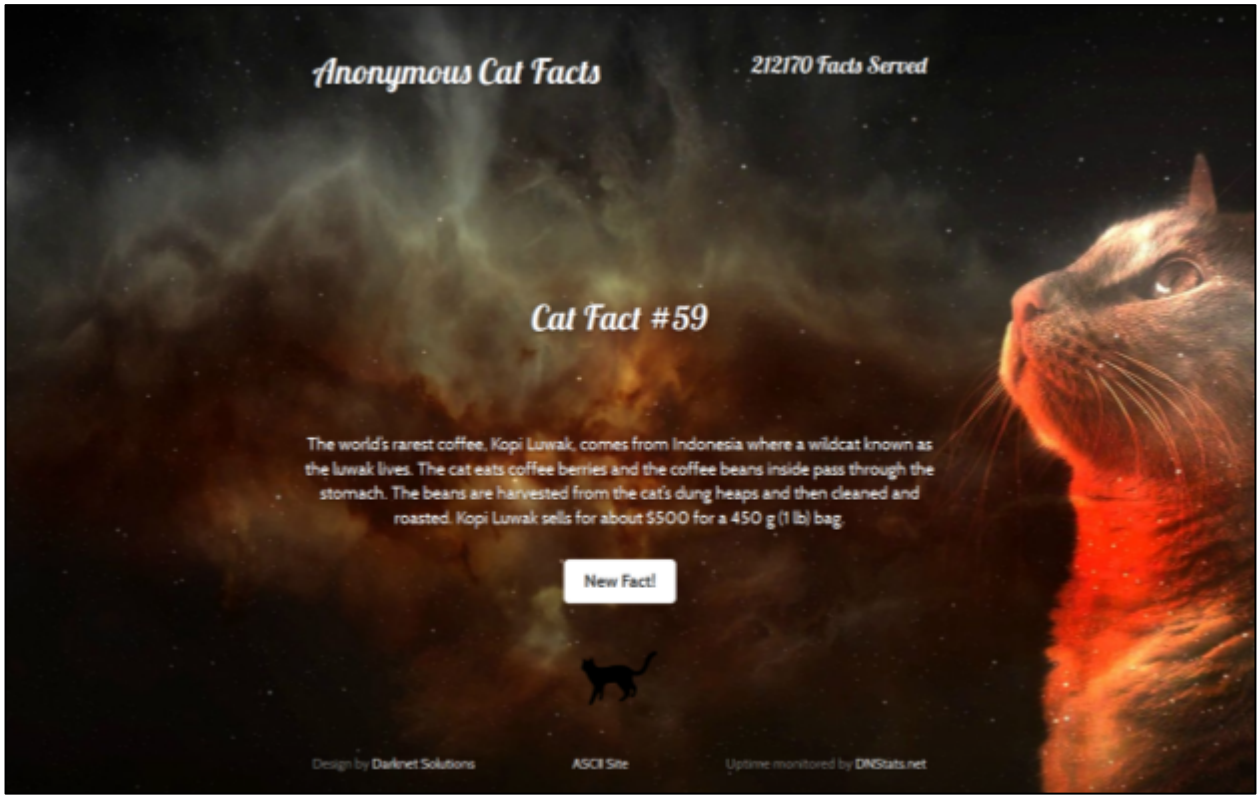


Figure 11: Anonymous Cat Facts
URL: http://2v7ibl5u4pbemwiz.onion/
Description: Generate cat trivia on demand
Date Accessed: March 27, 2015

Mainstream Organizations .onion Websites

Figure 12: The Tor Project
URL: http://tmdrhl4e4anhsjc5.onion/
Description: The .onion website for the Tor Project
Date Accessed: March 27, 2015

Figure 13: Samsung
URL: http://storegsq3o5mfxiz.onion/
Description: Official Samsung .onion website
Date Accessed: March 27, 2015

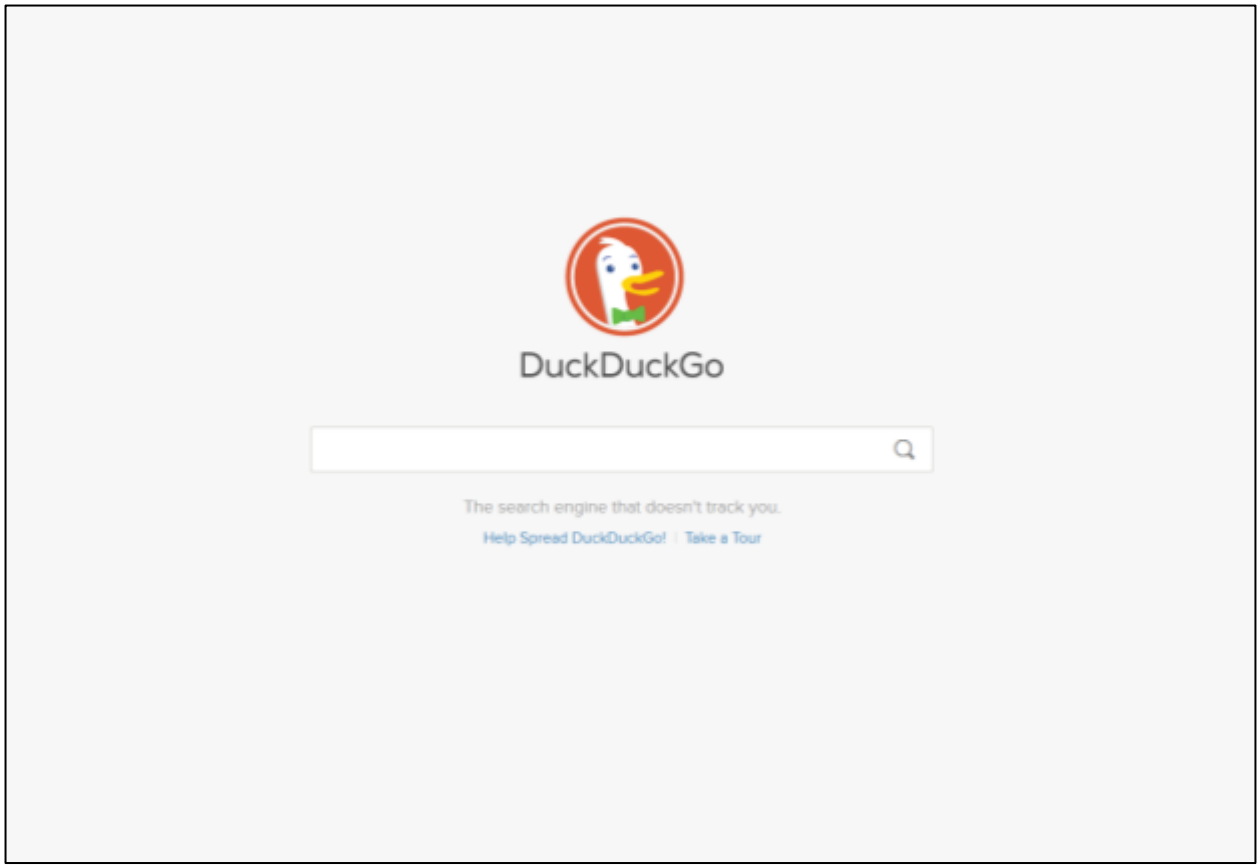


Figure 14: DuckDuckGo
URL: http://3g2upl4pq6kufc4m.onion/
Description: The Duck Duck Go search engine .onion
Date Accessed: March 27, 2015

Music

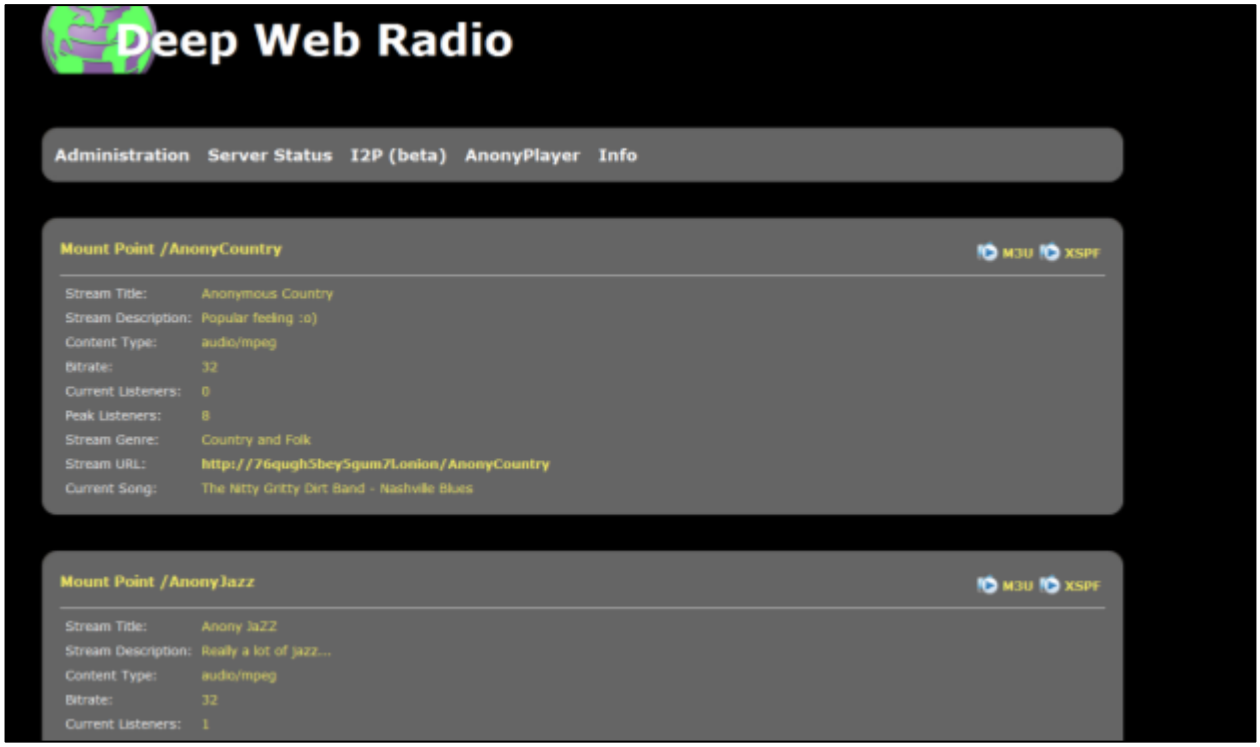


Figure 15: Deep Web Radio
URL: http://76qugh5bey5gum7l.onion/
Description: Streaming Internet radio
Date Accessed: March 27, 2015

Tor Email

Figure 16: TorBox
URL: http://torbox3uiot6wchz.onion/
Description: Anonymous Tor webmail
Date Accessed: March 27, 2015

Figure 17: Mailtor
URL: http://mailtoralnhyol5v.onion/src/login.php
Description: Anonymous Tor email provider
Date Accessed: March 27, 2015

Development

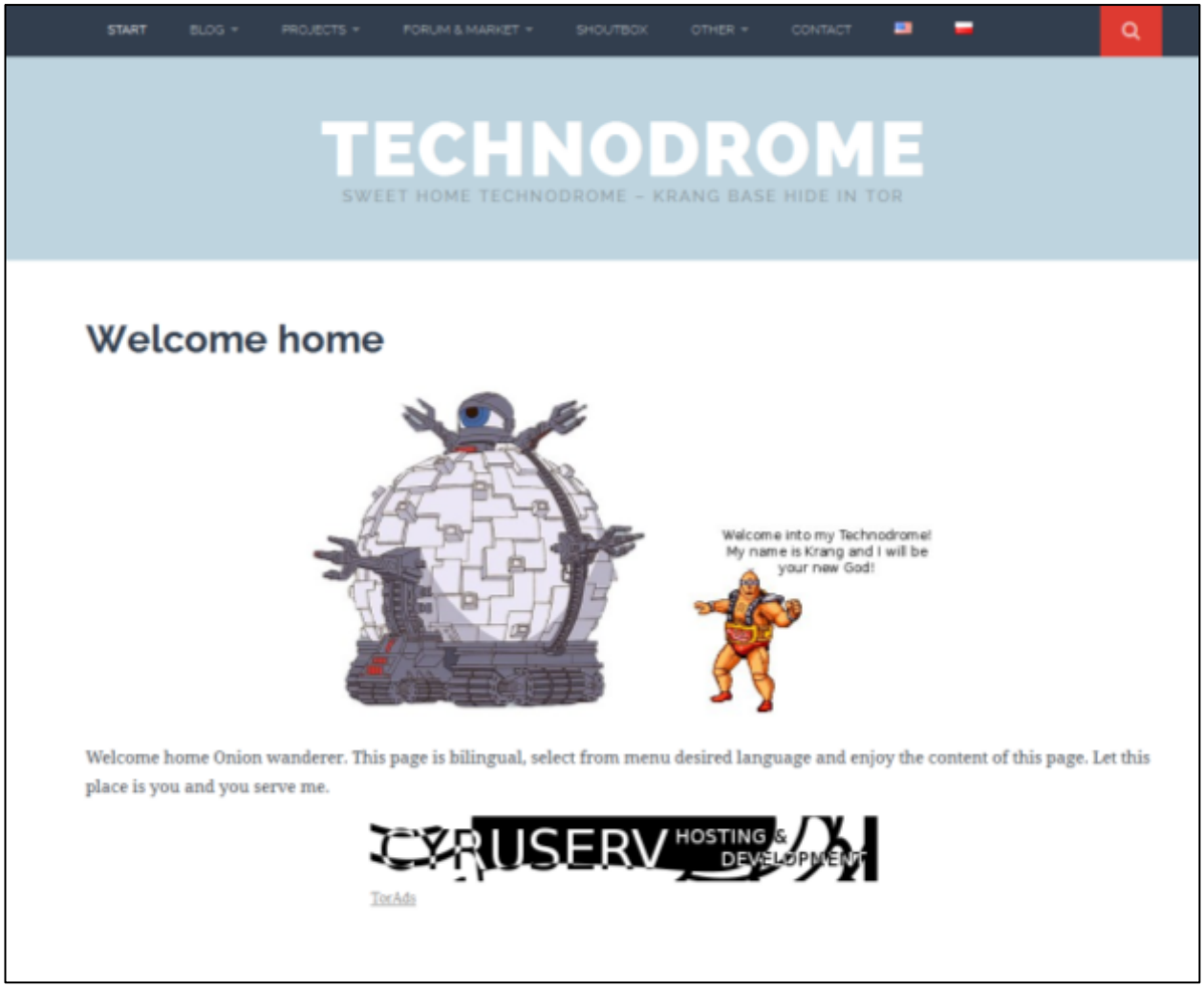


Figure 18: Technodrome
URL: http://54ogum7gwxhtgiya.onion/blog/index.php/welcome-home/
Description: Software development
Date Accessed: March 27, 2015

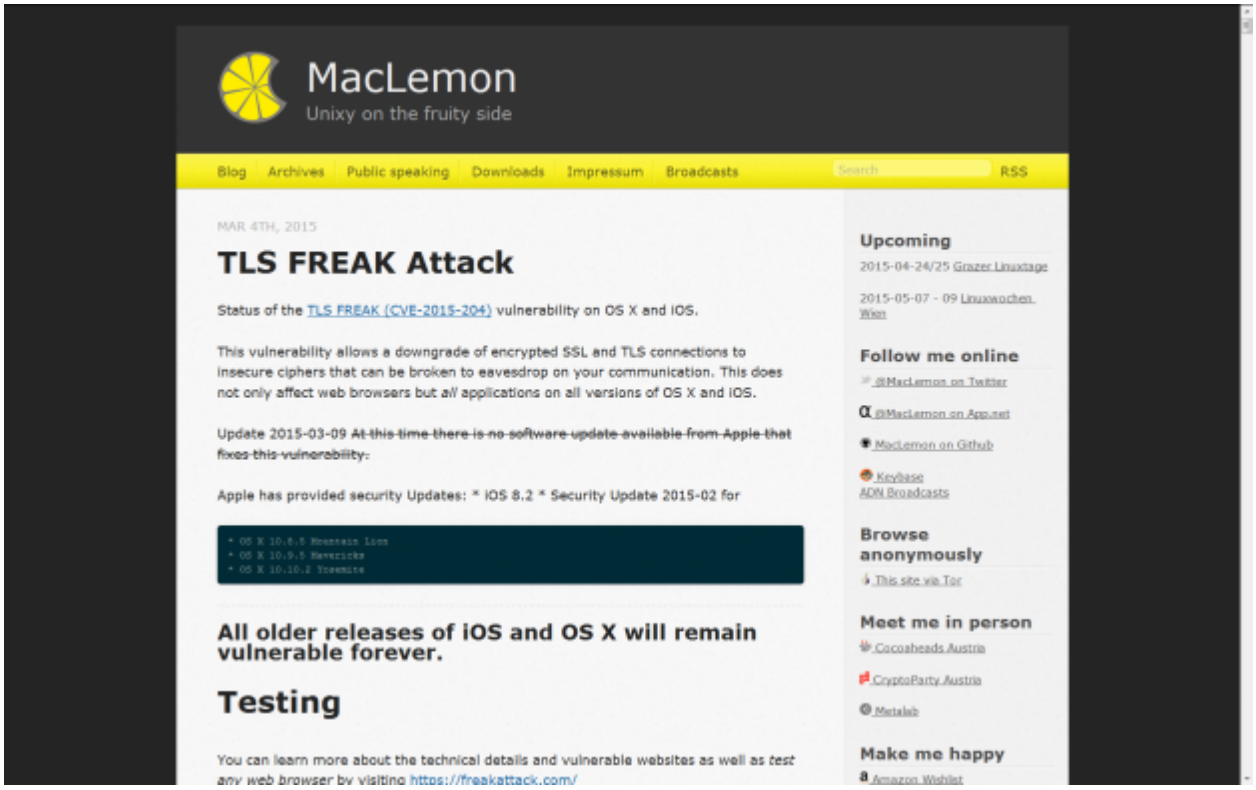


Figure 19: MacLemon
URL: http://fzybdgczph7xfdnr.onion/
Description: Security blog
Date Accessed: March 27, 2015

Whistlebowers Resources

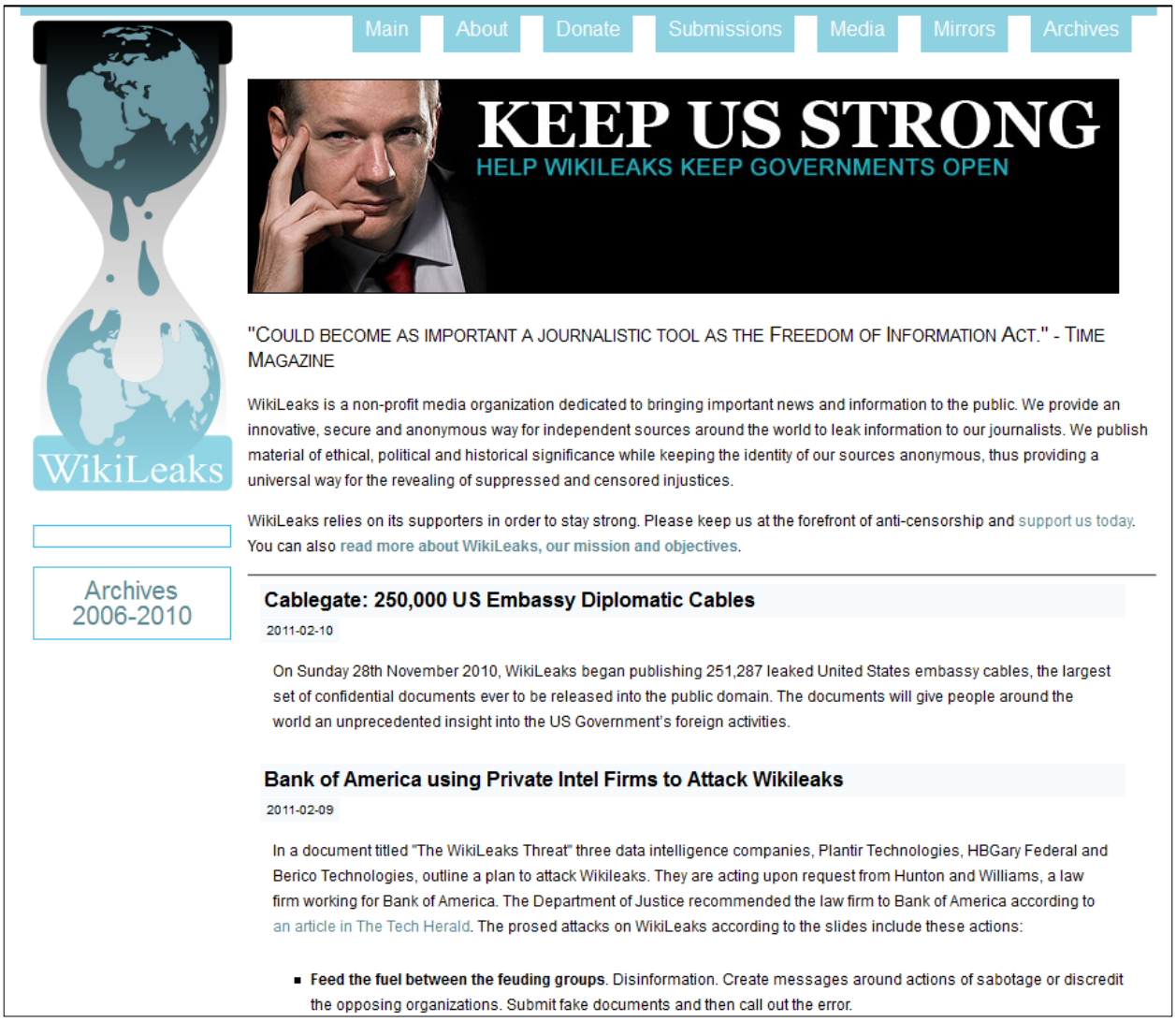


Figure 20: WikiLeaks
URL: http://zbnnr7qzaxlk5tms.onion/
Description: WikiLeaks Tor .onion site
Date Accessed: September 17, 2014

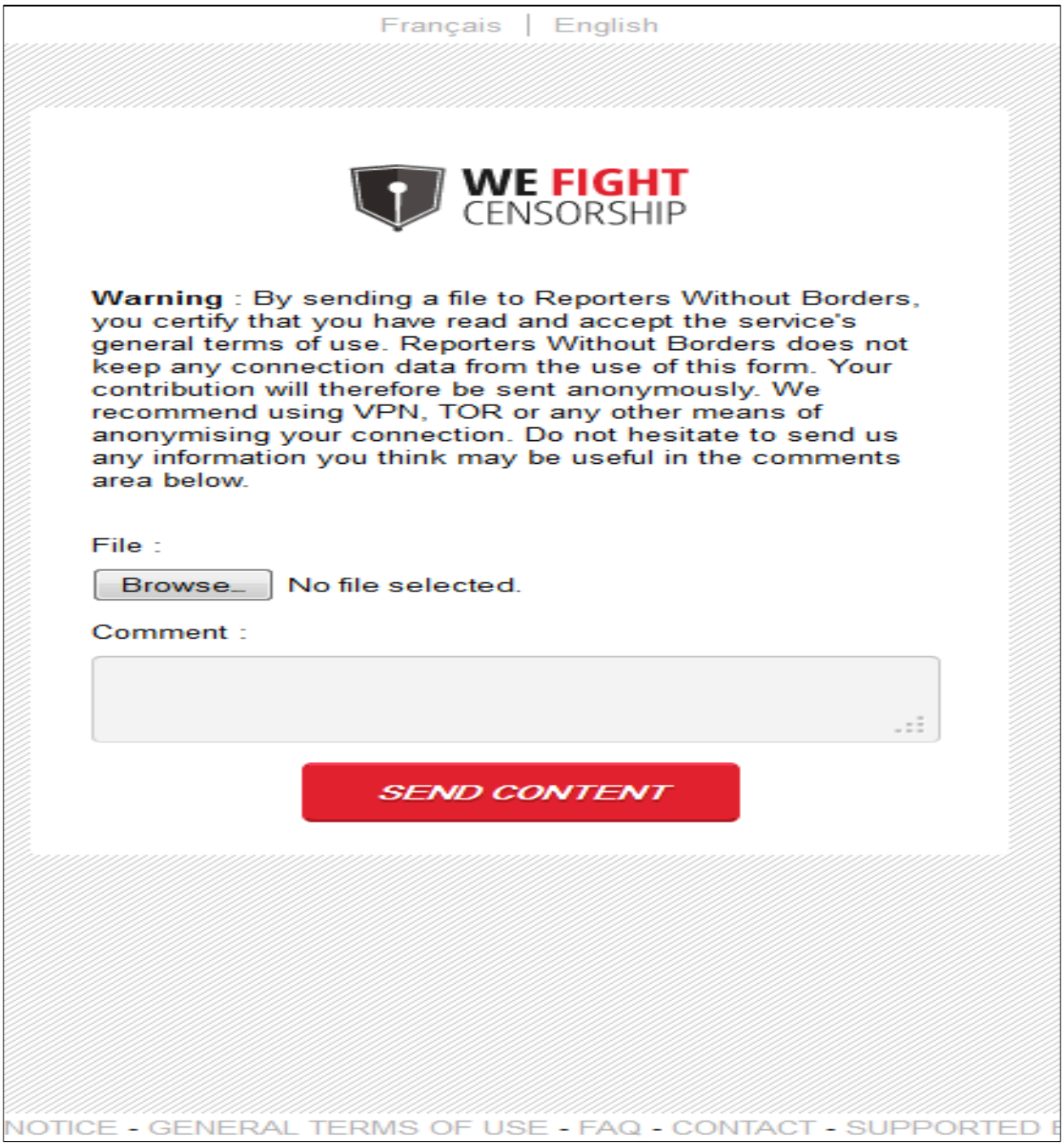


Figure 21: Reporters Without Borders: We Fight Censorship
URL: http://3kyl4i7bfdgwelmf.onion/
Description: Anti-censorship site managed by Reporters Without Borders that contains a secured drop box to submit potentially sensitive information without fear of reprisal
Date Accessed: September 17, 2014

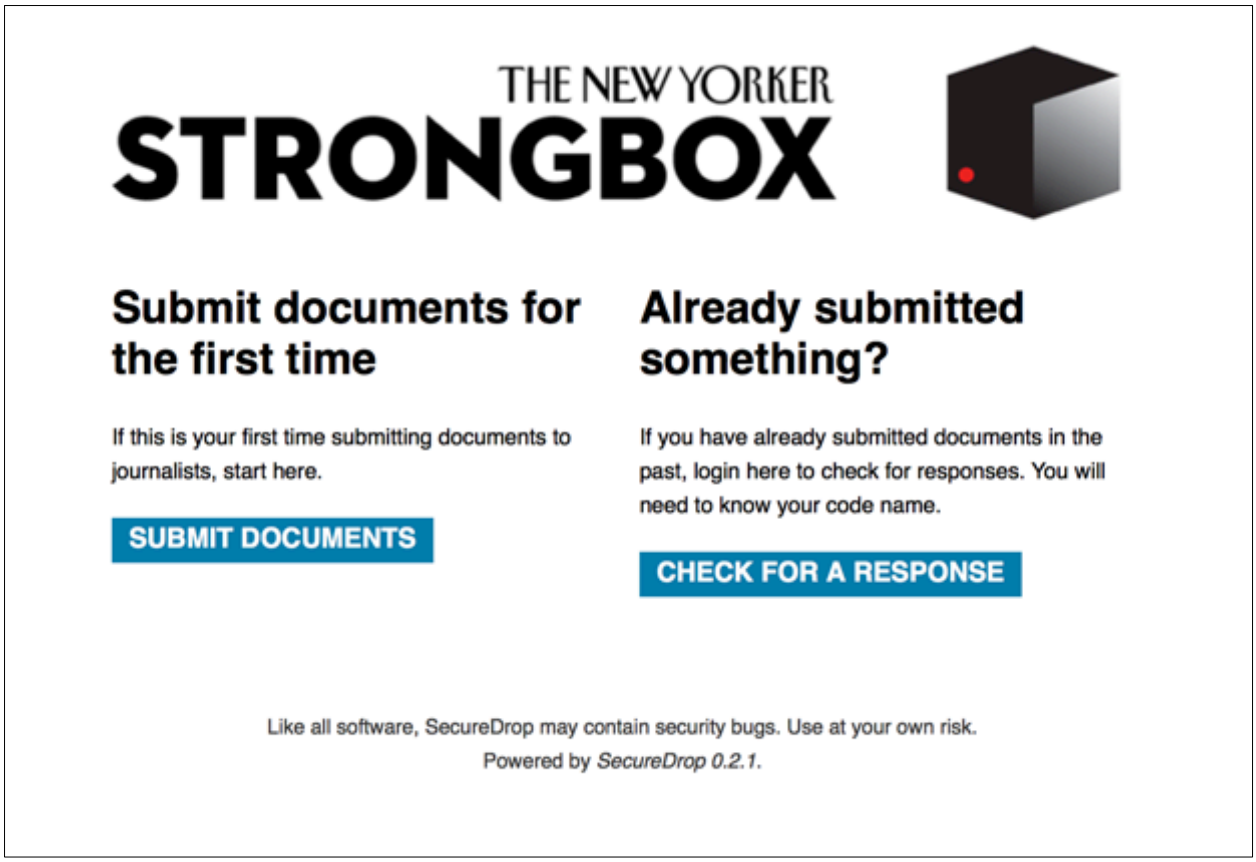


Figure 22: The New Yorker Anonymous STRONGBOX
URL: http://strngbxhwyuu37a3.onion/
Description: Safe-place for whistle blowers to anonymously release sensitive information to the New Yorker magazine
Date Accessed: September 17, 2014

Personal Information Clearinghouse

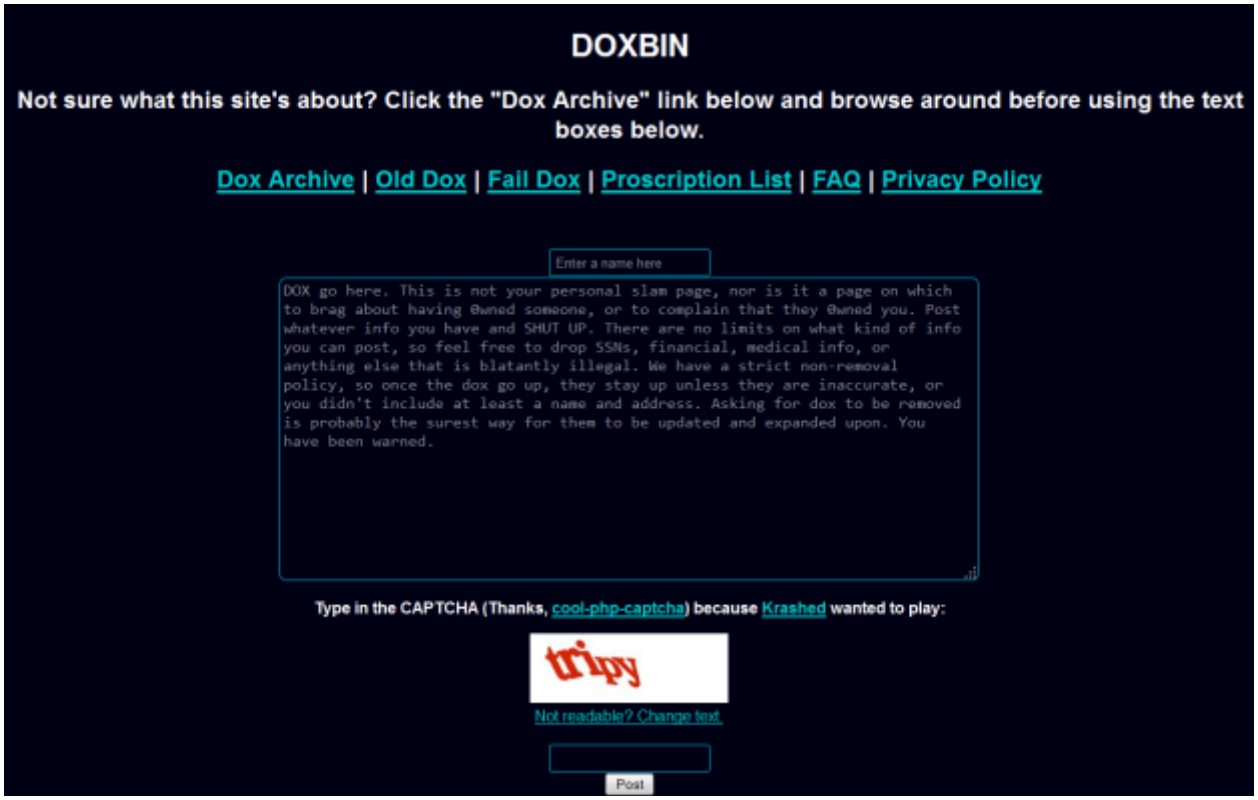


Figure 23: DOXBIN
URL: http://doxbinzqkeoso6sl.onion/
Description: Dumping ground for personal information
Date Accessed: September 17, 2014

Contract Murder

Figure 24: Hitman Network
URL: http://ybp4oezfhk24hxmb.onion/
Description: Killers for hire
Date Accessed: September 17, 2014

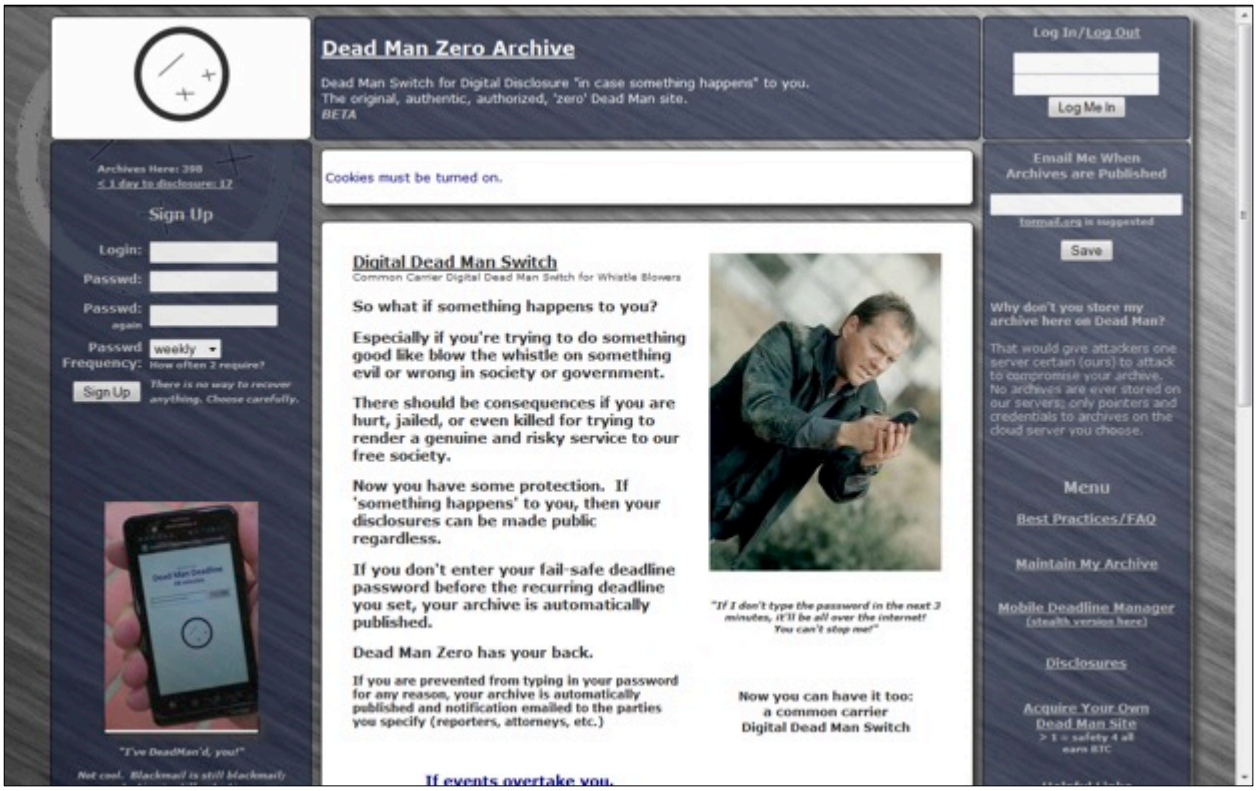
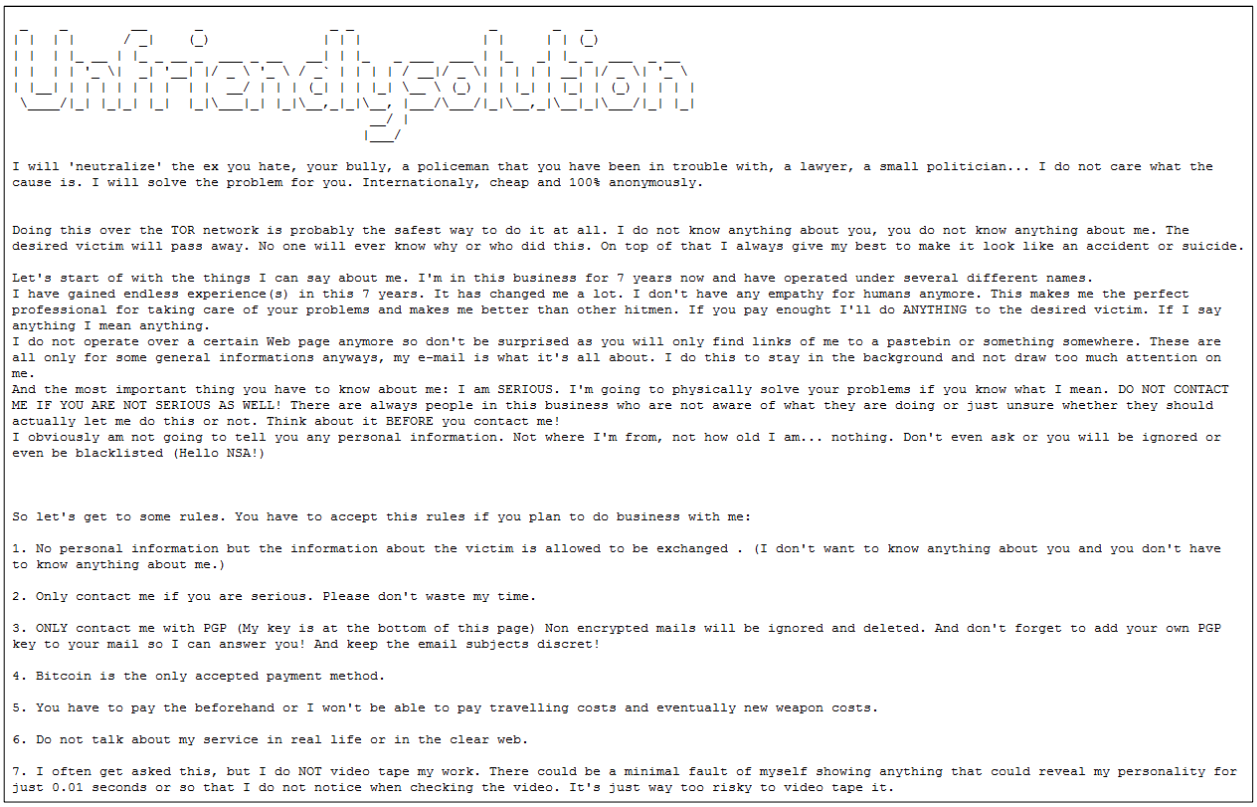


Figure 25: Dead Man Zero Archives
URL: http://wntxyw6zdeos7ag6.onion/
Description: Criminal insurance services
Date Accessed: September 17, 2014



I will 'neutralize' the ex you hate, your bully, a policeman that you have been in trouble with, a lawyer, a small politician... I do not care what the cause is. I will solve the problem for you. Internationaly, cheap and 100% anonymously.

Doing this over the TOR network is probably the safest way to do it at all. I do not know anything about you, you do not know anything about me. The desired victim will pass away. No one will ever know why or who did this. On top of that I always give my best to make it look like an accident or suicide.

Let's start of with the things I can say about me. I'm in this business for 7 years now and have operated under several different names.
I have gained endless experience(s) in this 7 years. It has changed me a lot. I don't have any empathy for humans anymore. This makes me the perfect professional for taking care of your problems and makes me better than other hitmen. If you pay enought I'll do ANYTHING to the desired victim. If I say anything I mean anything.
I do not operate over a certain Web page anymore so don't be surprised as you will only find links of me to a pastebin or something somewhere. These are all only for some general informations anyways, my e-mail is what it's all about. I do this to stay in the background and not draw too much attention on me.
And the most important thing you have to know about me: I am SERIOUS. I'm going to physically solve your problems if you know what I mean. DO NOT CONTACT ME IF YOU ARE NOT SERIOUS AS WELL! There are always people in this business who are not aware of what they are doing or just unsure whether they should actually let me do this or not. Think about it BEFORE you contact me!
I obviously am not going to tell you any personal information. Not where I'm from, not how old I am... nothing. Don't even ask or you will be ignored or even be blacklisted (Hello NSA!)

So let's get to some rules. You have to accept this rules if you plan to do business with me:

1. No personal information but the information about the victim is allowed to be exchanged . (I don't want to know anything about you and you don't have to know anything about me.)

2. Only contact me if you are serious. Please don't waste my time.

3. ONLY contact me with PGP (My key is at the bottom of this page) Non encrypted mails will be ignored and deleted. And don't forget to add your own PGP key to your mail so I can answer you! And keep the email subjects discret!

4. Bitcoin is the only accepted payment method.

5. You have to pay the beforehand or I won't be able to pay travelling costs and eventually new weapon costs.

6. Do not talk about my service in real life or in the clear web.

7. I often get asked this, but I do NOT video tape my work. There could be a minimal fault of myself showing anything that could reveal my personality for just 0.01 seconds or so that I do not notice when checking the video. It's just way too risky to video tape it.

Figure 26: Unfriendly Solutions
URL: http://pasterlczk6anaqz.onion/3d0b033eb3.txt
Description: Contract killing
Date Accessed: September 17, 2014

Professional Criminal Headhunting

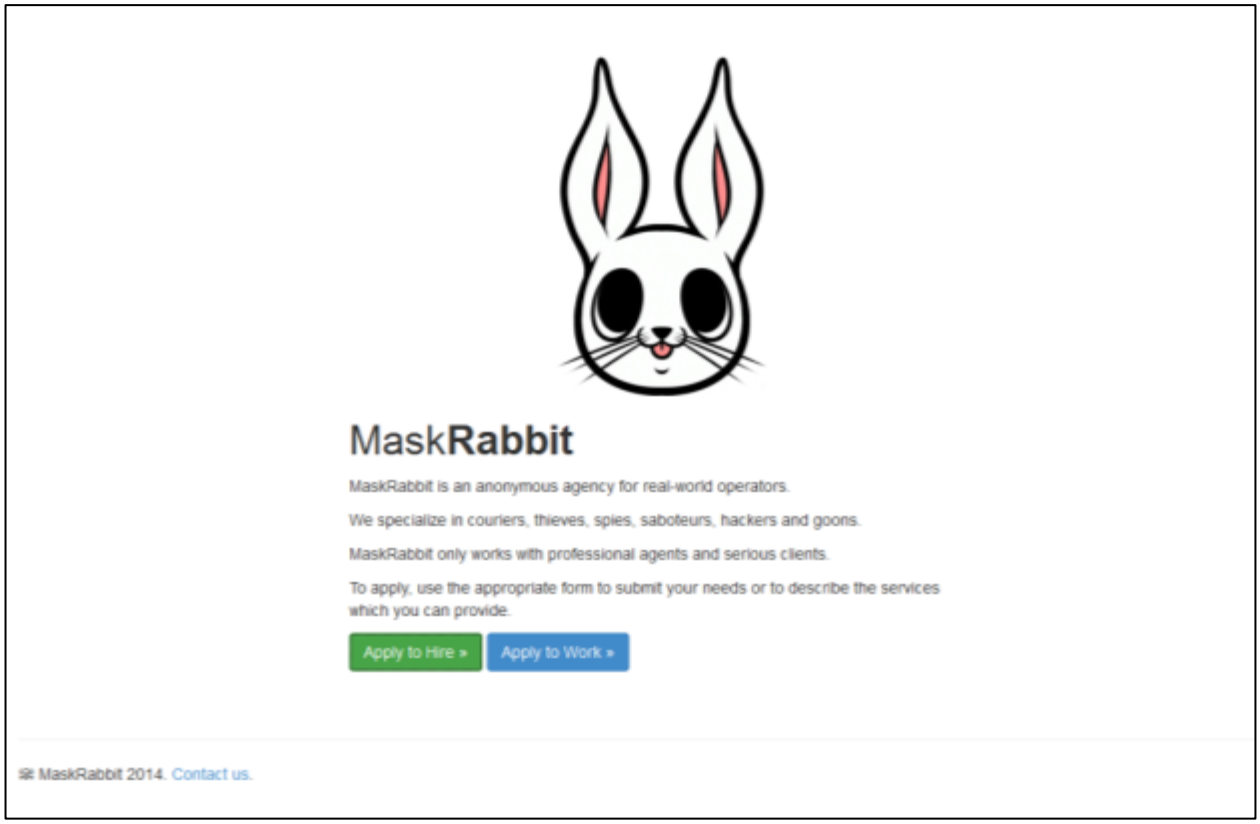


Figure 27: MaskRabbit
URL: http://maskravvbmurcaiz.onion/
Description: Professional criminal headhunting
Date Accessed: March 27, 2015

Forgeries

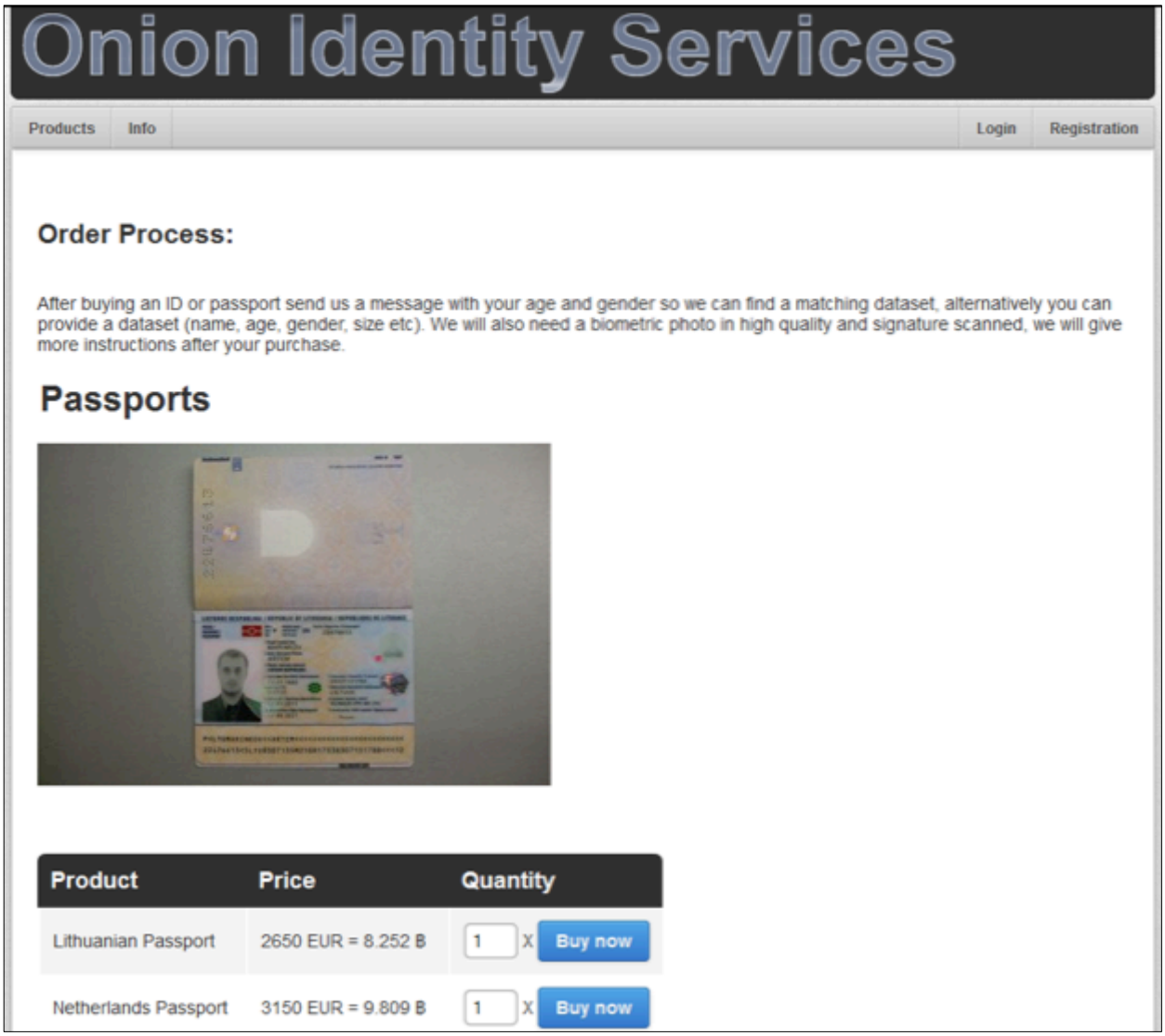


Figure 28: Onion Identity Services
URL: http://abbujjh5vqtq77wg.onion/index.php
Description: Custom forgeries
Date Accessed: September 17, 2014

Figure 29: Counterfeit USD
URL: http://qkj4drtgvpm7eecl.onion/
Description: Counterfeit American dollars
Date Accessed: September 17, 2014

Figure 30: Skimmed Cards
URL: http://cardpi2pickzonhr.onion/
Description: Equipment and information needed to produce cloned credit cards
Date Accessed: September 17, 2014

Fraud and Account Theft

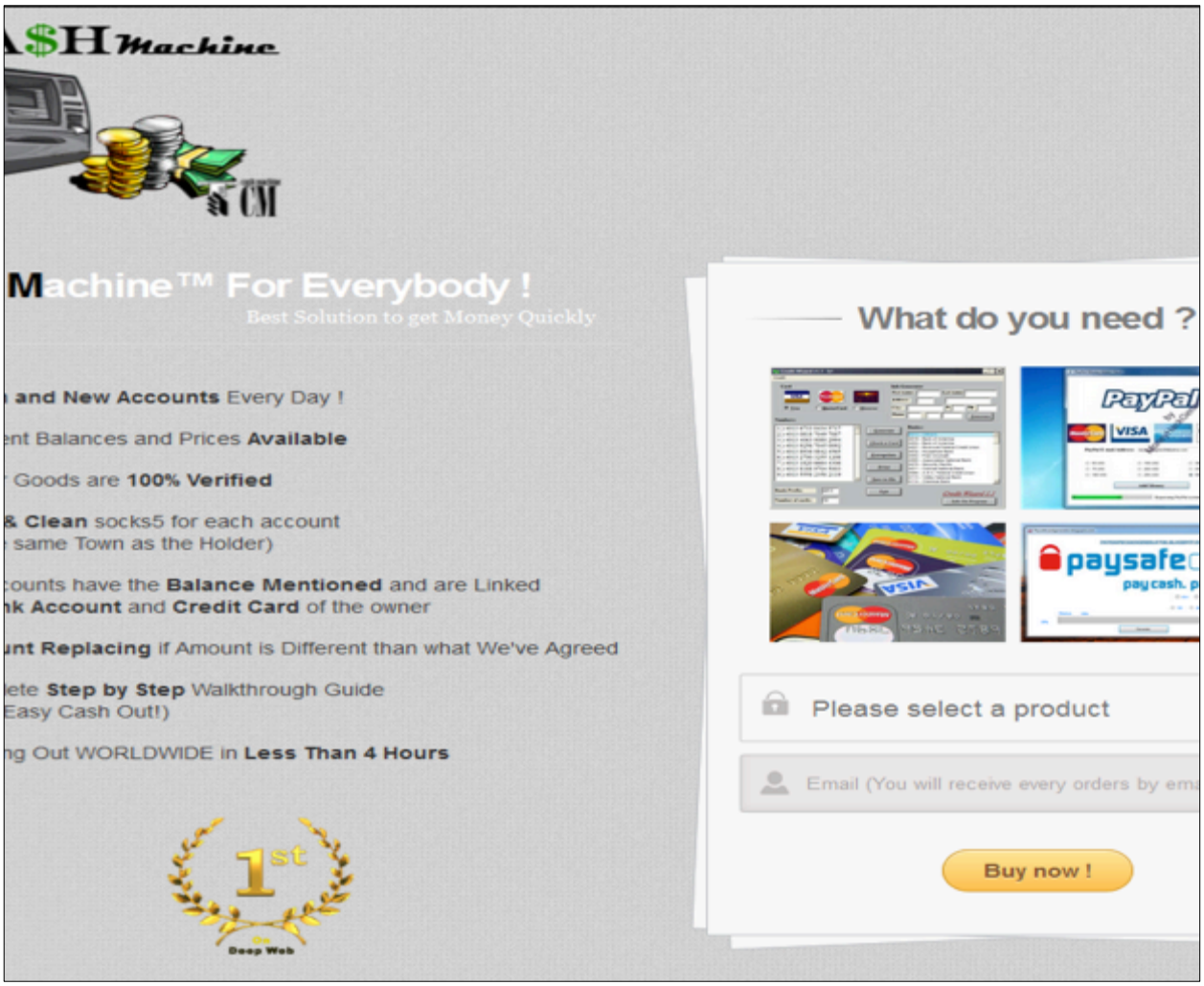


Figure 31: The Cash Machine
Link: http://hcutffvavocsh6nd.onion/
Description: Stolen credit card and financial information reseller
Date Accessed: September 17, 2014

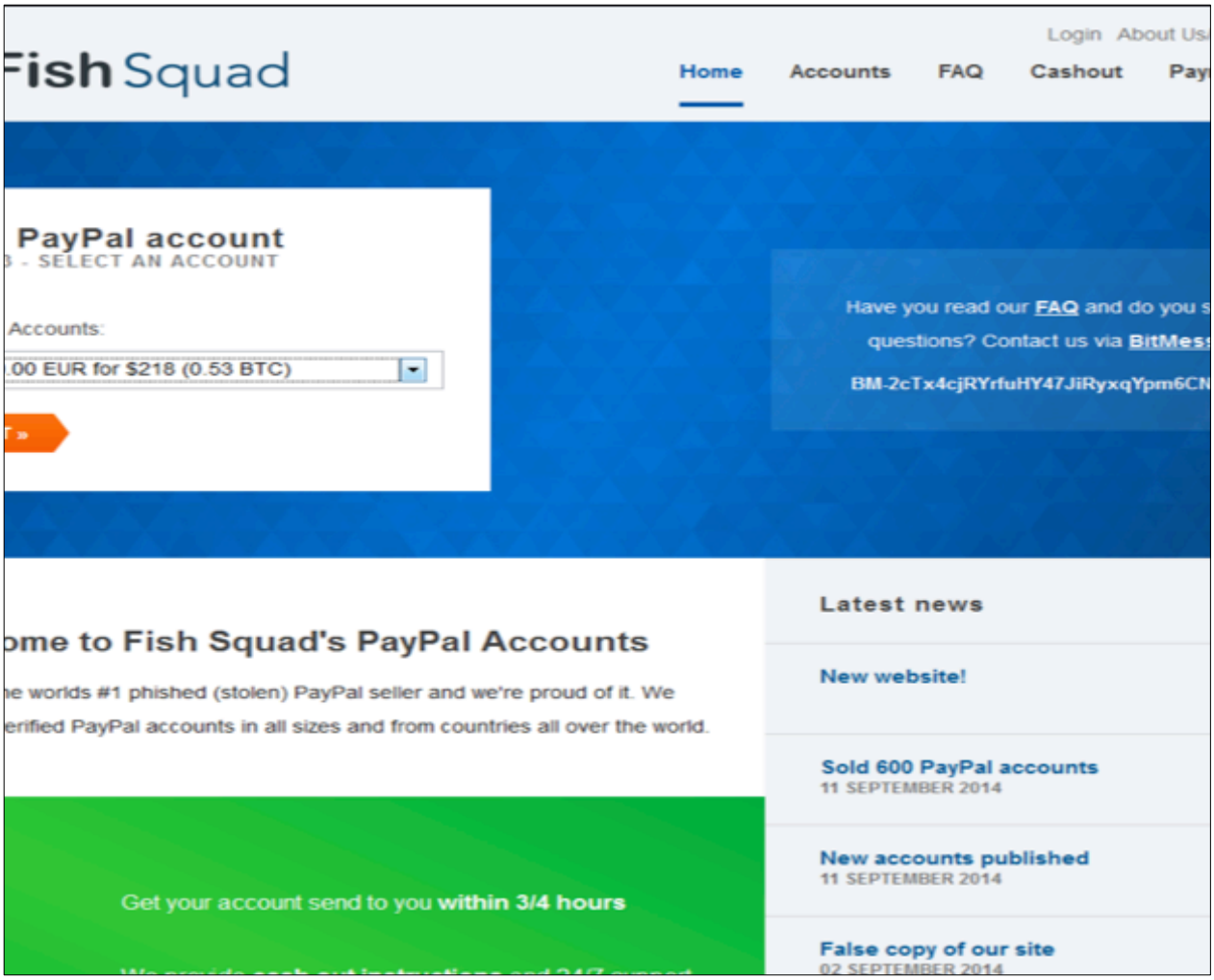


Figure 32: Fish Squad
URL: http://dxwmc6b3mtklq44j.onion/
Description: Resells stolen Paypal accounts
Date Accessed: September 17, 2014

Figure 33: Wall Street
URL: http://z2hjm7uhwisw5jm5.onion/
Description: Bulletin board hosting electronic crime related conversations
Date Accessed: September 17, 2014

Money Laundering & Escrow Services

Figure 34: BITMIX
URL: http://bitmixd2pgjsk373.onion/index.php
Category: Money Laundering
Description: Anonymizes Bitcoins bypassing Bitcoin exchanges and public block key
Date Accessed: September 17, 2014

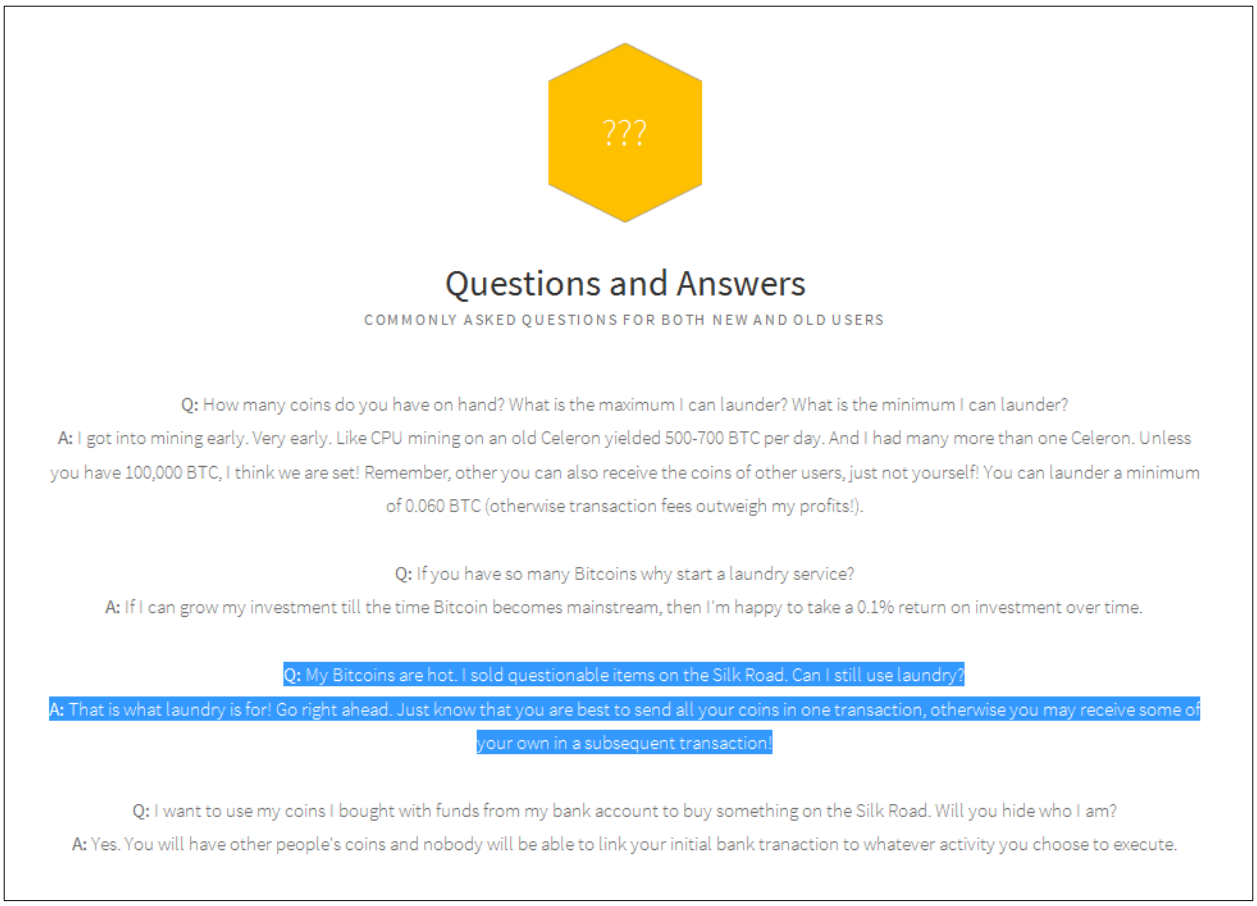


Figure 35: Clean My Coins!
URL: http://pa4g5tyna45tonbx.onion/
Category: Money Laundering
Description: Anonymizes Bitcoins bypassing Bitcoin exchanges and public block key
Date Accessed: September 17, 2014

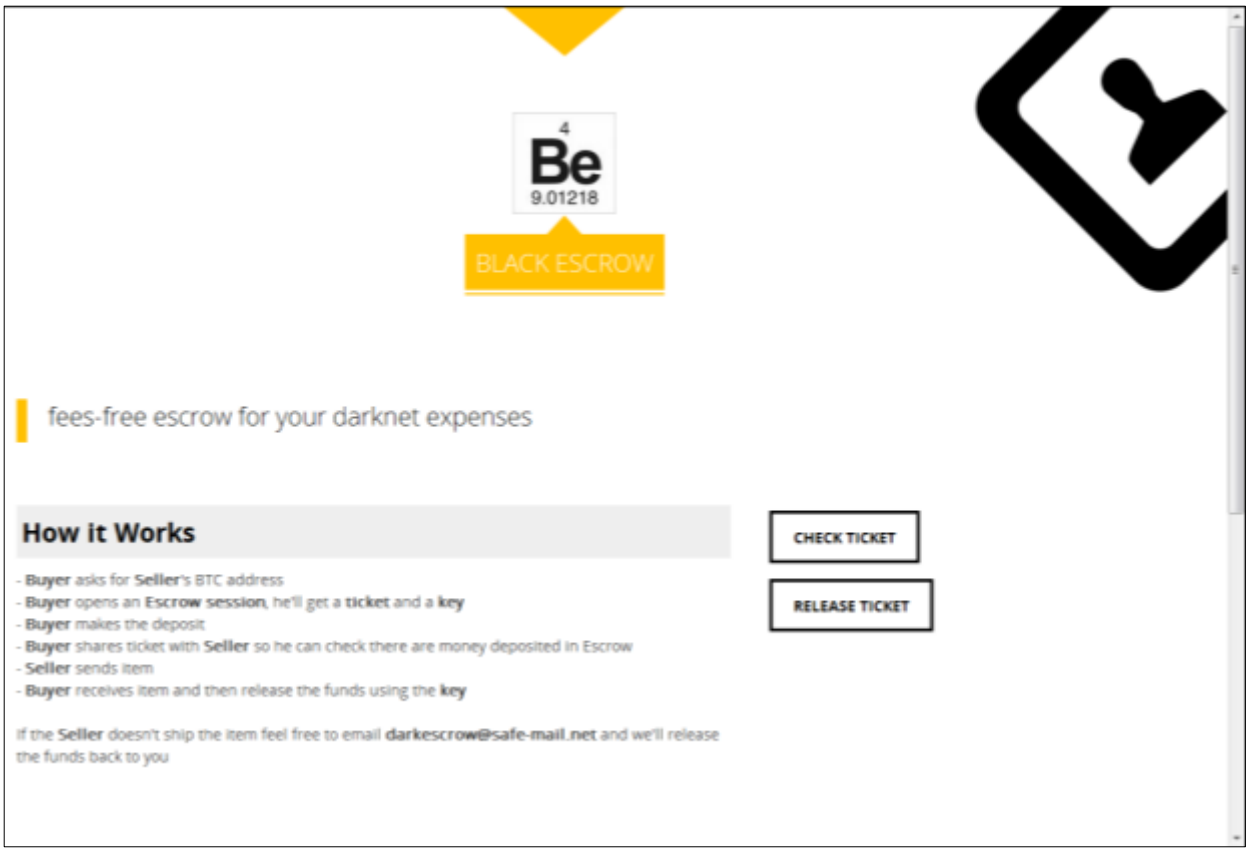


Figure 36: Black Escrow
URL: http://k5wpqksxx76zjmnz.onion/
Description: Bitcoin escrow service for darknet transactions
Date Accessed: September 17, 2014

Narcotics

Figure 37: People's Drugstore
URL: http://newpdsuslmzqazvr.onion/index.php?cat=200
Description: Deals controlled substances
Date Accessed: September 17, 2014

Firearms & Munitions

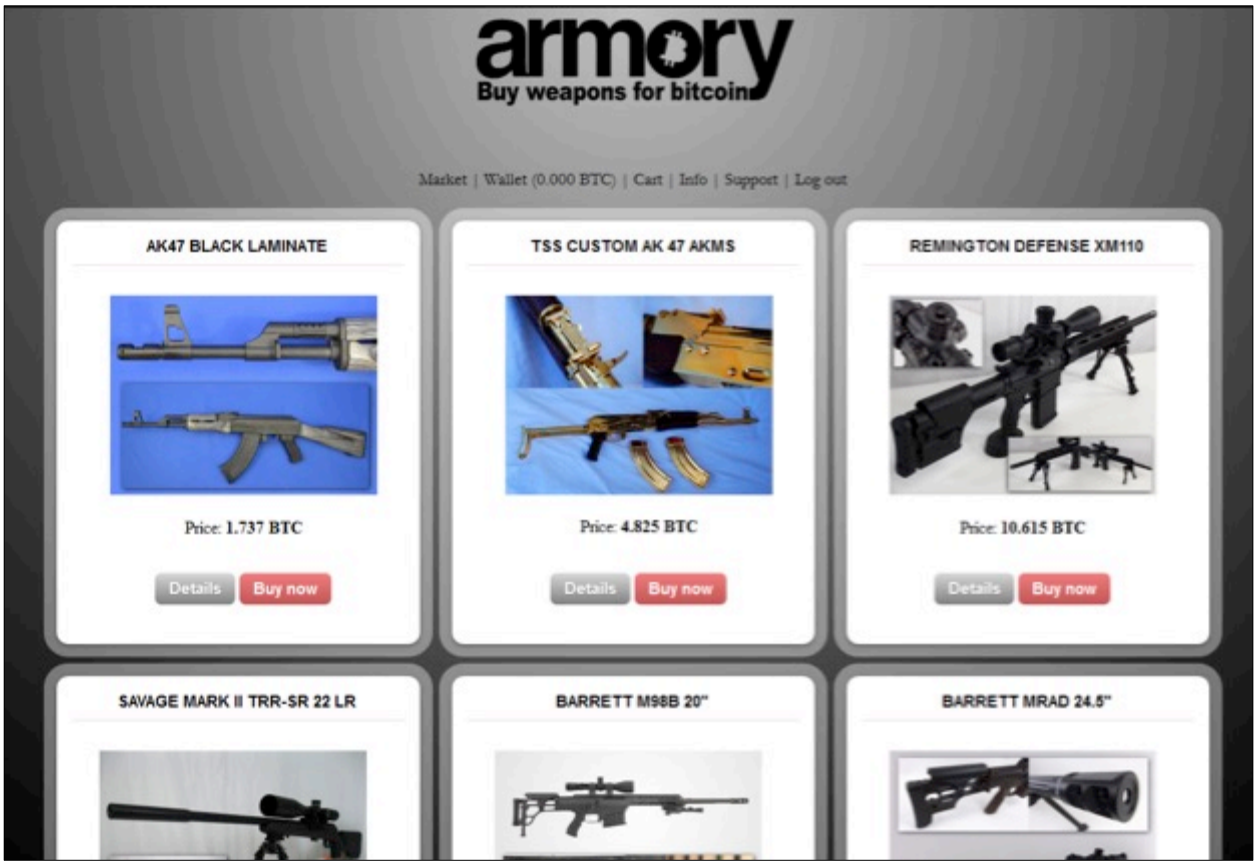


Figure 38: The Armory
URL: http://armoryuqhydqmpro.onion/index.php
Description: Unregistered firearms and ammunition sales
Date Accessed: September 17, 2014

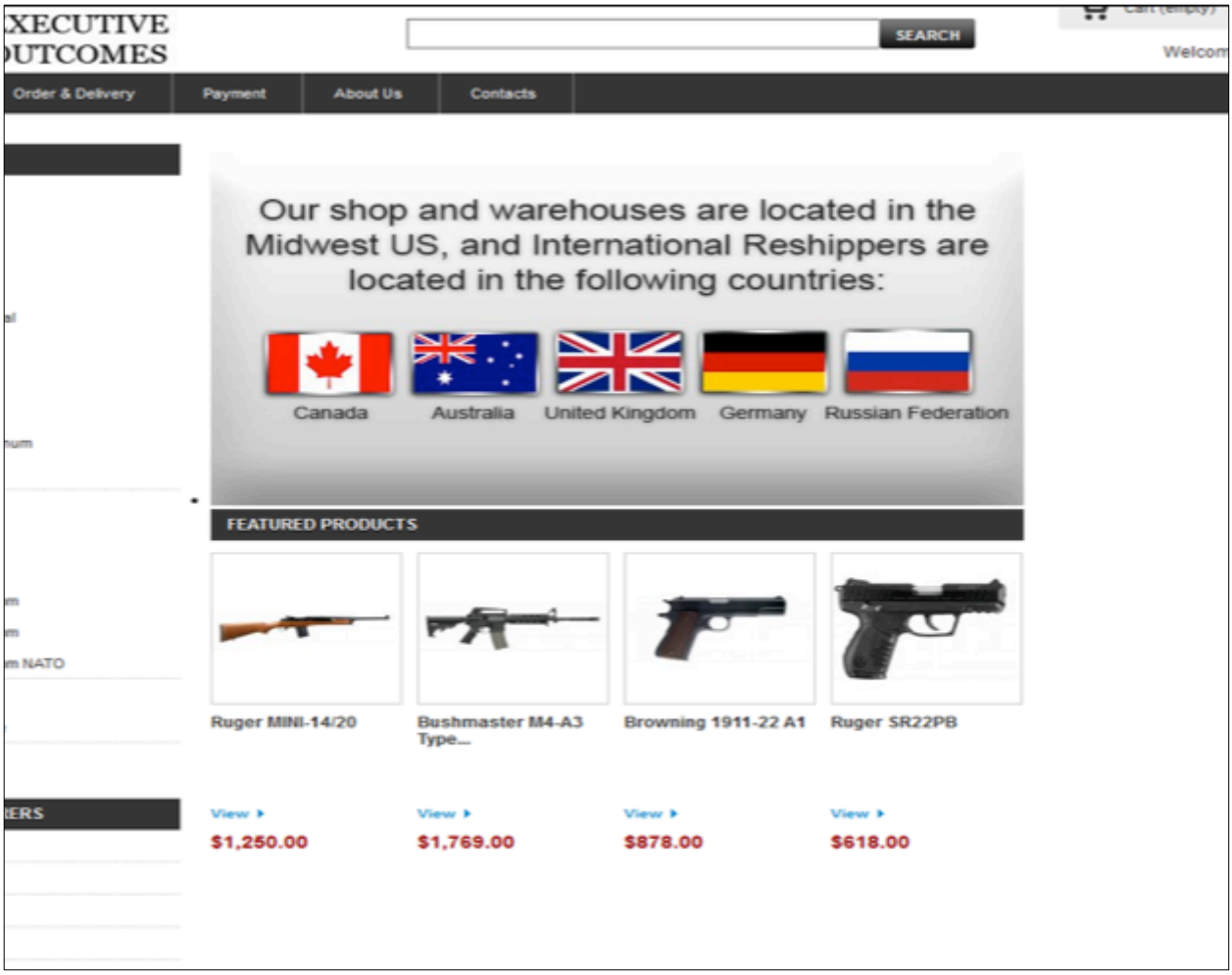


Figure 39: Executive Outcomes
URL: http://5zkfuvtrpotg2nzd.onion/index.php
Description: Unregistered firearms and ammunition sales
Date Accessed: September 17, 2014

Virtual Black Markets

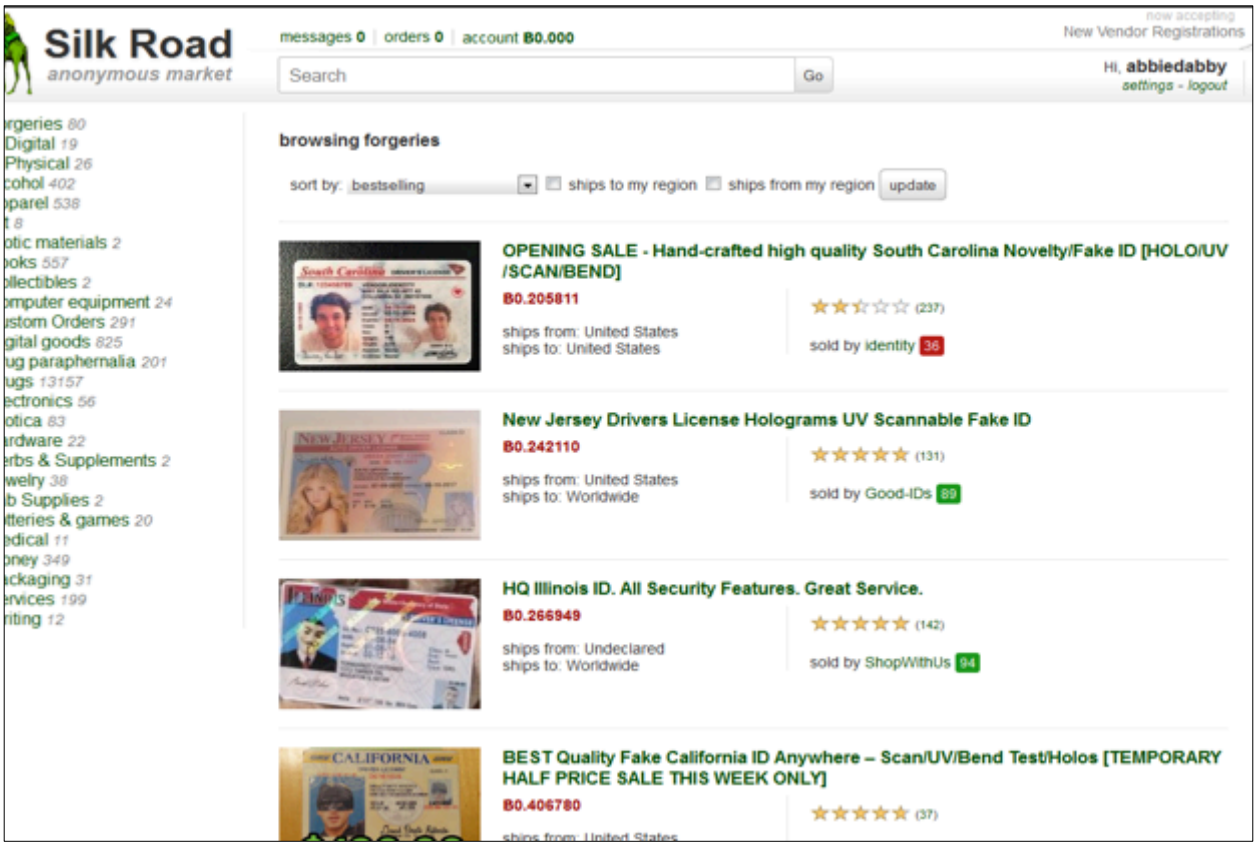


Figure 40: The Silk Road Anonymous Marketplace 2.0
URL: http://silkroad6ownowfk.onion/categories/forgeries/items
Description: Original darknet marketplace offering wide range of goods and services
Date Accessed: September 17, 2014

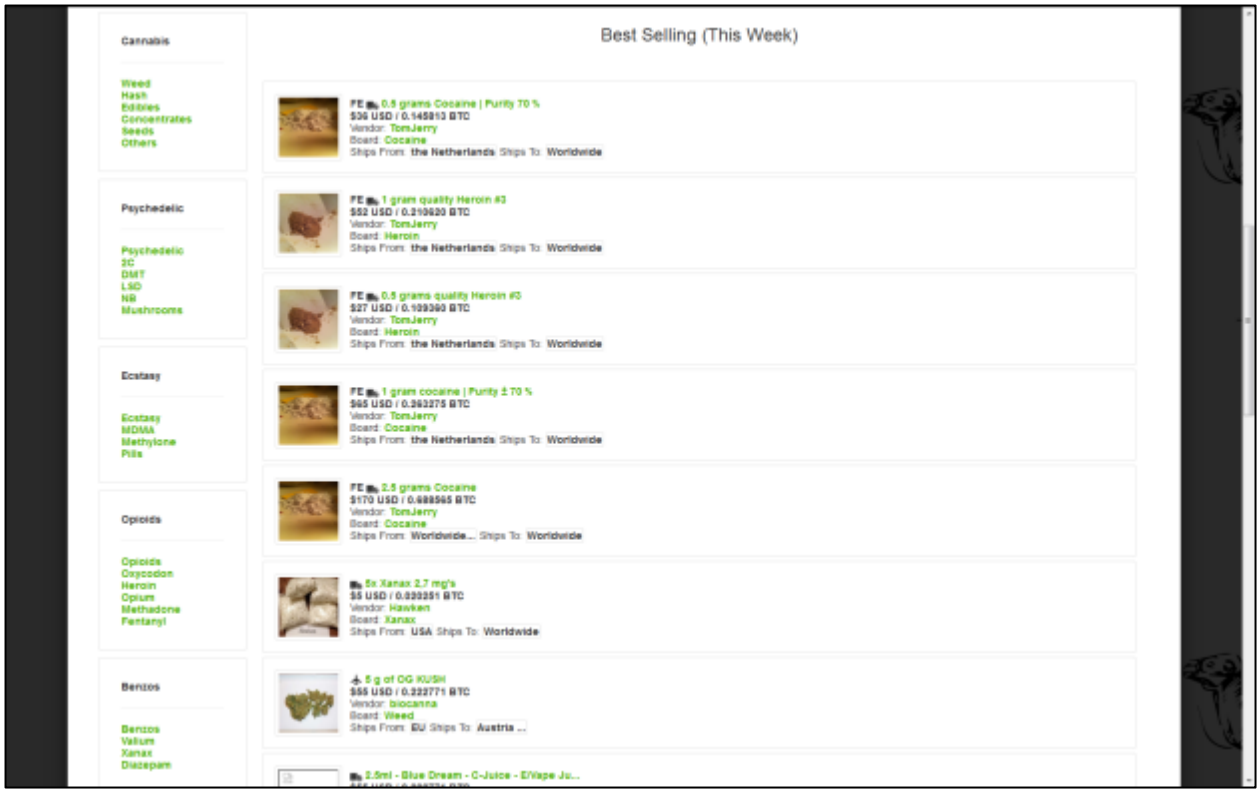


Figure 41: The Silk Road Anonymous Marketplace 3.0
URL: http://reloadedudjtjvxr.onion/road.php
Description: The third inception of the Silk Road (brought online after 2.0 was seized in November of 2014)
Date Accessed: March 27, 2015

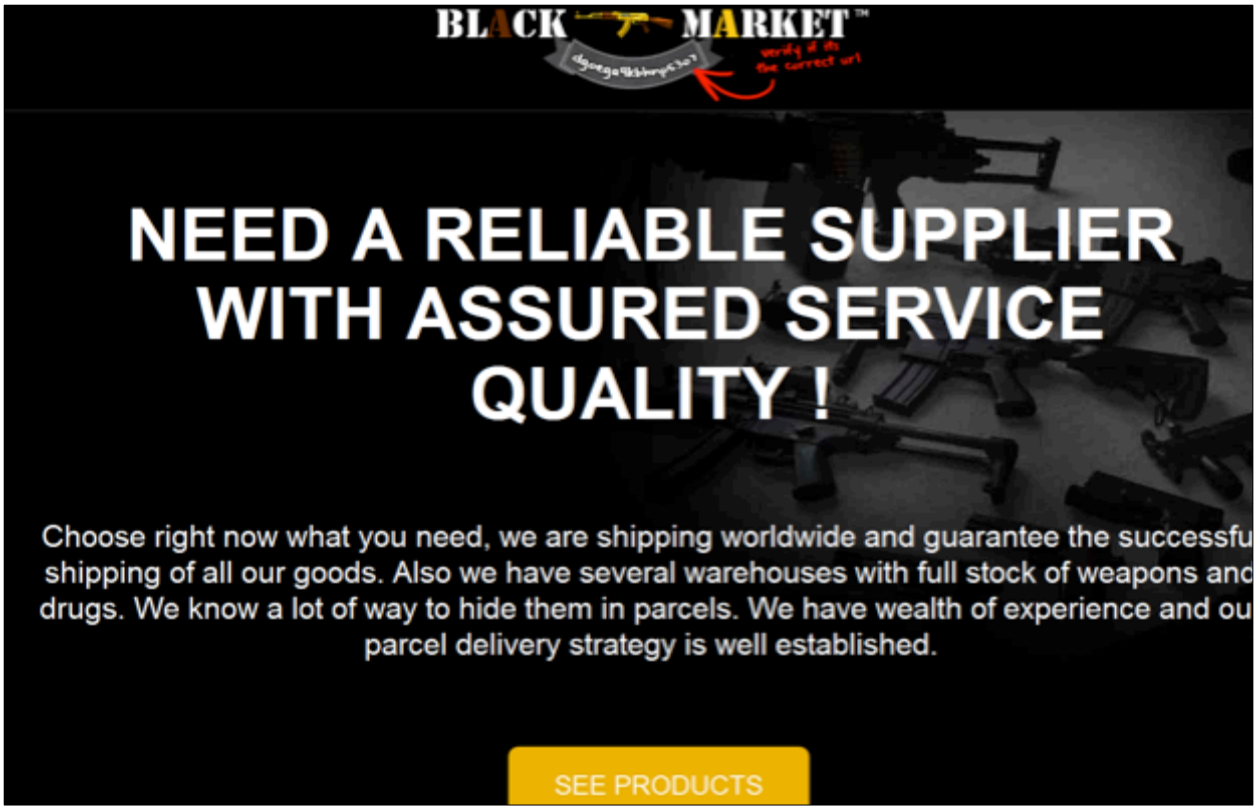


Figure 42: The Black Market
URL: http://dgoega4kbhnp53o7.onion/
Description: Darknet marketplace offering broad range of goods and services
Date Accessed: September 17, 2014

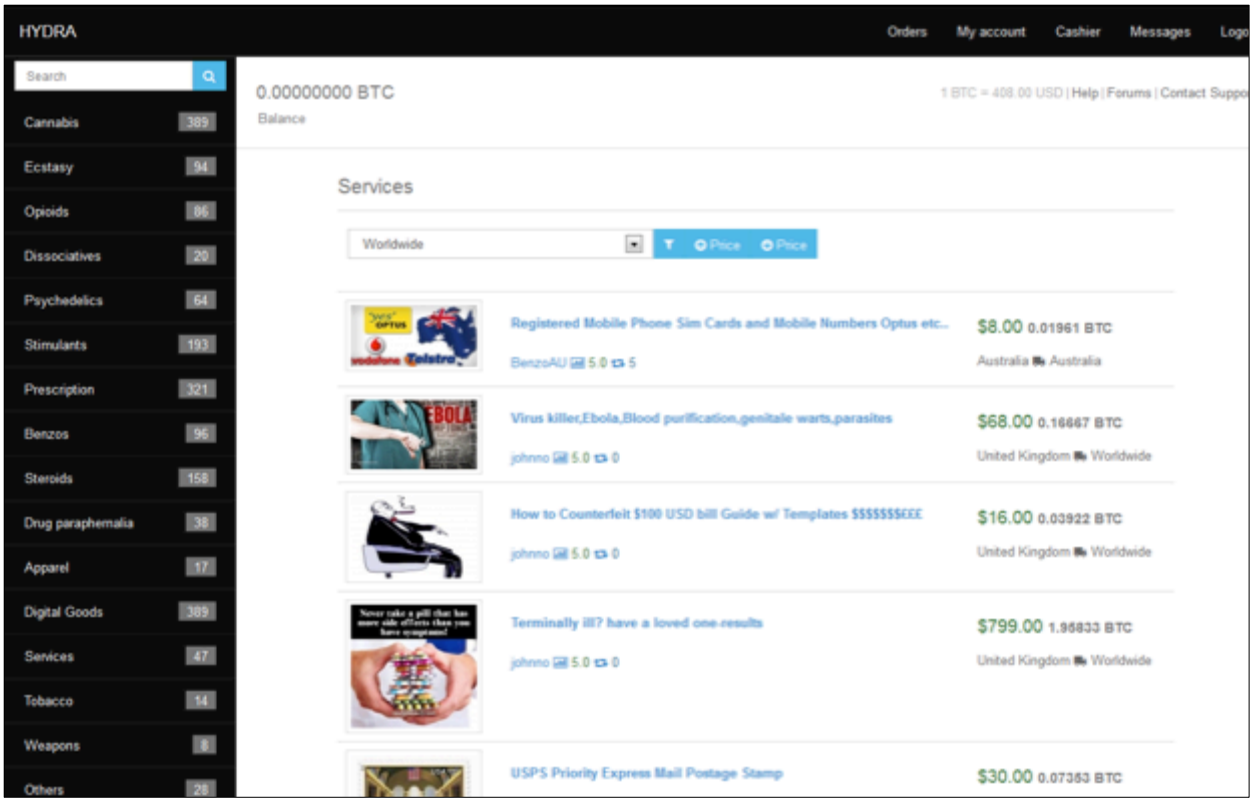


Figure 43: Hydra Marketplace
URL: http://hydrampvvnunildl.onion
Description: Darknet marketplace offering broad range of goods and services
Date Accessed: September 17, 2014

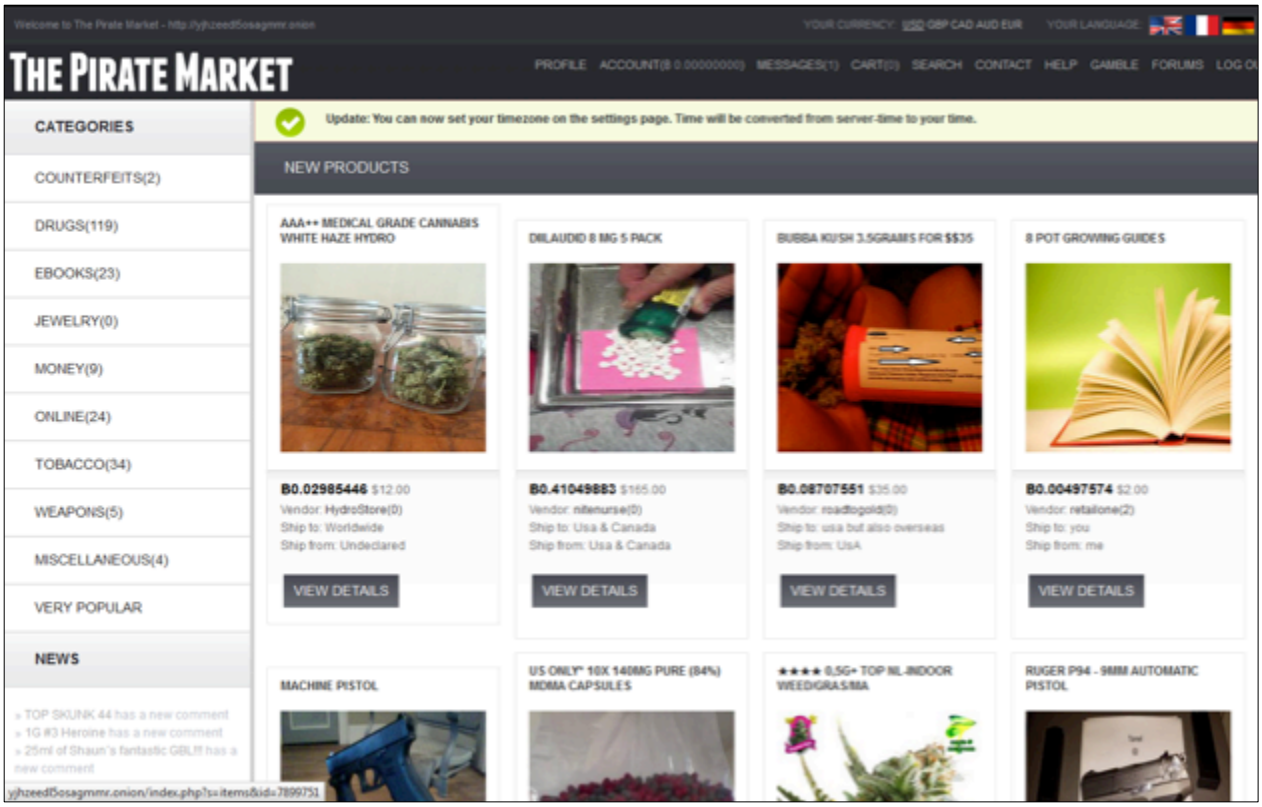


Figure 44: The Pirate Market
URL: http://yjhzeedl5osagmmr.onion/index.php
Description: Darknet marketplace offering broad range of goods and services s
Date Accessed: September 17, 2014