GOVERNMENT ACTIVITIES TO DETECT, DETER AND DISRUPT THREATS ENUMERATING FROM THE DARK WEB

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

NENAD DENIC, MAJOR, SERBIAN ARMED FORCES
B.S.E.E., Military Academy, Belgrade, Republic of Serbia, 2004

Fort Leavenworth, Kansas
2017

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
9-06-2017	Master's Thesis	AUG 2016 – JUNE 2017

4. TITLE AND SUBTITLE

Government Activities to Detect, Deter and Disrupt Threats Enumerating from the Dark Web

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Major Nenad V. Denic

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The surface web has become too risky for terrorist groups. The sites for spreading information about terrorist activities such as fundraising, training and recruiting on surface web can be easily shut down by government authorities. Terrorist forums, propaganda, fundraising sites and recruiting websites have been migrated from surface web to the dark web. However, the activities on the dark web are not easy to shut down. Either way, there is still a possibility to deny, degrade or disrupt illicit user activities.

Government activities to detect, deter and disrupt threats emanating from the dark web are successful. There are several examples of successful operations that happens in past to either shutdown illicit dark web site or to de-anonymize the administrators or users. Those operations were executed with coalition partners or unilaterally.

Government institutions in concert with coalition partners can detect, deter, and disrupt threats emanating from the dark web. By conducting offensive cyber activities across a wide geographical area, the dark web network funding can be reduced and infrastructure along with the hidden services degraded.

15. SUBJECT TERMS
Anonymity, Coalition, Crypto currency, Cyber terrorism, Dark Web, De-anonymization, Hackers, Hidden services, Internet, Surface web, Tor

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	90	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Nenad V. Denic

Thesis Title: Government Activities to Detect, Deter and Disrupt Threats Enumerating from the Dark Web

Approved by:

_____, Thesis Committee Chair
COL Kevin P. Romano, M.M.A.S.

_____, Member
LTC Glenn S. Robertson, Ph.D.

_____, Member
Michael R. Martinez, M.S.

Accepted this 9th day of June 2017 by:

_____, Director, Graduate Degree Programs
Prisco R. Hernandez, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

GOVERNMENT ACTIVITIES TO DETECT, DETER AND DISRUPT THREATS ENUMERATING FROM THE DARK WEB, by MAJ Nenad V. Denic, 90 pages.

The surface web has become too risky for terrorist groups. The sites for spreading information about terrorist activities, fundraising, training and recruiting on the surface web can be easily shut down by government authorities. Terrorist forums, propaganda, fundraising sites and recruiting websites have been migrated from surface web to the dark web. However, the activities on the dark web are not easy to shut down. Either way, there is still a possibility to deny, degrade or disrupt illicit user activities.

Government activities to detect, deter and disrupt threats emanating from the dark web are successful. There are several examples of successful operations that happen in past to either shut down illicit dark website or to de-anonymize the administrators or users. Those operations were executed with coalition partners or unilaterally.

Government institutions in concert with coalition partners can detect, deter, and disrupt threats emanating from the dark web. By conducting offensive cyber activities across a wide geographical area, the dark web network funding can be reduced and infrastructure along with the hidden services degraded.

ACKNOWLEDGMENTS

To my uncle Zoran Denic-Mime (1963-2017)
who helped me to know the causes of things

This thesis would not have been possible without guidance, opinion and advice of my committee members, COL Kevin P. Romano, LTC Glenn S. Robertson, Ph.D., and COL (R) Michael R. Martinez. I would like especially to acknowledge COL (R) Michael R. Martinez who guided me through the whole process and provide extensive support all the time.

I would like to express my appreciation to Staff Group 4B, especially to the Major Marcell Strbich who help me to reframe my thoughts and support me with extensive discussions to check my ideas.

Finally, I would like to thank my wife Jasmina and son Konstantin. Without their support and patience, this thesis will probably exist only in my thoughts.

TABLE OF CONTENTS

Page

ACRONYMS

BTC	Bitcoin
CC	Critical Capabilities
CCA	Caliphate Cyber Army
COG	Center of Gravity
CR	Critical Requirements
CV	Critical Vulnerabilities
DARPA	Defense Advanced Research Projects Agency
DNS	Domain Name System
FSB	Federal Security Service of the Russian Federation [Федеральная служба безопасности Российской Федерации-ФСБ]
FTP	File Transfer Protocol
I2P	Invisible Internet Project
ISHD	Islamic State Hacking Division
ISP	Internet Services Provider
MAC	Media Access Control
MEMEX	Memory and Index
NGO	Non-Government Organizations
NIT	Network Investigative Techniques
NSA	National Security Agency.
ONR	Office of Naval Research
P2P	Point to point
PRISM	Planning Tool for Resource Integration, Synchronization, and Management
RAFT	Relationships, Actors, Functions, and Tensions

SORM	System for Operative Investigative Activities [Система технических средств для обеспечения функций Оперативно Озыскных Мероприятий-СОРМ]
TLS	Transport Layer Security
Tor	The Onion routing
UCC	United Cyber Caliphate
VPN	Virtual Private Network.

ILLUSTRATIONS

Page

TABLES

Page

CHAPTER 1

INTRODUCTION

> Nothing is more creative . . . nor destructive . . . than a brilliant mind with a purpose.
>
> — Dan Brown, Inferno

The Internet, a network of all networks, is supposed to give all clients the same rights and capabilities. However, the Internet has to provide a certain level of security and anonymity to its users. The levels of anonymity and security have decreased in the last decade. The government is establishing more control in the cyber domain in order to increase security in a physical domain.

The average Internet user depends on web search engines. The search engines, such as Google, Baidu, Yandex, Yahoo, and Bing help a user to browse data across the Internet. The search engine's popularity is regionally dependent, but also the search engine depends on the device the user is using at the time. The most popular search engine, according to the Net Market Share[1] is Google with 72.2 percent share for desktops and 94.22 percent for mobile and tablet devices. The philosophy of search engines is as follows. The search engine sends automated robots, called "crawlers" or "spiders", through the Internet to collect as much data as possible. The special program analyzes data and creates a database. The database is based on indexed words for each document the crawlers collect. When a user searches for a term, the search engine uses a

[1] Net Market Share, "Market Share Statistics for Internet Technologies," accessed January 19, 2017, http://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0.

proprietary algorithm to query the database and send information back to the user. The user usually receives information based on the algorithm implemented by the search engine. The majority of websites are friendly to the crawlers or spiders. The site administrators who want to spread information or data from their own websites have an interest that their website data are indexed in search engine databases. Sometimes they optimize sites to be placed in a higher position when a search engine's algorithm sends information to the user. For the average Internet user, the Internet is everything that they can reach through a search engine. Unfortunately, the Internet is bigger than search engines can index. The percentage of the indexed volume of the Internet is estimated at 5 percent.[2] The rest of the un-indexed web is called the deep web, hidden web, or invisible web. The 5 percent estimation is based on overall Internet traffic. A part of the deep web is the dark web, see figure 1. More about the dark web is following.

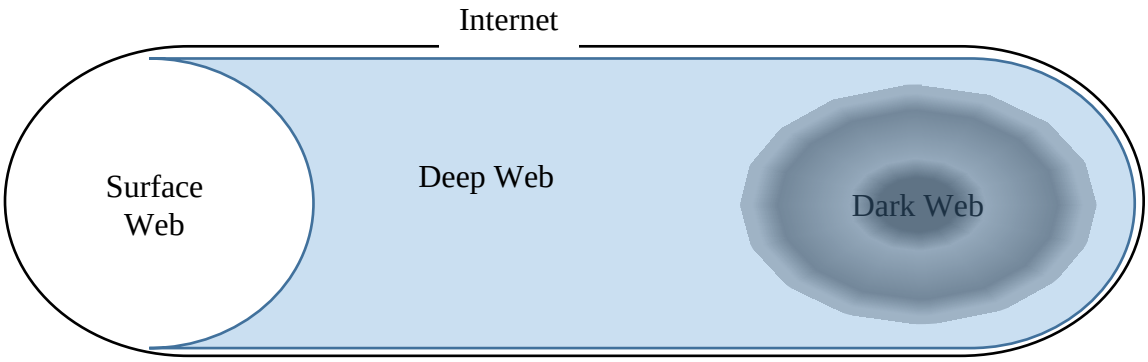


Figure 1. Internet partition

Source: Created by the author.

[2] CBS News, "New Search Engine Exposes the Dark Web," February 8, 2015, accessed October 17, 2016, http://www.cbsnews.com/news/new-search-engine-exposes-the-dark-web/.

At the beginning of the networking era in 1969, four computers were connected. In 1991, the World Wide Web consisted of hundreds of websites, and it was very easy to index them. Users were able easily to access the information they were seeking for. With the expansion of the Internet, the situation has become more complicated. Conventional search engines were able to get data from a static web page, but they become inefficient when they tray to index a dynamic web page. The static web page is linked only to one location on the Internet and data on this page is changed from time to time. On the other hand, the dynamic web pages are more complex. The skeleton of the page is something what is constant, but data on the page is retrieved in accordance with the user request. The dynamic pages are created by user request and obtain data from a connected source, usually a database. The dynamic pages started to grow and the un-indexed space between visible and invisible web has started to grow. In 1994 the phrase "invisible web" is introduced. The phrase referred to information that was invisible to conventional search engines used in that particular time period.[3]

The phrase "invisible web" was used until 2001 when Mihcael K. Bergman in his research paper "The deep web: Surfacing Hidden Value." introduced new term "deep web".[4] The opposition of the "deep web" become "surface web" what was previously referred on "visible web". The term "invisible web" has referred only to web pages that are not indexed by search engines.

---

[3] Michael K. Bergman, "White Paper: The Deep Web: Surfacing Hidden Value," *Journal of Electronic Publishing* 7, no. 1 (August 2001), accessed October 10, 2016, http://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main.

[4] Ibid.

The deep web does not represent only sites that cannot be accessed directly through conventional search engines. The deep web also represents content on the Internet which is:

1. Inaccessible to current conventional search engines
2. Accessible only for targeted queries or keywords
3. Protected from search engines crawlers
4. Protected by security mechanisms (login ID, password)
5. Protected by logical or encrypted structure which is inaccessible from outside

Table 1. Internet status in one second

Occurrence	Number-amount
Tweets sent	7,380
Instagram photos uploaded	747
Tumblr posts	1,169
Skype calls	2,313
GB of Internet traffic	38,851
Google searches	56,789
YouTube videos viewed	133,507
Emails sent	2,532,335

Source: The Internet Live Status, "In 1 Second, each and Every Second, There are. . . , accessed October 18, 2016, http://www.internetlivestats.com/one-second/.

The search engines beyond the year 2000 were capable of obtaining information from databases of dynamic web pages. The Bergman research estimates that the size of the deep web is 500 times greater than surface web. The percentage of surface services vary between 0.25 to 5 percent of the whole web. The estimation of surface web size based on internet live status and the amount of events that occurred in one second are

presented in table 1. The number of current Internet users is 3,481,124,022 which makes the Internet the most populated multinational shared domain. [5]

In order to protect their own national interests, countries are trying to establish legislation for the Internet and control of data flow under boundaries of their territory and beyond. The control has been established around the globe.

The government of Russia has established control on all electronic communication since 1996.[6] The System for Operative Investigative Activities [*Система технических средств для обеспечения функций Оперативно-Озыскных Мероприятий-СОРМ]*-(SORM) is a system that all service providers must implement. The SORM is a set of equipment that allows the Federal Security Service of the Russian Federation [*Федеральная служба безопасности Российской Федерации-ФСБ*]-(FSB) to duplicate traffic from communication equipment or to provide access to the email servers and copy data. Three legislative acts have passed in the last two decades to support FSB activities in three areas:[7]

1. SORM-1: surveillance of wireline and mobile communications
2. SORM-2: monitoring Internet communications

---

[5] The Internet Live Status, "Internet Users in the World," accessed October 18, 2016, http://www.internetlivestats.com/watch/internet-users/.

[6] Andrew Blake, "Russia Weighs Letting Telecoms Use Govt. Surveillance System for New Anti-Terror Law: Reports," *Washington Times*, August 10, 2016, accessed October 11, 2016, http://www.washingtontimes.com/news/2016/aug/10/russia-weighs-letting-telecoms-use-ex-kgbs-surveil/.

[7] Andrei Soldatov and Irina Borogan, "Russia's Surveillance State," *World Policy Journal* (Fall 2013), accessed October 11, 2016, http://www.worldpolicy.org/journal/fall2013/Russia-surveillance.

3. SORM-3: collecting all communications from all media and storing it for up to three years

The US government in the same period of time did similar activities. The National Security Agency (NSA) implemented the Planning Tool for Resource Integration, Synchronization, and Management (PRISM) to collect data from the US service providers. Prior to that, the Upstream program was used for tapping international cables that were crossing US territory.[8] To protect their own privacy, many people around the world started to seek for new services that can grant them a certain level of privacy and security.

The gateway from the totally controlled environment online is in the deep web. The surface web users are protecting themselves with applications that are created to protect privacy. The exploitation of the anonymity software started to grow with the rise of the awareness that control exists. At the beginning, anonymity started with simply Virtual Private Network (VPN), and Proxy, later programs followed that were created only to protect anonymity. The Freedom Network from Zero-Knowledge System, Inc. was the most common anonymous network that exists from 1999 to late 2001. The Freedom Network was a commercial service which depended mostly on users who were willing to pay for service.

Another project to protect security and anonymity was the Onion routing (Tor). The project started with initial release on September 20, 2002. What is Tor? Tor is

[8] Washington Post, "NSA Slides Explain the PRISM Data-Collection Program," July 10, 2013, accessed October 17, 2016, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

routing protocol that provides anonymous routing from end to end. Anonymous routing means that observers, network operators, or government officials are not able to find the origin or destination of information. Tor's main power are volunteers who support the project. Volunteers run relays and when they run relays, they actually donate their own bandwidth to the network. The network that is originally developed with the United States Navy has grown and users of Tor are:[9]

1. People who seek to protect their privacy
2. Journalists and their audience
3. Law enforcement officers
4. Activists and Whistleblowers
5. High and low profile people
6. Business executives
7. Bloggers
8. Militaries
9. IT Professionals

The official Tor website does not indeed mention who else are the users of the anonymity service. The advantages of hidden services and anonymity from end to end are tempting for people who do not care about legality, ethics, and human prosperity. Followed by censorship on the surface web they started to use hidden services to propagate diversity of illicit material and services. A portion of the deep web is hidden under secret web links and provides uncensored adult content, immoral forums, chats,

[9] Tor Project, "Who uses Tor," accessed October 18, 2016, https://www.tor project.org/about/torusers.html.en.

online material for terrorist training and recruiting, fundraising for illicit activities, human trafficking, and the black market. This illicit part of the deep web is referred to as the dark web. The dark web can be defined as a portion of the deep web which contains generally illegal and anti-social information and can be accessed either through conventional browsers or specialized browsers for accessing the secretive web links.[10]

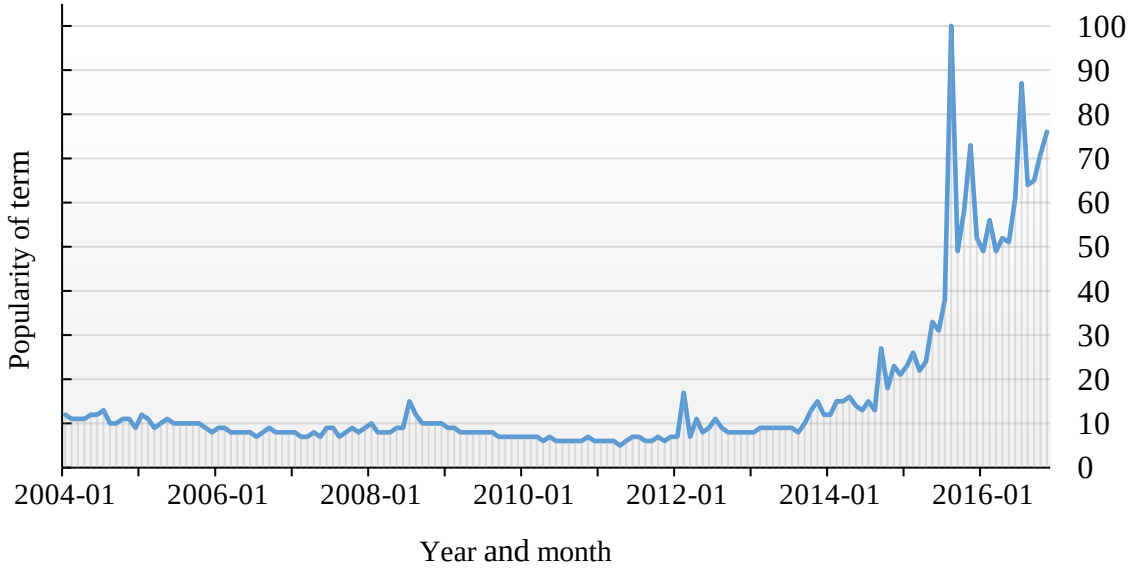


Figure 2. Global interests on term "dark web" over the time on Google

Source: Created by author, data from Google Trends, accessed November 10, 2016, www.google.com/trends.

The number of dark web users is unknown, but figure 2 represents a number of search requests for the term "dark web" on Google search engine.

[10] E. Dilipraj, "Terror in the Deep and Dark Web," *Air Power Journal* 9, no. 3 (2014: 121-140.

On figure 2 global interest on term “dark web” is presented. A value of 100 is the peak popularity of the term. A value of 50 means that the term is half as popular. Likewise, a score of 0 means the term was less than 1 percent as popular as the peak.

Problem statement

The surface web has become too risky for terrorist groups. The websites for spreading information about activities, fundraising, terrorist training and recruiting can be easily shut down by government authorities. However, the online services on the dark web are not easy to shut down. Either way, there is still a possibility to detect, deter or disrupt illicit activities on the dark web. Terrorist forums, propaganda and recruiting websites, fundraising websites have been migrated from the surface web to the dark web. At this point, there is a necessity to conclude that the dark web services are all illegal and antisocial services used in order to degrade human prosperity. Tor network, besides offering legal anonymity, services is an infrastructure for illicit online services which are part of the dark web.

The dark web is considered an ideal ecosystem for Islamic State in Iraq and the Levant-ISIL’s activities.[11] Since the November 2015 attack in Paris, ISIL has spread propaganda using hidden services on the dark web. There are three main reasons for terrorist migration from the surface web to the dark web.

First, they want to avoid censorship of their sites on the surface web.

[11] Beatrice Berton, “The Dark Side of the Web: ISIL’s One-Stop Shop?” European Union Institute for Security Studies (EUISS), June 26, 2015, accessed October 20, 2016, http://www.iss.europa.eu/publications/detail/article/the-dark-side-of-the-web-isils-one-stop-shop/.

Second, sites on the dark web permit access of the content to all users who know the URL, and simultaneously protects the identity of supporters to freely express support or to pull data from the site.

Finally, the content on the dark web is protected from hacktivists. The Paris attack in November 2015 has triggered hacker collective Anonymous to run Operation Paris[12] to take down hundreds of websites associated with ISIL. Terrorist migrated online services from the surface to the dark web. The URLs of hidden service on the dark web are spread by terrorists with Telegram application using an encrypted channel. The message is available only for ISIL followers who are registered on some of the channels.

The more important reasons why the terrorist organizations are using the dark web are fundraising, traceless money transferring, and the black market. They merge anonymous routing with the anonymous transaction. Virtual cryptocurrencies like Bitcoin are the digital equivalent of cash. It is very hard to trace cryptocurrency's transactions because there is not the intermediate (bank) as a third governmental party obligated to give information to the investigators.

For example, the "Found the Islamic Struggle without Leaving a Trace" is a web page on the dark web for Jihad donors using Bitcoins.[13] However, the black market on the dark web is crowded with drug, arms, weapons, ammunitions, fake IDs, skimmed

[12] Andrew Blake, "#OpISIS and #OpParis: Anonymous Hacktivists to Retaliate against ISIS after Paris Attacks," *Washington Times*, November 16, 2016, accessed October 20, 2016, http://www.washingtontimes.com/news/2015/nov/16/opisis-and-opparis-anonymous-hacktivists-to-retali/.

[13] Gabriel Weimann, "Terrorist Migration to the Dark Web," Perspectives on Terrorism, June 2016, accessed October 20, 2016, http://www.terrorismanalysts.com/pt/index.php/pot/article/view/513/html.

credit card details, banned books, etc. The black market is online services that can provide logistic support for terrorists, especially for “lone wolves”.

Another example of how terrorists utilize the dark web services is fundraising in Indonesia. A Jihadist group despite that they organized fundraising on the dark web, they used stolen identity from the dark web on the Forex trading website. The terrorist group committed a series of cyber crimes and collected US$600,000.[14]

The Silk Road, an illegal trade website, is an example of a profitable business. Similar to the surface selling web website, the Silk Road site offered a variety of illegal goods and served as a grant for the customer transaction. The customer ordered illegal goods from the website located on the dark web and paid in Bitcoins. The money stays on the site wallet until the customer receives the goods. When a customer receives goods, the Silk Road transfers the Bitcoins to the seller’s wallet, and the site had taken commission rate between 8 to 15 percent for its services. The FBI estimated that the Silk Road marketplace had 150,000 anonymous customers and 4,000 vendors. The value of completed transaction on the site is estimated at more than US$1.2 billion by July 2013 when the site was uncovered.[15] It can be assumed that a share of profit ended up in terrorist hands.

---

[14] Ibid.

[15] Daniel Sui, James Caverlee, and Dakota Rudesill, *The Deep Web and Darknet:A Look inside the Internet's Massive Black Box* (Washington, DC: Woodrow Wilson International Center for Scholars, August 2015).

Research Question

The central question this thesis addresses is: How can the government detect, deter, and disrupt threats emanating from the dark web? To answer this, the following secondary questions are considered:

1. What is the technical aspect of the dark web network-The onion routing?
2. What is the significance of Tor network?
3. How do safe and secure transactions occur on the dark web, and are they really secure?
4. Which sites are used for illicit activities and are they active now?
5. How can the dark web be exploited and who can exploit its medium?
6. What ways and means exist to influence the dark web?

Limitations

The primary limitation of this research is a lack of unclassified literature, and willingness of current cyber operators to discuss the topic. The discussion on any government future steps is classified and not possible without security clearance. The majority of resources for research are articles, reports, and documentation from the Internet (either surface or deep web). The aging of technologies and events narrows the frame of literature. With fast technology development and changes in the Internet policy, only literature from 2011 to 2017 year are considered for research.

CHAPTER 2

LITERATURE REVIEW

The purpose of this chapter is to describe technologies and techniques used to obtain anonymity on the Internet and to illustrate some of the successful examples of the de-anonymization activities conducted by government organizations to suppress illicit activities on the dark web. In this chapter, the basic terrorist activities in cyberspace are described with an emphasis on activities conducted with the exploitation of the services from the dark web. Anonymous cryptocurrency exchange is also explained. As previously stated, the anonymity of the dark web allows people to protect their privacy. Although used by whistleblowers, human rights activists and dissidents, the dark web is primarily used by people such as weapons dealers, terrorist and drug dealers who are conducting illicit activities.

The Internet connection is packet-based communication between entities. The two basic types of communications on the Internet are client-to-client and client-to-server. The data packet for each communication sent either by client or server consists of the data payload and the header. For successful communication between entities, every communication packet in the header carries information about the origin of data and destination of data. The nodes responsible for routing (redirecting) the packets have information of the entire network. Each node has access to the packet and obtains the data of origin and destination of the packet in order to execute proper routing. That information is also available to the administrator responsible for nodes. For instance, if Person A is on vacation in the hotel and he is accessing the web on a daily basis on his private company site, the hotel's network administrator may obtain information that

Person A is accessing the site of Company C. This simple example is deliberately used. The problem becomes more serious if Person A is a government employee in a foreign country. Even if Person A is using encrypted communication link with the company server, the information of the packet destination is still available for the hotel's network administrator. The solution to hide routing data from intruders is based on the anonymous routing. The anonymous routing is a technique where routing devices do not have information on the destination of the received packet. The routing devices know only the next instance of the packet.

Beginning of The onion routing

The Onion routing (Tor) research started in late 1995 with the initial goal to separate identification from routing.[16] At the beginning, the research was funded and conducted within the Office of Naval Research (ONR). However, in 1997 the Onion routing was funded by Defense Advanced Research Projects Agency (DARPA) under the High Confidence Networks Program.[17] In 2003 the online Tor project had a public release. In Spring 2004, the hidden wiki site was set up after ONR released the code for Tor under free licensing. Tor network started as a network of volunteers who set up nodes to increase privacy on the Internet. Volunteers did not only run relays in the network, they also helped to improve network capabilities. Volunteers continue to develop and readjust code, spread information about the network around the world, and they are

[16] Paul Syverson, "A Peel of Onion," *ACSAC'11* (December 5-9, 2011): 123-135.

[17] Onion Routing "Brief Selected History," accessed December 24, 2016, https://www.onion-router.net/History.html.

translating documentation on other languages to make network much more accessible to users from different regions.

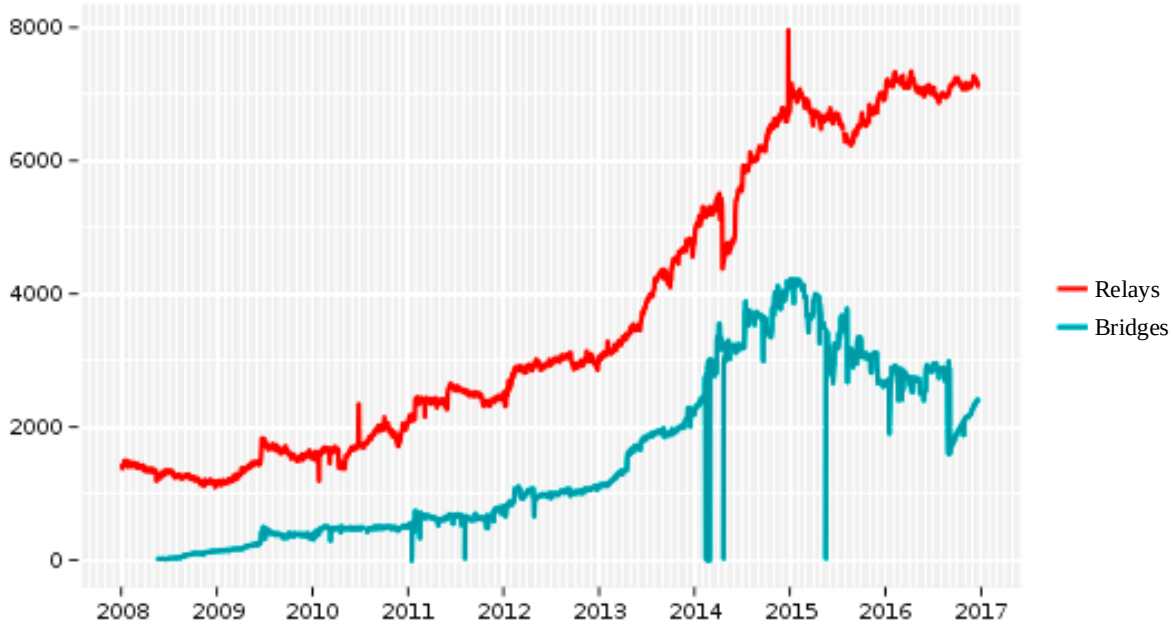


Figure 3. Number of running relays and bridges in Tor network

Source: Tor Project, "Tor metrics—Relays and Bridges in the Network," accessed December 25, 2016, https://metrics.torproject.org/networksize.html?start=2008-01-01&end=2016-12-25.

The network nodes are relays and bridges that route the packets. The communication in Tor network can be divided as:

1. client-to-client communication within the network
2. client-to-surface service
3. client-to-hidden services

According to the Tor website,[18] the nodes in network, relays, and bridges are defined as follows:

Relay: a publicly-listed node in the Tor network that forwards traffic on behalf of clients, and that registers itself with the directory authorities.

Bridge: a relay whose existence is non-public and which can, therefore, provide access for blocked clients, often in combination with pluggable transports, which registers itself with the bridge authority.

The number of bridges and relays on Tor network is presented in figure 3. This number has fluctuated in 2016 to around 7000 relays and 2000 bridges. Compared with the size of the Internet, the number of relays is about 10 times lower than numbers of autonomous systems on the Internet.[19] Besides the numbers of routing nodes in Tor network, the bandwidth of links between nodes significantly influences the network performance. The bandwidth depends on volunteers' willingness and capabilities to donate a certain amount of bandwidth to the network.

The Onion routing

The basis of Tor lays on cryptology and anonymous routing protocol. The anonymous routing protocol represents a way of routing where a packet's redirection is happening in an unpredictable way. The network has a variety of paths through which information can flow. Unlike the surface web, where a packet's flow depends on routing

[18] Tor Project, "Tor Metrices-About," accessed December 24, 2016, https://metrics.torproject.org/about.html.

[19] CIDR Report, "General Status," December 25, 2016, accessed December 25, 2016, http://www.cidr-report.org/as2.0/#General_Status.

protocol, and the decision for routing is made in accordance with cost, a number of hops, speed (bandwidth), the Tor's relays create paths "pseudo-randomly". Although the path is created "pseudo-randomly", there are specific control measures to prevent path creation from compromising the anonymity of client or service. The confidentiality of information is another advantage of Tor. The confidentiality is based on the implementation of two well-known cryptography systems: symmetric-key and asymmetric-key.

The symmetric-key cryptography is a crypto technique that most people consider as cryptology when talking about cryptography. The key used for encrypting and decrypting is a shared key, and both entities that communicate need to have the same key. This type of cryptography has advantages and disadvantages. The disadvantage of the symmetric-key cryptology is that the key has to be shared between two entities who want to communicate secretly. Sharing and protecting the key is generally difficult, especially if the distance between the communicating entities is long. The planner who directs the sharing of the key has to know the entities who needs to communicate. On the Internet, it is hard to predict which entities are going to communicate secretly. On the other hand, redistribution of the key to all entities is expensive and can break a complete system of cryptology if the key of one entity is uncovered and the other network entity does not have the information about it. However, the advantage of the symmetric-key is real-time crypto-communication. The processor burden necessary to encrypt and decrypt the information is at an acceptable level. There is less processor burden needed to decrypt a cryptogram encrypted with symmetric-key than to decrypt cryptogram with asymmetric-key. The illustration of symmetric key crypto-communication is the following: The entities use the same symmetric key for encryption and decryption. The first entity is

encrypting information with the key and then sends the cryptogram across the network. The second entity, who receives the cryptogram, uses the key to decrypt information.

Asymmetric-key or public-key crypto technique is different than symmetric-key cryptography. Each of the entities possesses two types of keys. The public and the private key are generated by an entity who initiates communication. The public key is advertised to everyone and besides the entity who need the key, other entities also know the key and so does the adversary.

The illustration of asymmetric key crypto-communication is the following: The first entity creates the private and the public key and advertises only the public-key to all entities. Public and private keys are correlated and interdependent. Communication starts when the second entity in the communication receives the public-key. The second entity then encrypts the information with the public key and sends a cryptogram to the first entity. An encryption algorithm is made so that the encrypted information can be decrypted only with the private key, and as previously mentioned, both private and public key are interdependent. The private key is known only to the first entity. It is not possible to make decryption again with the public key. The advantage of this cryptographic technique is sharing of the key between entities prior to the beginning of the encrypted information exchange. Sharing the key prior to communication allows communication between any node on the Internet. However, a necessary processor burden to decrypt a cryptogram is much larger than for symmetric-key decryption. As the payload of the information increases, the processor burden increases drastically. A high processor burden is a disadvantage of asymmetric key cryptology over symmetric key cryptology.

Tor network communication is encrypted between entities. This means that it does not matter if the communication is between client and network nodes, or if the communication is between service and network node both are protected. Tor encryption is a hybrid form of symmetric and asymmetric cryptology techniques. At the beginning of the communication, the asymmetric-key algorithm is used to distribute the symmetric-key to the entity that needs to communicate. The communication route, so-called "the circuit", is created in an unpredictable way across the network relays. The key is distributed between relays. All relay communication within the network is encrypted. The circuit is created by specific criteria defined for path selection. The path selection criteria allow choosing a route which provides a certain level of security against the adversary who can try to break network integrity running a relay or observing traffic.

When the route is defined, the next step is to create a circuit. The circuit is an encrypted path established between clients and relays in the network in order to make a condition for anonymous routing. The third generation of the Onion routing defines fixed-length circuit and this is three hop circuit route. The main entity in the network who distributes information about network status and network membership information is the directory server.[20] The directory servers are trusted and redundant servers set up under the Tor project. A client with installed Tor proxy access to the directory server can download the information about the network status. The client is using network status information and path selection criteria to build circuits. When a client software defines nodes which will be used in circuit building, the three step process can begin.

[20] Syverson, 123-135.

The first step in the process is to create a circuit between the user proxy and selected entry node (EN) in the network. Because there is not any encryption between the entry node and Tor proxy, to protect communication the Tor proxy exchange with entry node Transport Layer Security (TLS) key. The TLS key is acting as an overarching communication method. Then Tor proxy establishes node to node key. Communication between client and entry node circuit is created with two-way interaction. The interaction starts with the command “create circuit”. This command is sent to the entry node and then the entry node responds “circuit created”. When a circuit is created then the session key is established for this circuit. On figure 4, the circuit is represented as an ethereal layer between the Tor proxy and EN.

The next step is extending the circuit to the middle node (MN). Tor proxy is responsible for choosing all nodes in the circuit using data downloaded from the directory server. The TLS communication between nodes inside Tor network is already established because the nodes inside the network keep the TLS connection between each other. The Tor proxy sends a message to the entry node with instructions to extend the circuit. When the entry node receives encrypted instruction, from Tor proxy, it starts to decrypt. The node decrypts the instruction using session 1 key and acts in accordance with received instruction. The entry node sends instruction “create circuit” to the middle node. The middle node responds “circuit created” to the entry node. When the entry node receives a message it encrypts with session 1 key and sends to Tor proxy indicating that the circuit has been extended. The message sent to the Tor proxy has a session 2 key, which is the session key between the middle node and proxy. On figure 4 the circuit is represented as a circuit between the Tor proxy and middle node.

At the end, the Tor proxy is choosing exit node (EX). The exit node is chosen according to the availability and rules to choose exit node. The Tor proxy sends a relay request to the entry node. The entry node decrypts a relay request with the session 1 key and finds another relay request. The entry node sends the relay request to the middle node. The middle node decrypts the relay request and finds the message “create circuit” specifying exit node. When the exit node creates the circuit with middle node then EX sends back to the proxy session 3 key and the “circuit created” information. The data from exit node back to the Tor proxy is encrypted with an extra layer of encryption. There is the first layer from EX node then the second layer is from MN, and the final layer is from EN. At the opposite direction the proxy creates a layered cryptogram and then each node peels one layer of information before passing the cryptogram to another node. On figure 4 the circuit is represented as a circuit between the Tor proxy and EN.

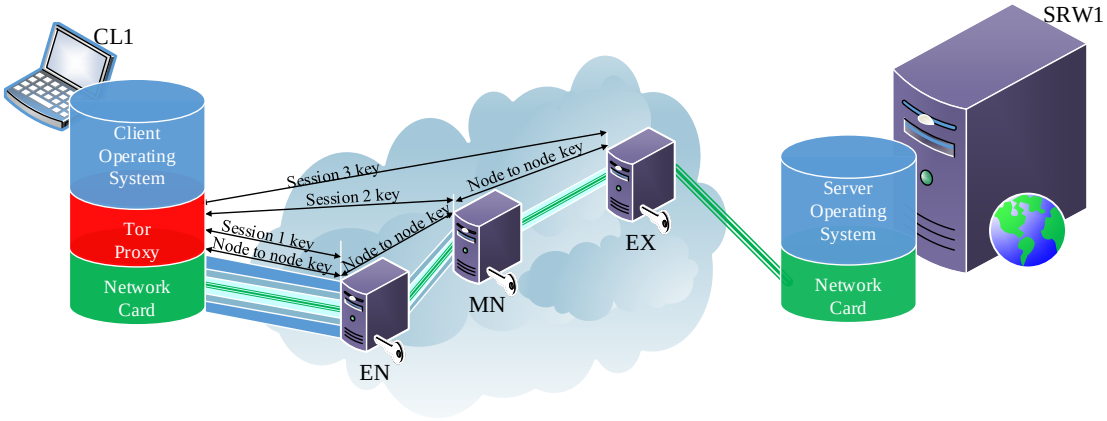


Figure 4. Browsing request trough Tor proxy

Source: Created by the author.

To put it briefly, the following example explains how communication takes place. When the client CL1, shown in figure 4, wants to browse information on server SRW1, the CL1 browsing request is sent through the Tor proxy to the entry node. The request is layered encryption. The entry node will decrypt the first layer of the cryptogram with the session 1 key, obtain the MN IP address and using the EN IP address as source, sends the cryptogram to middle node MN. The MN will decrypt the second layer of the cryptogram, obtain the EX IP address and using the MN IP address as a source, send cryptogram to the EX. The EX will decrypt the third layer of cryptogram, and find the destination IP address and send a request to the web server SRW1 using EX IP address as an origin of information. The SRV1 will return data to the EX, the EX will encrypt information with the session 3 key and send to the MN. The MN will encrypt information with the session 2 key and send back to the EN. The EN will repeat the procedure. The received cryptogram at the Tor proxy has three layers of encryption. The proxy server decrypts all layers with the specific session key and then sends information to the browser to be presented to the client. The example on figure 4 presents communication between a client who is accessing from a Tor network to the service on the surface web.

The routing information that the nodes in Tor network have are IP address of next hop and IP address of the neighboring source in the circuit. The nodes in Tor network do not have information about origin and destination, as is the case with surface web nodes. In Tor network, the anonymous routing is achieved with circuits and layered encryption. The onion routing hides the IP address of origin or the IP address of packet destination or both. For example, if eavesdropping is conducted at the entry node, the IP address of origin may be extracted but not IP address of destination. If eavesdropping is conducted

at the exit node, only the IP address of destination may be extracted. However, if the eavesdropping is conducted on the middle node neither information about the origin nor information about destination of the packet may be extracted.

Tor hidden services

The real advantages of Tor network are anonymous routing to the hidden services. These hidden services are network services such as Web servers, Secure Shell (SSH) server, File Transfer Protocol (FTP) server, and instant messaging servers whose locations in the network are hidden. To access a web server on the surface web, a client has to obtain the IP address of the web server from the Domain Name System (DNS) server. DNS sends the IP address to the client. With an IP address, it is easy to find the location of the web server. The protocol of accessing the hidden services will be explained below.

The hidden services in Tor, similar to the surface service, have to advertise its existence within the network. For advertisement, the hidden service randomly chooses three relays in the network and sends a request, asking relays to act as an introduction point for the hidden service. With the request, the hidden service is sending its own public key to the introduction points as well. Communication between the hidden service and introduction points is happening through the onion circuits, as previously explained. The hidden service is preserving anonymity in the network by building those circuits.

The next step in the hidden service establishment is a creation of a hidden services descriptor. The hidden services descriptor contains the following information for each introduction point:[21]

1. identifier - hash of introduction point's identity key
2. address -address of this introduction point
3. port -port where this introduction point is listening
4. onion key - public key for communicating with this introduction point
5. service key - public key for communicating with this hidden service
6. intro authentication -tuples (lists) of the form (auth_type, auth_data) for establishing a connection

The descriptor is uploaded to a distributed hash table. The descriptor is distributed on relays and information about the distribution is stored on the hidden services directory. When a client wants to browse a service, the client sends a request for browsing. The request has a form such as kpvz7ki2v5agwt35.onion. The 16-character name is delivered from the public key of hidden service. A client downloads the descriptor from the distributed hash table using a 16-character request. The descriptor and hidden service name are information necessary to obtain information about the introduction points and the public key of the hidden service.

The next step is creating a new circuit to a randomly chose a relay. This randomly chosen relay has to act as a rendezvous point. The client shares a temporary key with the rendezvous point. The client then assembles the message which contains the address,

[21] Tor Project, “Hidden Service Descriptor,” accessed December 29, 2016, https://stem.torproject.org/api/descriptor/hidden_service_descriptor.html.

temporary key of rendezvous, and requests for the services. The message is encrypted with the hidden services public key and the request is delivered to the introduction point through the circuit. The introduction point resends the message to the hidden service through the new circuit.

The next step begins when the hidden service receives the message. The hidden services decrypt the message and finds the address of the rendezvous point and the temporary key. The hidden services then establish a circuit to the rendezvous point and send a new temporary key through the circuit. The rendezvous point then notifies the client about the successful circuit establishment with the hidden services. The rendezvous point serves continuously as a relay between the two circuits.

In summary, in the connection between the client and hidden services six relays are used.

The next generation of hidden services will go one step further and the 16-character URL and will be changed to a 50-character URL. The hidden services will be created with stealth applications and access to the hidden service will only be possible if the client has been invited to access the service. The hidden services will not declare a .onion address to the hidden services directory. The hidden service will derive the unique cryptographic key from the address. This unique cryptographic key will then be delivered to the Tor hidden services directory. The anonymous user who is looking for certain hidden services can derive the same key from the .onion address and then access the hidden service. If the service directory is compromised there will be no chance to deliver the .onion address from the cryptographic key stored in the directory service. Nick Mathewson, one of three original designers of Tor has asserted about the future of the

hidden services: “The Tor network isn’t going to give you anyway to learn about an onion address you don’t already know.”[22]

Access to the Tor network

Browser, software, and operating systems for access to the Tor network are available on the surface web. All of those tools for access are open source and free. The Tor browser is the easiest way to access the Tor network. The browser can be freely downloaded from the Tor project website on the surface web. Once the Tor browser is installed on a computer, access to the Tor network is established and a Tor browsing client can access the hidden services. There is no difference between accessing the deep or dark web, all which are hidden somewhere behind services. A client who is seeking the services must know the 16-character address. The clients type or usually pastes this address into the Tor browser and after a certain time, the hidden site is presented on the client’s screen. To achieve full anonymity with the Tor browser is not sufficient to only install the browser. It is recommended to establish some habits to maintain anonymity. These habits include awareness of hardware identification, and not opening the Tor browser on a full screen. It is not recommended to use cookies, however, there are a recommendation about client operating system. The windows operating system is inadvisable for anonymity. A client who is using Tor without the protection of data on data storage has a false sense of anonymity. The most preferred operating systems are the systems that offer data operational security. The level of the information protection from

[22] Andy Greenberg, “It's About To Get Even Easier to Hide on the Dark Web,” *Wired*, January 20, 2017, accessed January 22, 2017, https://www.wired.com/2017/01/get-even-easier-hide-dark-web/.

an adversary in ways that a traditional security program does not have is defined as operational security-OPSEC.[23] The traditional way to protect classified information is the Information Assurance, but OPSEC is the way to protect unclassified indicators from being revealed to the adversary. Without OPSEC, the information that a client gets from the anonymous network can be revealed when he continues to use the same data storage on the surface web browsing with malware on his computer or if the client's computer is the subject of an investigation. A client's good OPSEC combined with anonymity network cause problems for law enforcement authorities to provide evidence on law violation.

The operating systems used to achieve OPSEC and anonymity in the Tor network are:

1. Tails Linux
2. Whonix

These two operating systems are the most frequently used in the Tor network. The common feature for them is secure access to the Tor network. All computer traffic goes through Tor relay to make those operating systems more "plug and play secure". The way that those two operating systems are used is not a same. While Tails Linux is live DVD, SD memory or a live USB operating system, the Whonix is an operating system which a user has to install virtually on the base operating system with the help of a virtualization software.

[23] Department of the Army, Army Regulation 530–1, *Operations Security* (Washington, DC: Government Printing Office, September 2014), 1.

The Tails Linux operating system is a Tor project open source operating system. The primary feature of the Tails is that it is live system booted from the medium (DVD, USB, or SD). This live medium is used to boot the Tails on any hardware that allows live booting. Live boot is allowed on most contemporary computers. The second feature of the Tails is cloning of the installed medium. The advantage of Tails is the ability to clone a live medium without tracking, which makes it a preferred system over other solutions. One person with good technical skills can clone one medium for a group and provide access and OPSEC for less skilled users. The cloning advantages allow the Tails users no forensic traces. There is no possibility to find the number of the live medium copies. Theoretically, only one piece of hardware can be recognized as the system that has downloaded installation of Tails. If the Tails is downloaded over the surface web, the recognition is possible with hardware MAC address identification. The Tails also offers encryption of emails and chats. A file encryption is something that increases OPSEC for users of this operating system. A persistence storage is a next feature that makes this operating system favorable among the Tor users. The persistence is encrypted storage with a unique password to access storage. The data and settings saved on the persistence storage remain preserved after a restart of the live medium system. All other data are permanently deleted after rebooting the live medium. The Tails do not leave any forensic traces on hardware where the system has been run. The Tails also offer a package of software that the user may use for editing documents, pictures, and cryptocurrency wallet, however, there is a software that can be used to wipe the metadata of any file stored on the data storage.

Whonix is another operating system used for anonymity developed from the TorBOX project but currently is independent from the Tor project. The Whonix is completely interoperable with the Tor network. Unlike the Tails, the Whonix is a preinstalled and preconfigured system prepared to be run on the virtual machine. The host system for a virtual machine can use any operating system with an installed virtual machine workstation. Whonix consists of virtual elements, the first virtual element is Whonix gateway and the second virtual element is Whonix workstation. Both virtual elements are preconfigured to be installed and run on the virtual machine. The host operating system is only used to run visualization software and can access the surface web any time without any interference from Whonix. However, the virtual connection between a Whonix workstation and a Whonix gateway forces all traffic originated from the workstation to flow to the gateway and then to Tor network. This virtual system prevents leaking of the IP address of the workstation. The workstation is operating in an isolated network. To reach the rest of the network, the workstation can only go through the gateway, and the workstation does not know the external IP address which is used for access to the Internet. Any malicious software, if is running on the workstation, is not able to find access to the Internet. The Whonix gateway IP address is default gateway IP address for the workstation to access the Internet and this is usually addressed from the private range of addresses. The Whonix gateway is configured to establish a circuit with Tor relay. Depending on the workstation operating system, the client can install and run the software he needs, and he does not have to be afraid that any malware can reveal his IP address. Administrating virtual boxes, virtual gateway and workstation requires a significant level of knowledge in order to stay anonymous.

While the Whonix provides a better level to prevent IP leaking, the Tails provides no traces of activities the client has conducted on his hardware. The decision of which one is better depends on client's preference.

De-anonymization of the hidden services

The term "de-anonymization" refers to the technique of data mining. The technique cross-references anonymized information with other available data in order to identify a person, group, or transaction.[24] The term is also known as re-identification.

The hidden services exist on Tor network and they are the same kind of services on the surface web, with one "small" difference. The IP address of hidden services is unknown, and as is the IP address of the client who is accessing the hidden services and this cannot be revealed by the hidden service. With a high level of anonymity, the Tor network becomes interesting for people who are dealing with illicit activities. The Tor network becomes a safe haven for illegal activities. The most known case for de-anonymization of administrator and hidden service is the de-anonymization of the administrator of Silk Road site on Tor network.

The Silk Road site was created in January 2011[25], with a purpose to provide an online marketplace for illicit goods. After the site was created, an administrator employed several people (at least five people) who were responsible for running an online

[24] Investopedia, "Investopedia terms," accessed March 23, 2017, http://www.investopedia.com/terms/d/deanonymization.asp.

[25] United States District Court Southern District of New York, "US vs Ross Ulbricht," United States Department of Justice, March 25, 2015, accessed January 10, 2016, https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/US%20v.%20Ross%20Ulbricht%20Indictment.pdf.

marketplace for income.[26] To conceal the identity of buyers and sellers, the main trade currency was Bitcoin. The site acted as a mediator between buyers and sellers. Mediator interest was commission per transaction. As a mediator who held Bitcoins until the buyer confirmed receipt of the goods, the site become a money laundering service. The possibility to trace transactions become impossible. The site then became a marketplace for:

1. Controlled substances
2. Weapons
3. Malicious software for hacking (key-loggers, remote-accessing tools, etc.)
4. Different types of Personally Identifiable Information
5. Fake documents

The Silk Road case is known for soliciting the user to commit murder-for-hire. On March 29, 2013,[27] a user of Silk Road who became a threat to reveal the identity of other users was killed. The administrator of the site ordered the murder of the user offering reward in bitcoins for the hitmen. The assassination was executed by another Silk Road user who was paid as promised.

On October 2013, Ross William Ulbricht, known as Dread Pirate Roberts (DRP), was arrested in Glen Park Branch Library in San Francisco. He had logged onto n Silk Road site as an administrator at the moment of arrest.

[26] Ibid.

[27] Ibid.

Government authorities struggled with the problem how to find administrators of the Silk Road site and to shut it down. According to the declaration of Cristopher Tarbell, the FBI agent involved in the case, the Silk Road site was not properly configured.[28] The FBI agent had recorded traffic during interaction with the site login interface. He revealed in a log file an IP address not belonging to the Tor relays IP address. The IP addresses of Tor relays are publicly listed, and anybody can see the addresses. When a revealed IP address was entered on the surface web, the browser showed a part of the login screen. The IP address presented crucial evidence to locate the Silk Road server.

After the Silk Road was shut down, other illicit market sites started to bloom. The government answer on emerging black markets sites was Operation Onymous. On November 6, 2014, the outcome of the global joint action, become visible. The US and 16 European nation members of Europol's European Cybercrime Centre (EC3) and Eurojust worked together to shut down over 400 dark market sites.[29] The technique on how such a large amount of hidden services was de-anonymized still remains classified. The information on how the successor of the Silk Road site, the Silk Road 2.0, was revealed during the Operation Onymous is unclassified. Silk Road 2.0 has been revealed using social engineering. An undercover agent became a member of the site and gained

[28] Christopher Tarbell, "US vs Ross Ulbricht." PlainSite, September 5, 2014, accessed January 12, 2016, https://www.plainsite.org/dockets/download.html?id=184393342&z=d06999bd.

[29] Federal Bureau of Investigation, "Dozens of Online Dark Markets Seized Pursuant to Forfeiture Complaint Filed in Manhattan Federal Court in Conjunction with the Arrest of the Operator of Silk Road 2.0," November 7, 2014, accessed January 15, 2017, https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/dozens-of-online-dark-markets-seized-pursuant-to-forfeiture-complaint-filed-in-manhattan-federal-court-in-conjunction-with-the-arrest-of-the-operator-of-silk-road-2.0.

the trust of the senior administrator of the site. The agent exploited the information as an administrator to de-anonymize other users. The organizer of the website, Blake Benthall, made an OPSEC error using his personal email address to register server Silk Road 2.0.[30]

The Tor project developers assume that there may be several reasons why the hidden services were located in the Operation Onymous. These reasons are listed below:[31]

1. Low level of OPSEC
2. SQL injection
3. Bitcoin de-anonymization
4. Attacks on the Tor network

De-anonymization of the users

De-anonymization of users on the dark web sometimes is more important than finding and shutting down a hidden service or arresting an administrator. On the Silk Road example, it was shown that even when the original site was shut down the next version became available several days later. The users of hidden services which provide training for terrorists, data for kill lists, illicit fundraising or child pornography, are more

[30] The Guardian, "Silk Road 2.0 targeted in Operation Onymous Dark-Web Takedown," November 7, 2014, accessed January 15, 2017, https://www.theguardian.com/technology/2014/nov/07/silk-road-20-operation-onymous-dark-web-drugs-takedown.

[31] Tor Project, "Thoughts and Concerns about Operation Onymous," November 9, 2014, accessed January 15, 2017, https://blog.torproject.org/blog/thoughts-and-concerns-about-operation-onymous.

dangerous than the site administrators who are responsible only for the maintenance of the site.

Operation Pacifier is the FBI activity that led to criminal charges against 186 people.[32] The operation was a government activity to suppress child pornography. The main activity started in spring 2015, after the administrator of the dark web child pornography site "The Playpen" was arrested and the hardware of the site was located. The FBI had obtained a court warrant to run the site "The Playpen" for two weeks. The first activity the FBI did was move the site to the government premises. FBI improved hidden service capabilities and made the service faster and easier for access. At this time the number of visitors to the "The Playpen" jumped from 11,000 to 50,000 people per week.[33] The second activity involved geolocation of the site's users. For this purpose, the FBI used a legal hacking technique against users who had accessed the child pornography site. The technique used to conduct that activity was Network Investigative Techniques (NIT). The basic of NIT are the following.

A known fact is that the site was set up as hidden services and the location (IP address) of users was not easily discovered. The users created circuits to the rendezvous relay and one more circuit was created from the rendezvous relay to the hidden service. The rendezvous relay IP address is the only address that may be revealed without the use of the NIT. In "The Playpen" case, the site as user's destination was operated by

---

[32] Mike Carter, "Investigation of FBI's Child Pornography Operations Sparks Controversy Over Internet Privacy," *Governement Technology*, August 31, 2016, accessed January 15, 2017, http://www.govtech.com/public-safety/Investigation-of-FBIs-Child-Pornography-Operations-Sparks-Controversy-Over-Internet-Privacy.html.

[33] Ibid.

government law enforcement personnel. However, for the two weeks that the site was operated under FBI control, the NIT was being put in place in order to de-anonymize users that were accessing the hidden service.

The NIT was applied to all users who were logged on the site. The modified site gave a unique identification number to the user at the moment when he was logged to the service. The identification number was unambiguously associated with the user. A key difference from previous versions of the site and the site operated by FBI is the transfer of malicious code to the user's computer. The malicious code established background control of the user's hidden services proxy and browser. The malicious code had control over sub software that copied basic data of the computer that can be used for forensic analysis. Some of those data are media access control (MAC) address, IP address of the computer, user username, and password for access to "The Playpen". The malicious software then established a connection to the logging server on the surface web and transmitted the collected payload. The role of the logging server is to gather all activities and information of users who have accessed the site and to create records of users' identification numbers and data obtained with malicious code. With an unmasked IP, the FBI served subpoenas on internet service providers to provide names and house address of users who had violated the law. When the court provided search warrant for FBI agents to look for evidence of child pornography and to seize the physical computer which executed the NIT, the agents had conducted search and seizure of relevant evidence.

Searching for the hidden services

A hidden services URL address is very hard to remember and to access the hidden service sites, a user needs to find or know a 16-character URL of services. The first web page that beginners are usually accessing after they install the Tor is the hidden wiki web page. The hidden wiki is a web page on the deep web with the list of hyperlinks to other uncensored hidden services. The list of services is divided begins with introduction points and continues with financial services, commercial services, email, messaging, blogs, social networks etc.

Introduction points on the hidden wiki web page list the search engines that can be used on the deep web. Some of the search engines are search engines created to improve anonymity on the surface web. Others do not have the capability to index the deep web sites even if they are used in the Tor network. The hidden wiki is the lists search engines that are capable of searching the hidden services. Search engines can be divided as:

1. Search engines that improve anonymity for searching services from deep web to surface web (DWSW)
2. Search engines used for searching for services from deep web to deep web hidden services (DWDW)
3. Search engines used for searching from services from the surface web to the deep web (SWDW)

Search engines DWSW, such as DuckDuckGo, are search engines used to search for services on the surface web, but the server is on the Tor network, and the search engine behaves as a hidden service. Instead of searching on the surface web, from where

the DuckDuckGo server is accessible, a user can search on the DuckDuckGo search engine that is running as a hidden service. Use of the search engine where the server is running on the Tor network, the OPSEC is increased.

Search engines DWDW, such as TORCH, GRAMS, Not Evil, Ahmia, are search engines used to search for hidden services. Those search engines are indexing hidden services and making them more accessible. All those services are on the Tor network and they behave as hidden services. The philosophy of searching is different from the surface web searching engines because some are used only for certain domains. For example, the GRAMS is recommended for dark market searching. The Not Evil search engine searches for a specific word in a textual part of a hidden service content, or for the title or for a specific word in the URL.

Search engines used for SWDW, such as TORCH, Ahmia, Onion.Link, are search engines used to search for hidden services from the surface web. Usage of these search engines leads to two questions concerning the purpose of SWDW. The first question is: What is the point to search for hidden services from the surface web? And the second question is: What can the user do with the results he got from searching for the hidden services from the surface web?

Answers are following: First, searching from the surface web is service provided for users who do not care too much for their anonymity, but they intend to access the hidden services. During this interaction hidden service anonymity is fully covered, when the user does not maintain any level of anonymity. Second, the Web2Tor proxy allows the surface web users to access the hidden services without the usage of any Tor proxy application to the Tor network. The Web2Tor proxy gives the opportunity to users to use

results they get from a search engine and allows users to use DWDW search engines. For example, to access the hidden services from the surface web, users have to add the new Tor domain attachment. Some of those attachments are tor2web.fi, onion.sh, onion.link, onion.to, onion.city, onion.cab, onion.direct. These abbreviations are links for different Web2Tor proxy servers that provide access to the hidden services.

A common feature for all search engines is that they provide a vast amount of data, and a person searching for data is not able to process all received data. Current search engines have been created to fit all-purpose searches. The processing point for received data at the end is a person searching for a term online. Site administrators optimize their sites to adjust them for a search engine to appear as result of searching on the first or second page. The surface web sites administrators have an interest to advertise and offer services for a wide audience. On the other hand, searchers are people who do not want to spend too much time in searching for a term. When searching information is presented, users usually read the first or second page of received information. Most do not read past the second or third pages. However, what happens with sites whose administrators do not optimize, or the sites or with sites that are not “crawlers” friendly? The government institution whose task is to find threat online need search engine capable of organizing or aggregate results. Besides indexing, those search engines has to be much more than a standard search engine.

The MEMEX (MEmory and indEX) program was launched by Defense Advanced Research Projects Agency (DARPA) in 2014.[34] The purpose for launching the program was to improve the deficiencies of current search engines and provide the government with a tool for advanced searching. For DARPA demo day 2014, the Memex was described as follows:

> Memex seeks to develop the next generation of search technologies and revolutionize the discovery, organization, and presentation of public-domain search results. Initially, DARPA intends to develop Memex to address a key DoD mission: fighting human trafficking.[35]

The Memex has been developed to suppress a human. The Memex search tools are domain specific and at the beginning, the searching domain was human trafficking. Mechanisms in the Memex allow searches to extract information from a discovered content. The discovered content are not only pages that contain a term of interest, the content are pictures, video, and metadata of searched object. The discovered content user can organize and search in a subset of information and visually analyze the interconnection between discovered terms on different online location. The Memex vision for the future includes:[36]

---

[34] DARPA, "Memex Aims to Create a New Paradigm for Domain-Specific Search," September 2, 2014, accessed January 19, 2017, http://www.darpa.mil/news-events/2014-02-09.

[35] DARPA, "DARPA Demo Day 2014 Highlights Innovative Approaches to Preserving and Expanding U.S. Technological Superiority," May 21, 2014, accessed January 19, 2017, http://www.darpa.mil/news-events/2014-05-21.

[36] Wade Shen, "Memex," DARPA, accessed January 19, 2017, http://www.darpa.mil/program/memex.

1. Development of next-generation search technologies to revolutionize the discovery, organization, and presentation of domain-specific content
2. Creation of a new domain-specific search paradigm to discover relevant content and organize it in ways that are more immediately useful to specific tasks
3. Extension of current search capabilities to the deep web and nontraditional content
4. Improved interfaces for the military, government and commercial enterprises to find and organize publically available information on the Internet

Terrorist exploitation of Cyberspace advantages

The first computer was the privilege of the armed forces or research centers. This piece of hardware was enormously expensive, and access to processor power was the privilege of the chosen and smart. Over time, computers become personal devices that are used on a daily basis and become an integral part of human life. As time passed, computers had become network devices and those devices have created a shortcut for human necessity and a majority of contemporary human interaction happens in cyberspace. Cyberspace has been created with the intention to provide a humankind prosperity. But not all people have the same intentions in the world. Malicious intention of people who have access to cyberspace has started to create some difficulty in cyberspace. A mirror of humankind is the dark web. All those services on the dark web have been created by people who had the motive to make them. Terrorists use the advantages of cyberspace as their way to achieve their goals. Cyberspace has become a domain where they have exploited cyber tools (means) for achieving goals (end state).

The means terrorists use in cyberspace are numerous, but they can be divided into two categories:[37]

1. Communicative
2. Instrumental

Communicative use of cyberspace is mainly for psychological warfare campaigns, to spread propaganda, securing internal communications, and radicalizing recruits.

Instrumental uses of cyberspace are mainly for online teaching and training, creating virtual camps for future assailants.

The hidden services on the dark web have become fertile ground for online platforms that may be used for:

1. Psychological warfare
2. Propaganda
3. Online indoctrination
4. Recruitment and mobilization
5. Virtual training
6. Cyber-planning and coordination
7. Ordnance trade
8. Fundraising
9. Financial fraud and trade with personally identifiable information
10. Kill-lists (hit list)

[37] Gabriel Weimann, *Terrorism in Cyberspace: The Next Generation* (New York: A Columbia University Press 2015), E-Book, 48.

Finally, the targeted audience of terrorist groups is not the wide audience, as the targeted audience for online surface service is. A targeted audience is a narrow group of people interested in a terrorist's activities, and people who support those activities. The terrorist's main audience is a specific population, such as a young population, women, "lone wolves", overseas community and diaspora.[38]

The young population is targeted as a population where terrorists indoctrinate more supporters. The themes to spread radical Islam are most common. Themes are spread through violent video games, social networks or sometimes tough recruiting and training services. Those services may be either on the surface web or on the dark web.

Women are targeted by spreading propaganda and indoctrination to join in "mujahid" (female mujahedeen). The messages targeting woman are calling them to "be strong in supporting Islam and assisting the male fighters."[39]

Diaspora and overseas communities serve as a source of revenue for finances and recruiting fighters. The Islamic State has extensive success with narrowing targeted audiences online in recruiting fighters from North America and Europe.[40]

The "lone wolves" are not the individuals who are targeting alone as the term implies. These individuals are assumed to be alone, but they have organizations or groups that provide logistic and material support. The hidden services provide online tools for recruiting, radicalizing, teaching, training and directing those individuals. The aspiring

[38] Ibid., 95-107.

[39] Ibid., 102.

[40] Ibid., 299-338.

terrorist can find on the dark web manuals how to create homemade explosive devices, maps, diagrams of a potential target, also they may find the target with all personally identified information. The kill-list has been published between March and May 2016 by three pro-Islamic hacking groups: the Caliphate Cyber Army (CCA), the Islamic State Hacking Division (ISHD), the United Cyber Caliphate (UCC). [41] This list has data of US citizens and the government employees who are marked for execution. Those hacking groups have targeted specifically the "lone wolves" who are supposed to conduct execution of the target. The link for accessing the data was shared with the "Telegram" application. The "Telegram" is a phone messaging application with end to end encryption. The question is, how the kill-list has been created and where did the data come from. The kill-list for ISIL did not come directly. The data for the kill-list was provided by a hacker who used tools available on the dark web, but most interestingly, they have used the dark marketplace to sell personally identifiable information from social networks such as LinkedIn and Myspace.[42] The hacker was not influenced by a terrorist, however, ISIS has bought data and then extracted necessary data from social networks' personal data information.

[41] SITE Intelligence group, "Kill-list from pro-IS hacking groups," SITE Intelligence group, Dark Web and Cyber Security, June 7, 2016, accessed January 18, 2017, http://sitemultimedia.org/docs/SITE_Analysis_of_Islamic_State_Kill_Lists.pdf.

[42] Motherboard, "These So-Called 'ISIS Kill Lists' Are a Great Reminder to Change Your Password," June 16, 2016, accessed January 21, 2017, http://motherboard.vice.com/read/these-so-called-isis-kill-lists-are-a-great-reminder-to-change-your-password.

Cryptocurrency

The cryptocurrency is the medium of exchange similar to other national currencies. The cryptocurrency is not same as online banking where even the transaction occurs online. The value of cryptocurrency lays in cryptography, a security of the transaction, and in the difficulty in solving a mathematical problem. At first, cryptocurrency was created in 2009 by the Japanese who used the pseudonym Satoshi Nakomoto.[43]

> Bitcoins are like the rewards for a correct answer to a certain math problem. Both the problem and the answer are completely unique. There will be a limit of about 21 million (the eventual exact number is 20,999,999.97690000) of these special solution rewards known as the bitcoin.[44]

The Bitcoin (BTC) is used for online trading, and transactions in Bitcoin is most similar to the cash transaction. The Satoshi is the smallest unit of BTC and represents about millionth part of single bitcoin (0.00000001 BTC). The government cannot tax or track that transaction, because of lack of information about individuals who conduct the transaction. The advantage of BTC is that everyone can create (mine) them. A transaction with BTC is verified by nodes which confirms and maintains records about the transaction. Volunteers run the nodes. The number of BTC is limited and it is not possible to create more than the maximum number. Transaction of BTC is anonymous, however, an official exchange with BTC requires personal information. For trading with BTC, users need a wallet. The wallet stores BTC code, and can exist on any data storage,

---

[43] Daniel Forrester and Mark Solomo, *Bitcoin Exposed:Today's Complete Guide to Tomorrow's Currency* (US: Createspace Independent Pub, 2013), 25.

[44] Ibid., 21.

or cloud. BTC wallet gives BTC address which is used as identification for trading. For example, this group of characters 19N3KUZhZujGuGSpjhBuMzqfGptKXZo1Yo is an example of the wallet address. A trade with BTC can occur without giving any personal information. The BTC transaction is public, and everybody can see the amount of BTC and the wallet addresses involved in the exchange. If a client wants to make an exchange in BTC for any currency or to buy BTC, the client needs to leave bank account information on the wallet and authenticate himself with a phone number. To protect anonymity, clients trade with BTC personally. They find online people interested in buying or selling BTC for cash. A client can exchange BTC on BTC ATM, or "laundering" BTC on an online "laundering service". The hidden or the surface web "laundering service" takes a commission for its service. A process of laundering BTC is following.

A client creates N wallets, the first wallet is a regular wallet with his personal data and the wallet is linked to a bank account. The second, third, …, Nth wallets are created with a fake email address and they are anonymous. Clients trade with anonymous wallets. Usually, for every trade, a client creates a new wallet, but when the client needs to exchange BTC for any currency, he sends BTC from an anonymous wallet through "laundering service" for the first wallet. Then the client withdraws BTC with the first wallet from the "laundering service". Within the "laundering service" BTC are mixed with other BTC and the client never withdraws the same amount or BTC, or the same BTC, that he sent from the anonymous wallet. After exchange through "laundering service", it is impossible to prove a connection between the anonymous and the first wallet. The client than legally exchanges BTC for currency.

CHAPTER 3

RESEARCH METHODOLOGY

The primary purpose of this study is to analyze the dark web services and possible solutions to detect, deter and disrupt threats emanating from the dark web. The study examines ways how terrorist organizations utilize services on the dark web. For the study, the Tor network and the Tor network hidden services are analyzed as the most likely platforms for anonymity on the dark web.

The onion routing system was originally created to protect government communications. The protection was based on a separation of routing information from identification of the network users. The basic routing system carries a risk that can jeopardize anonymity of network users. In the classical routing network, nodes have information of the origin and destination of the communication. On the other hand, the location of the services on the surface web are very easy to find. In order to protect government employees, journalists, whistleblowers, bloggers etc., the Tor project offers a significant level of anonymity and online protection. However, a significant level of anonymity and protection has become alluring for users who utilize services to conduct illicit activities online. Among those users are terrorists who are using the dark web as a platform for psychological warfare, propaganda, online indoctrination, recruitment and mobilization, virtual training, cyber planning and coordination, ordnance trade, and fundraising. Governments all around the word have recognized the threat emanating from the dark web and have started to find solutions to detect, deter and disrupt threats from the dark web.

The purpose of this chapter is to outline the method used to answer the primary research question:

"How can the government detect, deter, and disrupt threats emanating from the dark web?"

The literature review has confirmed that for the examination of this topic unclassified, quantitative data is not available. A qualitative study is the only feasible approach to examine terrorist activities on the dark web. The outcomes of this research are government ways and means for reducing the amount of illicit activities on the deep web. The sources for the research are doctrinal publications, journals, articles, Internet sources, books and eBooks relevant to provide information about activities, technology and means and ways for addressing the research question.

The research is divided into four parts. The first part consists of the introduction to the literature review. A growing trend for anonymity is described, and the problem statement is presented. The central research question and the secondary questions that are considered in this research are featured. The most used technology to gain anonymity on the Internet, the Onion routing, is described. The hidden services technique is described and three most common ways to access the dark web are presented. The examples of a successfully conducted operation in order to de-anonymize either the hidden service or the user on the dark web are described. Also, the terrorist activities that use the dark web are illustrated and the way of conducting anonymous transactions is presented. The sources for the first part, which consists of an introduction and a literature review chapter, are publicly available unclassified sources, mainly from the Internet, and research papers which describe the technology used and terrorist activities conducted on the dark web.

The second part of this research is the methodology chapter and describes how research is conducted. The methodology of this research is qualitative.

The operational approach is the method used to conduct an analysis, which is the third part of this research. The current environment is presented with a Relationships, Actors, Functions and Tensions (RAFT) diagram. After the diagram analysis, the dark web services come to the fore as the platform for online illicit services. The dark web is then analyzed through Center of Gravity, Critical Capability, Critical Requirements, and Critical Vulnerabilities. The two operational approaches are analyzed.

The first operational approach is created for the most dangerous end state, a high-risk outcome. This operational approach then analyzes ways the government can use to block all access to the Tor network and identifies advantages, disadvantages, and risks.

The second operational approach is created for the most likely end state. This end state is to downgrade the number of illicit hidden services and global suppression of illicit hidden services. This step has a moderate risk, but global international cooperation has to be established for a long time period.

Finally, the conclusion is the fourth part of this research. In the conclusion, the answer is given to the primary research question and all secondary research questions are revised. All crucial information on the study is summarized into findings and recommendations for future research are proposed.

The qualitative research is conducted with unclassified information. The unclassified sources are selected with caution and all of the sources have provided facts on how these activities are conducted. The assumptions listed in this research are from respected individuals who are subject matter experts in the hidden services and the dark

web. The assumptions are given to explain how the operations are most likely done. Those assumptions are not used for the analysis. Because of the changes in modern technology and constant changes in the area of research, the sources considered for this research are from 2011 to 2017.

CHAPTER 4

ANALYSIS

> An element of virtually every national security threat and crime problem the FBI faces is cyber-based or facilitated. We face sophisticated cyber threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists.
>
> — James Comey, FBI Director

The purpose of this chapter is to analyze possible action that governments can take in order to detect, deter, and disrupt threats emanating from the dark web. The expected outcomes from the analysis are two operational approaches, the most dangerous and the most likely. A complex position of the dark web in a current environment requires more than simple observation of the problem in order to understand the environment. The operational methodology will be conducted to develop each operational approach.

Operational design

According to Joint Publication 5.0, the commander links ends, ways, and means to achieve the desired end state through operational art. The commander is required to answer the following questions:[45]

1. What is the military end state that must be achieved, how is it related to the strategic end state, and what objectives must be achieved to enable that end state? (Ends)

[45] Department of Defense, Joint Publication 5-0, *Joint Operation Planning* (Washington, DC: Government Printing Office, 2011).

2. What sequence of actions is most likely to achieve those objectives and the end state? (Ways)
3. What resources are required to accomplish that sequence of actions within the given or requested resources? (Means)
4. What is the chance of failure or unacceptable consequences in performing that sequence of actions? (Risk)

The general methodology to understand the situation and problem in the application of operational art is known as operational design. The operational design has three components and they are:

1. Understanding the environment
2. Defining the problem
3. Producing operational approach

Understand the environment

The anonymous cyber environment is a complex environment where actors have different backgrounds and different motives to exploit advantages or disadvantages of the dark web. The Relationships, Actors, Functions and Tensions (RAFT) between actors in this environment vary depending on the power of the actor and how the actor may use his power. In this research, the RAFT diagram of the Tor network is presented in figure 5, in order to visually represent what is going on in the environment. The Tor network can be exploited by either a democratic or totalitarian government. The main goal of the Tor network is to promote democracy, human rights, and freedom of speech.

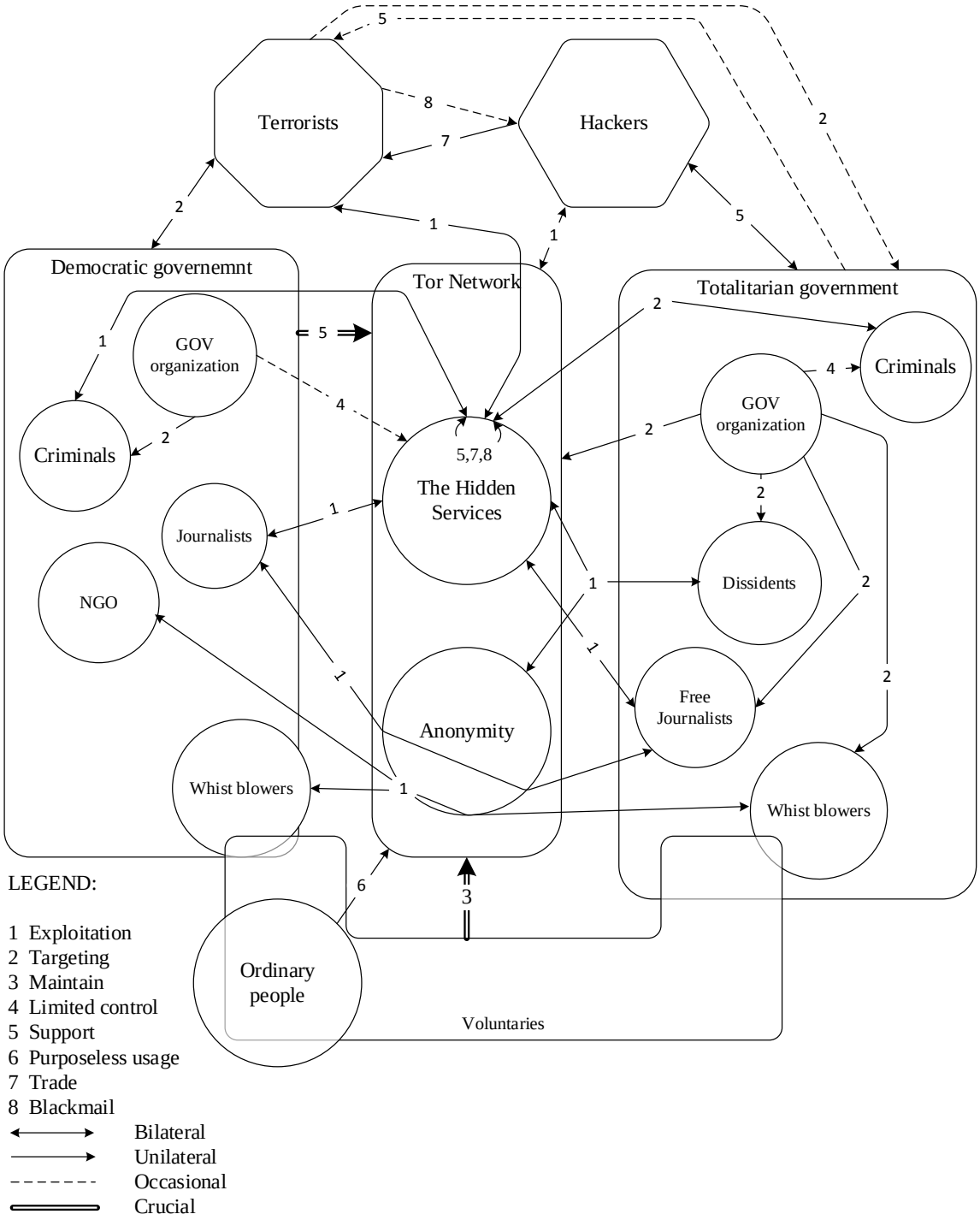


Figure 5. The RAFT in Tor

Source: Created by the author.

The Tor network serves as an online platform for a journalist who promotes freedom of speech and allows a broad audience to access the information without fear that the government will identify users. Either in democratic or totalitarian governments, the Tor network allows the whistleblowers to provide information about illegal activities of their superiors. The Tor network is free of communication control. The anonymous communication between whistleblowers and journalists or Non-Government Organizations (NGO) through messaging services, online forums, email, etc. is granted.

The NGO can be virtually present in totalitarian regime territory and support covered activists or dissidents. The Tor network is the secure infrastructure in the territory of the democratic government also. Moreover, the Tor network protects users from democratic stakeholders who try to establish "the limited control" of the Tor network. The democratic government goal is to fight threat originating from the hidden services that are used for illicit activities.

The totalitarian government is exploiting the anonymous services to avoid international blockades, to conduct illegal activities online, or to support illegal activities.

The hackers are mainly supported by the totalitarian authority to provide information or to provide an advantageous position on the market. The hackers, either organized by some totalitarian government organizations or self-organized, use the dark web as a platform to sell their products or illegal spoil. With or without awareness of their business partner's identity, they sell everything for profit, support, or redemption. Sometimes the hackers conduct illegal activities because of the belief that they doing a noble deed.

The terrorist, business partners of hackers, or terrorists supported by totalitarian government use the Tor network as an online platform for their activities. Some of the main activities they conduct on the dark web are, recruitment, indoctrination, radicalization, ordnance or controlled substance trade, and fundraising.

The volunteers install, operate, and maintain network nodes (relays-bridges), services, and keep the whole network independent from any government organization. They develop network capabilities and compensate for security shortfalls. They are ordinary people or professionals who dedicate their time and resources to the network.

On the other hand, the Tor network is used by curious people who want to explore different services or to maintain their own privacy in the trend of global surveillance.

The Tor network has become an online platform for illicit activities of criminal or terrorist groups. Those individuals have exploited anonymity and advantages of the hidden services to run their business. The terrorist groups use the Tor network mainly for recruitment, indoctrination, radicalization, ordnance or controlled substance trade, and fundraising. Other users such as hackers, either aware or unaware, participate in supporting those activities. The reason that terrorists have started to exploit the Tor network as a communications platform is a level of anonymity on the network, security, and the hidden services. That kind of network allows people who do illegal activities online to be protected and to expand their activities all around the world. The hosting services that are offering services on the Tor network, allow hosting of the illicit services with or without awareness of it. All those hosting companies operate in accordance with the policy of the network and do not request identification of the customers.

The desired state of the system is either to significantly decrease the number of illicit activities on the deep web and enable network for human rights expansion or to block the entire Tor network.

Define the problem

Terrorist organizations exploit advantages of the Tor network and use the network as the online platform for illegal and unacceptable activities. The platform allows clients to stay anonymous and protected in the same way as the services are protected. The platform allows terrorists to gain an advantage in directing, recruiting and training their followers. The terrorist's investment in the network infrastructure is inconsequential comped with the gain they obtain from the significantly protected network infrastructure. They obtain services of transport, protection, and anonymity without paying. Moreover, combining advantages of network advantages and cryptocurrency, the terrorist groups can collect money for their activities without any fear that the government can uncover and seize the sources.

After the RAFT analysis, the two actors of the deep web come to the fore. The first is the Tor network infrastructure, and the second is the hidden services. Those two actors play a significant role for terrorist activities on the dark web. The Tor network is the infrastructure platform that allows the terrorist organizations to have anonymity and to access the hidden services. The hidden services represent an online platform that allows the terrorist to influence, radicalize, recruit, train direct followers, or trade and raise funds anonymously. The government actions against illicit activities on the dark web can target those two actors to reach following end state:

1. Block access to the whole Tor network,
2. Decrease the number of illicit hidden services.

The terrorist's strength relays on the Tor network, anonymous transactions, black market, volunteers who run the network and organized hacker groups supported or blackmailed.

The Tor network is independent and relies on volunteers who dedicate their technical skills to run the network. The lack of support of any government or government organization makes the Tor network trustworthy to different actors. Volunteers want to run the network to exploit their own needs from the network and they do not care about the negative context of the network. The purpose of the network is to spread human rights and freedom, as is stated on the official Tor project site. Organized hacker groups, either supported or blackmailed by terrorists, partially represents a source of knowledge for running the illicit anonymous services. Hackers exploit advantages of anonymity of the network and weakness of surface web services. They are harvesting all necessary information from the surface web and use dark web services to share their spoil. However, they use tools that they can buy on the dark web to be more efficient in harvesting surface web services. The tools are available for everybody who is willing to trade. The market is not only for hacking tools. The market allows "lone wolves" to find ordnances they need to conduct tasks they get from superiors.

The weakness in this system include user's or services administrators' OPSEC, a lack of knowledge about the system, and the possibility for deceiving hackers who chase illicit actors, especially terrorist groups. The whole system is relying on trust between actors. Weak OPSEC is shown as the main reason why the illicit activities were

suppressed on the dark web. The mistake that administrators of the hidden sites made before they were arrested shows that their OPSEC was weak or degraded during the time. Clients' weak OPSEC also leads to the de-anonymization of the clients. The less they know about how to protect their data, the greater the possibility to uncover their activities. The lack of knowledge how to access safely to the hidden services allows the government to easily track activities of the clients if they do not set up protection in a proper way. Operating or running services on the dark web mainly rely on trust between actors. The trust is shared between administrators and clients, and at some point, the administrator gives administrators rights for service to a person that he has never met, but he trusts him because of his contribution to the services. It has been shown that the deception is leading to the de-anonymizing of key actors that are running the service. The data that the administrator of the service gets from his console are valuable for starting the process of de-anonymization. In the case of Silk Road 2.0, the trust that the undercover agent got from the site administrator led to finding data of key holders of the service because of the weak OPSEC of the site administrator. Namely, the administrator of Silk Road 2.0 used his own public address to register the server.

The hackers who chase terrorists represent a weakness for the terrorist. It is hard to compare those hackers with government organizations or to put them under government control but they have advantages over government activities. They do not have any law that they have to obey, they do not need permission from a higher level to destroy or downgrade services, however, they can share information that is valuable for government organizations to follow the terrorists. They use illicit tools to shut down illicit services. For example, hacker collective Anonymous has run hacking operations to

suppress all terrorist activities online after the terrorist attack in Paris 2015. The government cannot rely on those hackers, because they only have the same goal temporarily as the government has, and they do not always share same values as the government.

As previously mentioned, there are two solutions to the problem. The first is blocking the Tor network, and the second is decreasing the number of illicit services on the Tor network. In order to propose a solution, key terms need to be identified.

The solution for the problem involves the Center of Gravity (COG) with its supporting elements Critical Capabilities (CC), Critical Requirements (CR), and Critical Vulnerabilities (CV). In the Joint Publication 5.0 the terms are defined as follows:

1. COG is a source of power that provides moral or physical strength, freedom of action, or will to act
2. CC are those that are considered crucial enablers for a COG to function as such and are essential to the accomplishment of the adversary's assumed objective(s)
3. CR are the conditions, resources, and means that enable a critical capability to become fully operational
4. CV are those aspects or components of critical requirements that are deficient or vulnerable to direct or indirect attack in a manner achieving decisive or significant results

Solution 1: Block access to the Tor network

Blocking the Tor network is an act which needs global consensus in order to be successful. The solution requires effort but the risk of this solution is high. Blocking the

whole network has the consequence (collateral damage) of blocking services that are used to develop human rights and freedom in some countries.

If the identified adversary COG the overall Tor network the CC are:

1. Setup the Tor relays or bridges
2. Global volunteering
3. Trust at the network
4. Provided level of anonymity
5. Protection of the hidden services

The CR that enables the Tor network CC are:

1. Relay's or bridge's software
2. Relay's or Bridge's hardware
3. Internet providers
4. Client proxy software or operative system
5. Client operative system protection
6. Knowledge to develop or run the network
7. Knowledge of properly setup client and services system
8. Volunteers
9. Crypto algorithms

The CV of the Tor network are:

1. Client operative system protection
2. Knowledge of setup client and service system
3. Lack of trust in the network
4. Unlimited access to the network

Solution 2: Decrease the number of illicit hidden services

To decrease the number of illicit hidden services is a solution which needs more effort than blocking whole Tor network. However, the number of illicit services will never be zero, but the operation will be considered successful if the government decreases and maintain a number of illicit online services below an acceptable level. The collateral damage of this solution is minimal especially because the target is certain hidden services, not all services.

The COG for solution 2 are the illicit hidden services. For this COG the CC are:

1. Setup the Tor relays/bridges
2. Global volunteering
3. Hosting the hidden service
4. Trust at the service
5. Provided level of anonymity
6. Protection of the hidden services

The CR that enables illicit hidden services CC are:

1. The relays or bridges
2. Directory services
3. The guard node
4. Internet providers
5. Hosting providers
6. Protection of hosting services
7. Knowledge to install, maintain and operate the hidden service
8. Client OPSEC

9. Client proxy software or operating system
10. Unlimited network access
11. Cryptocurrencies
12. Secure service to share URLs
13. The “Crawl” unfriendly services
14. Trust in administrators of the hidden services

The CV of the illicit hidden services are:

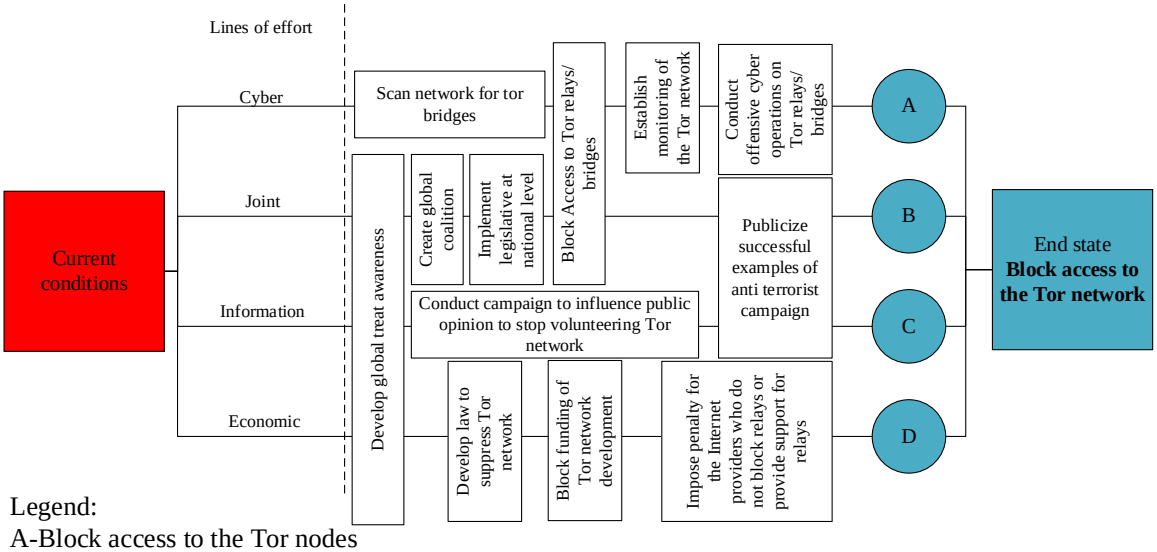
1. Client operative system protection
2. Knowledge of setup client and service system
3. Lack of trust in the network
4. Unlimited access to the network
5. Deception
6. Indexing of the hidden services

Operational approach – Block access the Tor network

The solution 1 as the center of gravity considers the Tor network infrastructure with all elements. The Tor network is serving as a platform for legal and illicit services. If we consider the Tor network as the center of gravity for illicit activities on the dark web, blocking the Tor network follows as a logical solution. On figure 6 the operational approach for blocking the Tor network is depicted.

Current conditions on figure 6 are described and depicted with RAFT diagram, figure 5. The desired end state to block access to the Tor network can be achieved through four lines of effort: Cyber, Joint, Information, and Economic. Each line of effort has a desired end state, and they are:

1. Block access to the Tor nodes using objectives of cyber effort
2. Decrease number of volunteers, supporters to the Tor network using objectives of a joint effort
3. Decrease trust at the Tor network using objectives of information effort
4. Decrease legal funding of the Tor network using objectives of economic effort



Legend:
A-Block access to the Tor nodes
B-Decrease number of volunteers, supporters
C-Decrease trust at the Tor network
D-Decrease legal funding of the Tor network

Figure 6. Operational approach– Block the Tor network

Source: Created by the author.

The key effort for blocking access to the Tor network is a broad coalition of the countries who will accept legislation for blocking the Tor network and to accept the fact that at this point, the Tor network provides more threat than good. This network has experienced expansion not for promoting the human rights and freedom. It has become a

network that is known as the foundation for illegal online services worldwide. Some of those services that are exploited by terrorist groups jeopardize people's lives, rights, and freedoms. The network becomes a free Command and Control (C2) network for terrorist activities, the base for fundraising, training, and influencing supporters. With that awareness of threat originating from the Tor network, the broad coalition is necessary in order to block access. The majority of relays for Tor network are geographically located in Canada, EU, Russia, and the US. About 87 percent of all Tor nodes are located in those countries. Germany has 20 percent of all nodes, the US has 18 percent, and France has 13 percent.[46] Blocking the whole network requires the coalition to maintain a small number of the network elements and to maintain the permanent blockade on new network elements from coalition countries.

The risk for blocking access to the Tor network is a direct influence on NGO, whistleblowers, and dissidents who will lose the anonymity they have, especially in countries with totalitarian regimes.

There are several examples of countries that tried to block access to the Tor network and establish censorship on the Internet. One of those countries is Turkey. The Turkish government issued an order to their Internet Services Providers (ISP)[47] at the beginning of December 2016 to block access to the Tor network. Besides blocking access to the Tor network, ISPs had an obligation to report the success of the order weekly. Even

[46] Tor Status, "Tor Network Status," February 22, 2017, accessed February 22, 2017, http://torstatus.blutmagie.de/.

[47] BBC, "Turkey Blocks Access to Tor Anonymising Network," December 19, 2016, accessed February 23, 2017, http://www.bbc.com/news/technology-38365564.

with strong repressive measures on ISPs to block access, there were reports from Turkey that some of the experienced network users were able to access the Tor network but the majority of users were impacted by this censorship.[48] The reason for blocking the Internet was not to fight against illicit services but to increase the level of censorship in the country. Turkey is an example how one country does not have full capacity to block the Tor network. Without a broad coalition, especially without the consensus of Canada, EU, Russia, and the US, the success to the block network is not granted. If there are more countries involved in the coalition, there is a greater possibility to be successful in blocking access to the Tor network.

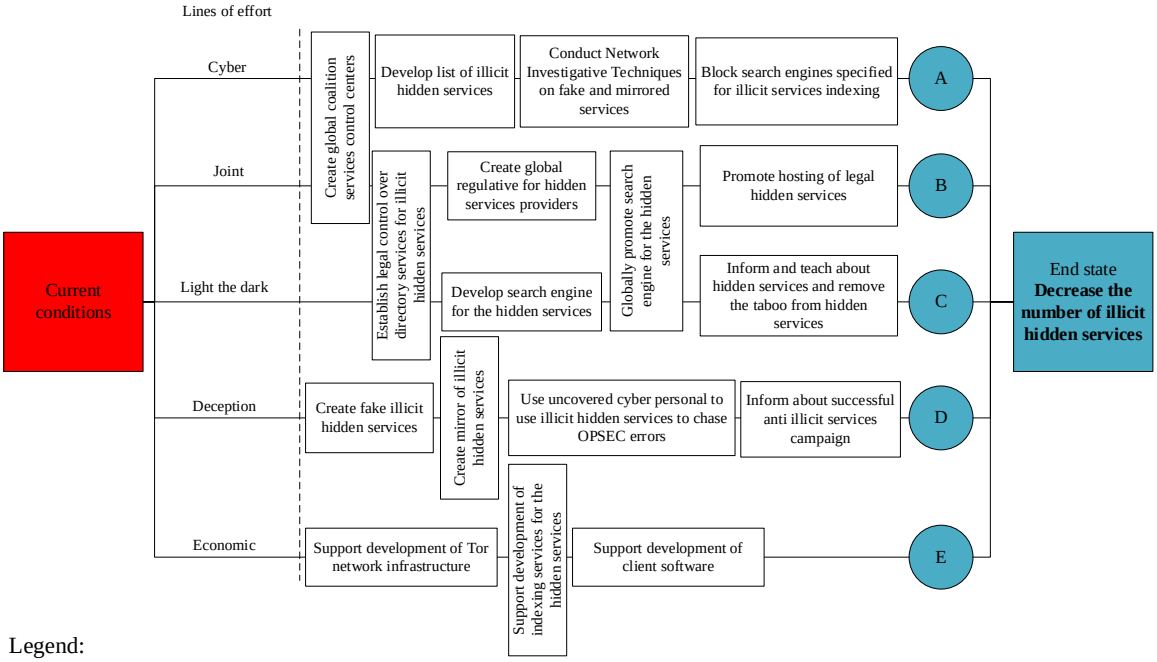
Operational approach – Decrease the number of illicit hidden services

The second proposed solution is to reduce the number of illicit hidden services. Terrorist groups and criminals use the hidden services as an online platform for different illicit activities. If we consider the illicit hidden services as a center of gravity for illicit activities on the dark web, decreasing the number of illicit hidden services follows a logical solution for the problem. On figure 7 the operational approach for decreasing number of illicit hidden services is depicted.

Current conditions on figure 7 are described and depicted with RAFT diagram, figure 5. The desired end state to decrease the number of illicit hidden services can be achieved through five lines of effort: Cyber, Joint, Light the dark, Deception, and Economic. Each line of effort has a desired end state, and they are:

[48] Editorial, "Tor Blocked in Turkey as Government Cracks Down on VPN Use," December 18, 2016, accessed February 23, 2017, https://turkeyblocks.org/2016/12/18/tor-blocked-in-turkey-vpn-ban/.

1. Shut down the de-anonymized illicit hidden service.
2. Establish broad control over hosting of the hidden services.
3. Index the hidden services.
4. Decrease terrorist or criminal trust at the hidden services and client software.
5. Increase governmental support on hidden services infrastructure.



Legend:
A-Shutdown the deanonymized illicit hidden services.
B-Establish broad control over hosting of the hidden services.
C-Index the hidden services.
D-Decrease terrorist/criminal trust at the hidden services and client software.
E- Increase governmental support on hidden services infrastructure

Figure 7. Operational approach– Block the Tor network

Source: Created by the author.

The key effort for this operational approach is a strong offensive cyber effort, together with coalition partners. In order to decrease the number of illicit hidden services,

the coalition has to increase the level of deception on the dark web. Namely, in Operation Pacifier, the government seized a server, and then improved capabilities, moved the server to its own facilities, continued to run services, and conducted NIT on clients. This example is particularly important for chasing the terrorists, “lone wolves”, domestic supporters, and recruits. The activities to decrease the number of illicit hidden services has to be part of the bigger anti-terrorist campaign. The government has to support the development of the Tor network infrastructure, client software for anonymous access to the network. By supporting the network, the terrorist level of confidence in the network will decrease. The next generation of the Tor network will develop stronger protection mechanisms at the directory server. It will be better to have technicians involved in this project to understand and exploit weak points of the system in order to protect the population from terrorism and criminal activity. Development of the search engine capable to index most of the services of the deep web has to be a priority in the future. Current search engines on the deep web have been developed to search for specific purposes, and some of them such Grams Search Engine are used to search for dark market goods. Those search engines have to be suppressed and make searching the dark web harder that it is now. From a legislative point of view, there are steps necessary to create a legislative foundation for controlling hosting on the deep web. This control has to recognize the objectives of the web host companies. The first goal for the web hosting companies has to be overall security and then profit.

The duration in the time necessary to achieve this operational approach is long and this is actually the risk that this operational approach carries. The fourth generation of the Tor network will make the system more resistant on de-anonymization and more

complicated for indexing. Blocking specific services has to be the goal of the coalition fight against illicit services on the dark web. However, blocking the Tor services will likely inflict collateral damage on services that promote freedom and human rights.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

> The single biggest existential threat that's out there, I think, is cyber.
> — Admiral Michael Mullen-Chairman of the JCS

Conclusions

Increased level of control on surface web, caused some users to move from the surface web to the deep web, seeking for anonymity and protection. The reasons for anonymity and protection over government control vary from the desire to protect privacy or to protect anonymity when high-level corruption is reported through petty and high criminal activities to the acts of terrorism. Over the time different types of network structures have been developed to offer anonymity and protection for the clients. Some of those networks have offered anonymity for monetary compensation. All of those networks were not well known or widespread over the world. The client who has money to pay has used those networks and services. In September 2002 the Tor network appeared on the Internet. The following year it was publicly released and then within 12 months, a hidden wiki site had been set up. The blooming of Tor network has started from 2004. The Tor network as one of the deep web network infrastructure has been accepted by a wide variety of users. Some of the users continued to use the deep web services as they were used in surface web, but there are users who have created hidden services that were basically used for illicit activities. The services used for illicit activities become services of the dark web. With a significant degree of protection and high level of anonymity, Tor has become more well known as a platform for dark web services. In

2011 the first controlled substance market, Silk Road site, was developed. There was a high amount of controlled substance occurring online for two years. The benefit of anonymous transaction retrieved the cryptocurrency Bitcoin.

The control over the surface web, especially strong censorship over terrorist propaganda sites caused terrorists to move to the dark web. The reasons why terrorist exploit the dark web services are to avoid censorship on the surface web, significant protection and anonymity, and protection from hacktivists. More than this, the hidden services as an online platform in combination with cryptocurrency is a safe haven for fundraising, money transfer, and the black market. Moving from the surface web to the dark web the terrorist has kept old techniques they have been using on the surface web and adapted them to a new system. As time goes on they will invent new types of services that will be used to support their terrorist activities.

The government has the ability to detect, deter, and disrupt illicit activities on the dark web but not with the same speed as is done with surface web services. There are constraints that influence the government speed of action, however, Tor as the network technology is highly resistant to any kind of governmental control. The law norms limit governmental institutions ability to act broadly and target wide areas in order to suppress illicit services. On the other hand, the wide geographical diffusion of servers that host illicit services causes a problem to any government organizations ability to bring offenders to justice.

The purpose of this research is to describe a possible solution for the government to detect, deter, and disrupt threats emanating from the dark web. To find a solution the following secondary questions have been analyzed:

1. What is the technical aspect of the dark web network-The onion routing?
2. What is the significance of Tor network?
3. How do safe and secure transactions occur on the dark web, and are they really secure?
4. Which sites are used for illicit activities and are they active now?
5. How can the dark web be exploited and who can exploit its medium?
6. What ways and means exist to influence the dark web?

The finding from research are following:

The Onion routing is one of the techniques used to build a network below the Internet surface. The primary Tor has been founded by U.S. Naval Research Laboratory, but in the year 2003, the network had a public release. Beside Tor network, there are a variety of the networks that offer a certain level of anonymity and protection on the deep web. The key elements of the tor network are relays and bridges. Volunteers are running those network elements. Volunteers use existing internet connections to establish circuits between the key network elements. Those circuits are encrypted, and three-layer encryption is used to protect circuits. The packet's payload is encrypted with the first level of encryption than the cryptogram is encrypted again and the layers remind on the onion layers. The network elements are run by volunteers and the whole concept is currently open source project. At the moment of this research, the third generation of Tor network is in use.

A separation of the identity of the user from the routing of information, as well as the availability of illicit goods and services, is the significance of the Tor network. Tor network element, unlike traditional routing, routes IP packets through the network

without knowing information about origin and destination of the packet. The network elements know only which element is sending a packet and which element is going to receive the packet. The transporting circuit is known only to the client. The second significance of the Tor network are the hidden services. Those services are similar to the surface services but unlike the surface services, neither client nor server know the location of each other in the network.

The transaction with cryptocurrency is safe and secure. Cryptocurrency transactions rely on blockchain and volunteers who update and maintain logs for the transaction. Volunteers get an award or payment for maintaining those logs and for solving transaction problems. The process to exchange cryptocurrency for cash has many legal loopholes that allow owners of the cryptocurrency to maintain anonymity. Those transactions are invisible from a legal perspective. There are online services for laundering cryptocurrency to hide any trace of cryptocurrency transactions and origin of transactions. Those services increase the level of anonymity and security for an illegal transaction, and in combination with client OPSEC measures for protecting anonymity, the theoretical probability of tracing the transactions is very low.

The services used for illicit activities can be divided into services for the black market, fundraising, propaganda or influence, disseminating orders or communication (chat, forums, emails, etc.). Those services are durable and governments have to accomplish complicated procedures to downgrade and disrupt their functionality. However, examples from the past have shown that it is possible to suppress those services. When the government shuts down some of those services the new version of the site appears a short time later. For example, currently, there is Silk Road 3.0, with

services that have been offered on the first version of the services. Fundraising is another way to get money online. Some of those sites are real, but lately, there has been fake sites appearing, similar to fundraising site but with the different address of the wallet. Those fake sites may be created deliberately to turn the focus away from the real target.

Tor network was primarily designed to protect the anonymity of government employees. Later the Tor project has offered a high level of protection and anonymity to a variety of clients some of them are harmless but the majority of them were clients with a mission. Besides criminals and hackers, the terrorists and their supports may represent the most dangerous users of the dark web. The terrorist mainly exploits the dark web for either communicative or instrumental purpose. Communicative use of the dark web is mainly for psychological warfare campaigns, to spread propaganda, securing internal communications, and radicalizing recruits. Instrumental uses of the dark web are mainly for online teaching and training, creating virtual camps for future assailants. Criminals and hackers are using the dark web as a market space for their products. However, there are curious people who want to see what is the dark web and what kind of services or information they can find there. There are a lot of rumors about several levels of the dark web but those stories are just for people who are curious and interested in something different than they cannot find on the surface web.

In this study, two possible solutions (end state) were proposed for addressing illicit activities on the Tor network as a platform for the dark web. The first solution is to block access to the Tor network and the second solution is to decrease the number of the hidden services that are used for illicit activities. Two operational approaches are analyzed to propose ways and means to achieve end state. For both operational

approaches, there are three common efforts, Cyber, Joint, and Economic. The three lines of effort have different objectives (means) but the common ways do detect, deter and disrupt illicit activities on the dark web are to conduct offensive cyber activities on the wide geographical area, in order to decrease funding of the network or the illicit hidden services infrastructure. The risks for those two approaches are different. For blocking whole Tor network, there is risks for the users who uses the network for human prosperity. For example, activities who spread liberty and human rights, people who report high-level corruption will be censored or observed. Critical coalition or unwillingness of countries to access to the coalition is another risk that appears to block the whole Tor network. The risk becomes higher if some of the key countries such as Canada, EU, Russia, and the US refuse to be part of the coalition. For the approach to decrease the number of the illicit hidden services the risk is time. The Tor network is constantly evolving and there are assumptions that fourth generation of the Tor network will be more resistant on de-anonymization. However, the operation to decrease the number of illicit services will need a long and dedicated effort.

Unexpected findings

The next generation of Tor hidden services will go one step ahead and the URL will be 50 characters long. The hidden services will be created with stealth applications and access to the hidden service will only be possible if the client had been invited to access the service. The Tor user who is looking for certain hidden services can derive the same key from onion address and then access through the network to the hidden service.

Recommendation for future study

In this study, the dark web has been analyzed through the Tor network as an infrastructure platform. Of course, illicit activity occurs on the platforms other than Tor. Some of these platforms are:

1. Invisible Internet Project (I2P): Distributed anonymous point to point (P2P) network
2. Freenet: Distributed anonymous P2P network
3. Vuvuzela: Scalable Private Messaging System
4. Riposte: An Anonymous Messaging System

For future research, it will be beneficial to analyze the other platforms used for anonymity and protection on the dark web. However, the surface web offers some of the services that are used for illicit activities. The site "JustPaste.it", in combination with the Telegram application was used to disseminate the ISIS kill-list. Examination and analysis of those activities will be beneficial for future research.

Summary

The study analyzed the dark web services that are exploited by terrorist organizations. The focus of the study was on Tor network infrastructure and the hidden services. A study, explanation, and examples of terrorist activities were presented. The government successful achievement in de-anonymization of services administrators and clients were presented and technique how those operations were accomplished. For all of those successful operation, offenders have used network elements in several countries. The most successful operation on the dark web was Operation Onymous. In this operation, the targets were illicit sites and site administrators. The key actor of this

operation was the US along with 16 European countries. This coalition shut down more than 400 hidden services. Operation Pacifier has shown that sometimes the de-anonymized hidden services presents an opportunity to catch high-value terrorist targets or criminals. Well-designed cyber action with proper utilization of cyber tools such as NIT has led to charges against offenders. Seizing money from illicit sites has shown that without the revenue offenders were not able to be successful in their activities.

In summary, the government in concert with coalition partners can detect, deter, and disrupt threats emanating from the dark web. By conducting offensive cyber activities across a wide geographical area, the dark web network funding can be reduced and infrastructure along with the hidden services degraded.

BIBLIOGRAPHY

BBC. “Turkey Blocks Access to Tor Anonymising Network.” December 19, 2016. Accessed February 23, 2017. http://www.bbc.com/news/technology-38365564.

Bergman, Michael K. “White Paper: The Deep Web: Surfacing Hidden Value.” *Journal of Electronic Publishing* 7, no. 1 (August 2001). Accessed October 10, 2016. http://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main.

Berton, Beatrice. “The Dark Side of the Web: ISIL’s One-Stop Shop?” European Union Institute for Security Studies (EUISS), June 26, 2015. Accessed October 20, 2016. http://www.iss.europa.eu/publications/detail/article/the-dark-side-of-the-web-isils-one-stop-shop/.

Blake, Andrew. “#OpISIS and #OpParis: Anonymous Hacktivists to Retaliate against ISIS after Paris Attacks.” *The Washington Times*, November 16, 2016. Accessed October 20, 2016. http://www.washingtontimes.com/news/2015/nov/16/opisis-and-opparis-anonymous-hacktivists-to-retali/.

———. “Russia Weighs Letting Telecoms Use Govt. Surveillance System for New Anti-Terror Law: Reports.” *The Washington Times*, August 10, 2016. Accessed October 11, 2016. http://www.washingtontimes.com/news/2016/aug/10/russia-weighs-letting-telecoms-use-ex-kgbs-surveil/.

Carter, Mike. “Investigation of FBI’s Child Pornography Operations Sparks Controversy Over Internet Privacy.” *Government Technology*, August 31, 2016. Accessed January 15, 2017. http://www.govtech.com/public-safety/Investigation-of-FBIs-Child-Pornography-Operations-Sparks-Controversy-Over-Internet-Privacy.html.

CBS News. “New Search Engine Exposes the Dark Web.” February 8, 2015. Accessed October 17, 2016. http://www.cbsnews.com/news/new-search-engine-exposes-the-dark-web/.

CIDR Report. “General Status.” December 25, 2016. Accessed December 25, 2016. http://www.cidr-report.org/as2.0/#General_Status.

DARPA. “DARPA Demo Day 2014 Highlights Innovative Approaches to Preserving and Expanding U.S. Technological Superiority.” May 21, 2014. Accessed January 19, 2017. http://www.darpa.mil/news-events/2014-05-21.

———. “Memex Aims to Create a New Paradigm for Domain-Specific Search.” September 2, 2014. Accessed January 19, 2017. http://www.darpa.mil/news-events/2014-02-09.

Department of Defense. Joint Publication 5-0, *Joint Operation Planning.* Washington, DC: Government Printing Office, 2011.

Department of the Army. Army Regulation 530–1, *Operations Security.* Washington, DC: Government Printing Office, September 2014.

Dilipraj, E. “Terror in the Deep and Dark Web.” *Air Power Journal* 9, no. 3 (2014): 121-140.

Editorial. “Tor Blocked in Turkey as Government Cracks Down on VPN Use” December 18, 2016. Accessed February 23, 2017. https://turkeyblocks.org/2016/12/18/tor-blocked-in-turkey-vpn-ban/.

Federal Bureau of Investigation. “Dozens of Online Dark Markets Seized Pursuant to Forfeiture Complaint Filed in Manhattan Federal Court in Conjunction with the Arrest of the Operator of Silk Road 2.0.” November 7, 2014. Accessed January 15, 2017. https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/dozens-of-online-dark-markets-seized-pursuant-to-forfeiture-complaint-filed-in-manhattan-federal-court-in-conjunction-with-the-arrest-of-the-operator-of-silk-road-2.0.

Forrester, Daniel, and Solomo Mark. *Bitcoin Exposed: Today's Complete Guide to Tomorrow's Currency.* US: Createspace Independent Pub, 2013.

Fox-Brewster, Tom. “Silk Road 2.0 Targeted in Operation Onymous Dark-Web Takedown.” *The Guardian*, November 7, 2014. Accessed January 15, 2017, https://www.theguardian.com/technology/2014/nov/07/silk-road-20-operation-onymous-dark-web-drugs-takedown.

Greenberg, Andy. “It's About To Get Even Easier to Hide on the Dark Web.” *Wired*, January 20, 2017. Accessed January 22, 2017. https://www.wired.com/2017/01/get-even-easier-hide-dark-web/.

Investopedia. “Investopedia terms: De-Anonymization.” Accessed March 23, 2017, http://www.investopedia.com/terms/d/deanonymization.asp.

Motherboard. “These So-Called “ISIS Kill Lists” Are a Great Reminder to Change Your Password.” June 16, 2016. Accessed January 21, 2017. http://motherboard.vice.com/read/these-so-called-isis-kill-lists-are-a-great-reminder-to-change-your-password.

Net Market Share. “Market Share Statistics for Internet Technologies.” Accessed January 19, 2017. http://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0.

Onion Routing. “Brief Selected History.” Accessed December 24, 2016. https://www.onion-router.net/History.html.

Shen, Wade. “Memex.” DARPA. Accessed January 19, 2017. http://www.darpa.mil/program/memex.

SITE Intelligence group. “Kill-list from pro-IS hacking groups.” SITE Intelligence group, Dark Web and Cyber Security, June 7, 2016. Accessed January 18, 2017. http://sitemultimedia.org/docs/SITE_Analysis_of_Islamic_State_Kill_Lists.pdf.

Soldatov, Andrei, and Irina Borogan. “Russia's Surveillance State.” *World Policy Journal* (Fall 2013). Accessed October 11, 2016. http://www.worldpolicy.org/journal/fall2013/Russia-surveillance.

Sui, Daniel, James Caverlee, and Dakota Rudesill. *The Deep Web and Darknet: A Look inside the Internet's Massive Black Box*. Washington, DC: Woodrow Wilson International Center for Scholars, August 2015.

Syverson, Paul. “A Peel of Onion.” *ACSAC'11* (December 5-9, 2011), 123-135.

Tarbell, Christopher. “US vs Ross Ulbricht.” *PlainSite*, September 5, 2014. Accessed January 12, 2016. https://www.plainsite.org/dockets/download.html?id=184393342&z=d06999bd.

The Internet Live Status. “Internet Users in the World.” Accessed October 18, 2016. http://www.internetlivestats.com/watch/internet-users/.

Tor Project. “Who uses Tor.” Accessed October 18, 2016. https://www.torproject.org/about/torusers.html.en.

———. “Hidden Service Descriptor.” Accessed December 29, 2016. https://stem.torproject.org/api/descriptor/hidden_service_descriptor.html.

———. “Thoughts and Concerns about Operation Onymous.” November 9, 2014. Accessed January 15, 2017. https://blog.torproject.org/blog/thoughts-and-concerns-about-operation-onymous.

———. “Tor Metrices-About.” Accessed December 24, 2016. https://metrics.torproject.org/about.html.

Tor Status. “Tor Network Status.” February 22, 2017. Accessed February 22, 2017. http://torstatus.blutmagie.de/.

United States District Court Southern District of New York. “US vs Ross Ulbricht.” United States Department of Justice, March 25, 2015. Accessed January 10, 2016. https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/US%20v.%20Ross%20Ulbricht%20Indictment.pdf.

Washington Post. “NSA Slides Explain the PRISM Data-Collection Program.” July 10, 2013. Accessed October 17, 2016. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

Weimann, Gabriel. “Terrorist Migration to the Dark Web.” *Perspectives on Terrorism*, June 2016. Accessed October 20, 2016. http://www.terrorismanalysts.com/pt/index.php/pot/article/view/513/html.

———. *Terrorism in Cyberspace: The Next Generation.* Washington, DC: Woodrow Wilson Center Press, 2015.