THE UTILISATION OF THE DEEP WEB FOR MILITARY COUNTER TERRORIST OPERATIONS

MJ Aschmann[1], L Leenen [2,3], and JC Jansen van Vuuren[2,4]

[1] South African National Defence Force, South Africa
[2] CSIR, Pretoria, South Africa
[3] Cape Peninsula University of Technology, Cape Town, South Africa
[3] University of Venda, Thohoyandou, South Africa
michael.aschmann@sita.co.za
lleenen@csir.co.za
jjvvuuren@csir.co.za

Keywords: Deep web, Dark web, Counter-terrorism, Cyber offensive

Abstract:
The Internet offers anonymity and a disregard of national boundaries. Most countries are deeply concerned about the threat cyberspace and in particular, cyberterrorism, are posing to national security. The Deep and Dark Web is associated with anonymity, covert communications and trade. This brings to the table a new opportunity for organised crime and terrorist organisations to trade, communicate, plan and organise specific strikes or market their future activities. Simultaneously, this has opened military operations to a new facet of collecting and processing information to gain an advantage over an adversary who wants to remain anonymous and unseen, especially in the intelligence realm. The military of any nation must be on the forefront in protecting and defending its citizens from these types of threats. Asymmetrical use of the Deep and Dark Web has allowed for rogue actions to take place in which the military has a responsibility to strike back at terrorist organisations who threaten the safety of its citizens. There is a need for new methods and approaches for military forces to plan and conduct counter cyberterrorism operations. This paper gives an overview of using the Deep and Dark Web in military counter terrorist operations, presents an adaptation of the "Cyber Kill Chain" methodology aimed at gathering information for cyber counter terrorist operations, and presents a rudimentary approach to incorporate cyber counter terrorist operations with military terrorist operations.

1. Introduction

The Internet or the "GRID" as it is commonly known is a sea of data and information that is sent, received, stored and viewed by multiple people whether incognito (private), anonymous or open. No one actually owns the Internet, and no single person or organisation controls the Internet in its entirety. The Internet is more of a concept than an actual tangible entity, and it relies on a physical infrastructure that connects networks to other networks. The Internet is analysed by people and machines, and it is interpreted in multiple different ways. The Internet holistically is divided into mainly three Spaces, namely the Surface web, Deep web, and the Dark web which can also be referred to as the Unseen Web (Sui, Caverlee, & Rudesil, 2015). In this paper the Internet will be discussed in the terms of the three main spaces or layers; the Surface Web, the Deep Web and the Dark Web. In this light it will be brought into context of how collecting information of terrorist communication and activities within the Unseen Web, namely the Deep and Dark Web, can assist in military counter terrorist Operations as a concept.

In the remainder of this section the three Internet spaces are discussed as well as the concept of cyberterrorism. Section 2 considers Military Cyber Operations and Counter-terrorism and introduces the "Cyberterrorism Kill Chain" methodology for counter cyberterrorism. In Section 3 a methodology for military counter cyberterrorism operations is presented. The paper is concluded in Section 4.

1.1 Internet Spaces

The three Internet spaces will each be discussed holistically. The Surface web is a space which is indexed and which information in websites is viewed or accessed through search engines such as Google or Bing are crawled. Google, currently the largest search engine, has only indexed 4-16% of the Surface web (Sui, Caverlee, & Rudesil, 2015). The uses are more for general information viewing, searching for websites such as marketing sites, public blogs, forums or intranet pages of companies. Different estimates of the size of the Surface Web have been published; according to the

Website Magazine, Google had indexed 200 Terabytes of data in 2014 which is just 0.004 percent of the total Internet (Website Magazine, 2014).

The Deep Web (Invisible, Unseen or Hidden Web) is a space of the Internet that has not been crawled and indexed, thus is not seen by standard search engines. Users need to authenticate themselves for a specific service or database that they want to be part of, or subscribe to. It is a platform in which users interact within a closed network in private or anonymously, and information is password protected and encrypted. It is technically impossible to determine the size of the Deep web; it is estimated to be 400-500 times bigger than the Surface Web (Sui, Caverlee, & Rudesil, 2015). It is estimated that in 2013 the data stored on the 60 largest Deep web sites alone were 40 times larger than the size of the entire Surface Web (HiddenWiki, 2013). Examples of sites in the Deep Web are The U.S. Library of Congress, the economic data site FreeLunch.com, Census.gov, Copyright.gov, PubMed, Web of Science, WWW Virtual Library, Directory of Open Access Journals, FindLaw, and Wolfram Alpha. It also includes pay-to-use databases (such as Westlaw and LexisNexis), credit card systems and PayPal accounts and various social networks namely Twitter and Facebook, YikYak and Webchat, Instant messaging (IM) (Sui, Caverlee, & Rudesil, 2015).

The Dark Web (Dark Net, or Dark Internet) is a space of the Internet that is part of the Deep Web which is a closed specific group of networks for specific users with access. It is not a separate network but applications and protocols that make use of existing networks (Biddle, England, Peinado, & Willman, Unknown). Most Dark web sites can only be accessed anonymously. The Dark Web is associated with online criminal trade and services, as well as users in certain countries that do not allow citizens to freely communicate, post or view the Surface web. They thus circumvent enforced censorship via the Dark Web. An example of a Dark Web trade platform is a site called GRAMS.onion (http://grams7enufi7jmdl.onion/), which is a search engine specifically for the Dark Web.

Another use of the Dark Web is image sharing (e.g., http://www.zw3crggtadila2sg.onion/imageboard/) in which users take advantage of the security provided by the Deep Web. Some applications are aligned with Dark Web culture, such as secure whistleblowing sites (e.g. http://5r4bjnjug3apqdii.onion/) and eBook collections that focuses on subversive or revolutionary works (e.g., https://xfmro77i3lixucja.onion.lt/). Journalists have used SecureDrop or GlobalLeaks to share files via the “The Onion Router” (TOR) network as well as from an investigative and sources view point. There are chat services available, i.e. OnionChat (http://www.chatrapi7fkbzczr.onion/) which can be used to communicate and share information with other Deep Web users (Sui, Caverlee, & Rudesil, 2015). The systems and technologies which are used to access the Dark Web are TOR, I2P and Freenet, and this will be discussed later in the paper. The TOR network allows users to access the Hidden Wiki (Onion Link Directory). Certain services are available and are somewhat indexed. To access this one can use TOR and access the Hidden Wiki with the following URLs http://kpvz7ki2v5agwt35.onion, https://wikitjerrta4qgz4.onion or https://www.torlinkbgs6aabns.onion (Kalomni, 2012). There are many Dark Web users who are using the Dark web to communicate and are using its other functionalities for criminal or terrorist activities. Governments, terrorists, law enforcement and criminals are amongst the biggest users of these services (TurboFuture, 2015).

1.2 Terrorist vs Cyberterrorist

A terrorist can be defined as a radical who employs violence against civilians, uses terror as a political weapon usually organises with other terrorists in small cells and often uses religious fundamentalism or political radicalism as a cover for terrorist activities (Mirriam Webster). There is no commonly accepted definition of a cyberterrorist, but we quote two definitions. According to the US Federal Bureau of Investigation, cyberterrorism is “any premeditated, politically motivated attack against information, computer systems, computer programs, and data that results in violence against non-combatant targets by sub-national groups or clandestine agents” (TechTarget). Dorothy Denning has offered the following definition of cyberterrorism: “Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not” (Weimann, 2005). The U.S. Federal Bureau of Investigation considers cyberterrorism to be any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents" (Rouse, 2010). Collin (Collin, 1997) describes in “The Future of Cyberterrorism” how the disruption of a country’s banks or even international financial transactions and stock exchanges can cause loss of confidence in the economic system and subsequent destabilisation. He also offers scenarios where an attack on air traffic control systems can cause the collision of aircraft or a remote attack on pharmaceutical manufacturers may alter the formulation of medication with the subsequent loss of life.

Although there is not consent whether violence is required for an act to be regarded as cyberterrorism, the difference between a terrorist and a cyberterrorist is regarded to be the use of information technology and its means, by terrorist groups according to Krasavin of the Computer Crime Research Center cyberterrorism (Krasavin, Unknown). Cyberterrorism is mainly focused on inciting psychological terror online.

Cyberterrorists may use hacking techniques to reach the end state of the specific terrorist mission. Although one can argue that hacktivism does not amount to counter-terrorism because hacktivists do not endeavour to kill, maim or terrify, it should be considered that terrorists can hire hacktivists to execute a certain objective in the terror campaign. "The modern terrorist will be able to do more damage with a keyboard than with a bomb" (Computer Science and Telecommunications Board, 1991).

A number of articles have been published on how cyberterrorism can be combatted in the new domain of cyberspace (Weimann, 2005), (Stewart, 2015). An understanding of the motives and ideology of terrorists and cyberterrorists are required; the enemy and the emanating threat need to be defined. Cyberterrorism offers several benefits to a terrorist: it is definitely cheaper than traditional terrorist methods, it is anonymous in nature, the attack surface is enormous, it can be conducted remotely, and attribution is extremely difficult.

2. Military Counterterrorist and Cyber Operations

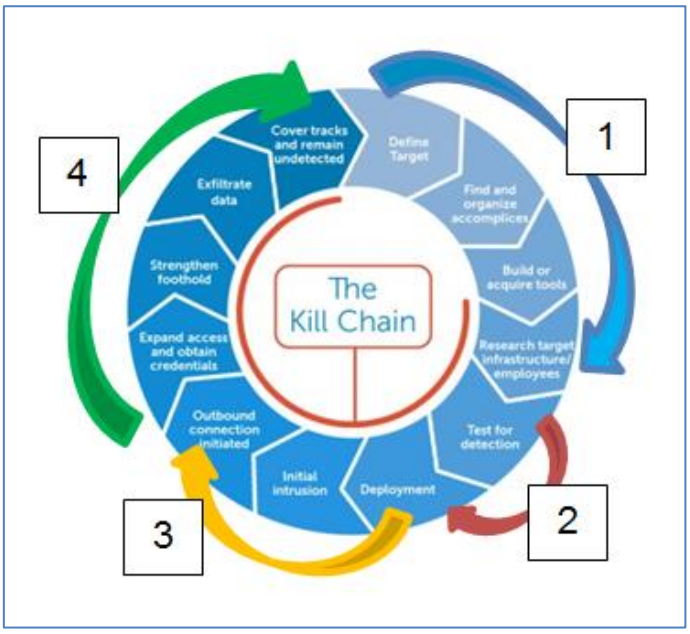
Military counter terrorist operations "incorporate the practice, military tactics, techniques, and strategy that government, military, law enforcement, business, and intelligence agencies use to combat or prevent terrorism" (Wikipedia, unknown). There has been a terrorist migration to the Dark Web due to the risk of being monitored, traced and found on the Surface Web (Weimann, 2015). Cyber counter terrorist military operations can augment physical military counter terrorist operations, enhancing the capability by collecting and analysing possible data that can assist in the apprehension, possible proactive approach to a terrorist attack or a cyberterrorist attack. Lisa Monaco, the United States Homeland Security Advisor to President Obama, indicated that the US counterterrorism strategy will be applied to counter cyberattacks as well: "There are structural, organizational and cultural shifts that were made in our government in the counter terrorism realm that also apply to cyber" (Bennett, 2015). At the center of the United States strategy is a new agency, the Cyber Threat and Intelligence Integration Center (CTIIC), with the aim of integrating cyber intelligence information and sharing it with civilian agencies. Monaco said this center will do for cyber counterterrorism what the National Counterterrorism Center does for terrorism (Pellerin, 2015).

There are multiple approach avenues in which data can be collected from various Internet spaces, and many of these methods are well recorded. Free software can be used for collecting certain information especially on the Surface web; this is referred to as Open Source Intelligence (OSINT). However, for delving into the Deep and Dark Web more intensively there is a need for sophisticated methods and cyber tools. One of the obstacles in countering terrorism activities on the Dark Web has been the lack of methodology to collect and analyse Dark Web data (Weimann, 2015).

There are an abundance of websites that are invisible to the normal Internet user, as described in section 1.1, and criminals and cyberterrorists can use the Deep and Dark Web to hide websites and services to execute cyber actions. There are multiple technologies that can anonymise Internet users and they are often used; however, these technologies have also facilitated organised crime (Kriechbaumer & Nath, 2015). Some progress has been made in the development of techniques to counter cyberterrorism, for example, DARPA (Defence Advanced Research Projects Agency) stated in 2014 that MEMEX, software originally developed to monitor human trafficking on the Deep Web, can be used to improve the of cataloging Deep Web sites and to track other illegal activity on the Deep Web (Weimann, 2015).

2.1. The "Cyberterrorist Kill Chain" Methodology

An adopted methodology that can be used for cyber counter terrorist operations is the Kill Chain methodology (Schmidt, 2013). A kill chain is a military methodology describing a sequence of actions, the "kill chain", that has to be completed by an adversary to attack own forces. A defence will focus on the weakest links in the chain (iconix). This methodology has been modified into a so-called "Cyber Kill Chain" for Advanced Persistent Threat defences by Lockheed Martin (Hutchins, Cloppert, & Amin, 2011), based on the premise that an attack has an operational life cycle to gather information. This process allows cybersecurity practioners to counter advanced cyber threats and can, in turn, be adapted to search for cyberterrorists in the Deep and Dark Web. The adapted process is presented below. It has been divided into four stages as depicted in Figure 1.



Four Stages

Stage 1: Collect information and define the target. Appreciate a terrorist group's profile picture, where are they, who are they, who is connected to who, what is the intention, what systems/technology are used.

Stage 2: Test tools for detection: Evaluate available tools through simulation and emulation.

Stage 3: Deploy. Specially built or acquired cyber collection tools.

Stage 4: Exfiltrate data. Collect the data and analyse for suspected terrorist / cyberterrorist acts.

Figure 1: Cyberterrorist Kill Chain Methodology (adapted from (On the Net Gang, 2013))

The first phase may be applied before a terrorist threat is suspected, that is when data is being gathered to monitor the environment. It is also used to gain more information on a suspected target. During the collection of data, it is possible that the cyberterrorist has left behind a digital fingerprint, e.g. through fake social media (SM) personas when using social media sites. This allows opportunities for counter cyberterrorist analysts (phases 2 to 4) to search for data, manipulate cyberterrorist social media accounts, and infect devices to exfiltrate (egress) information in ways which may cause them to expose both individual and collective organisational vulnerabilities (Brennan, 2012).

The monitoring of the Dark web is thus essential. Weimann (2015) summarises recommendations by Michael Chertoff and Tobby Simon presented in a special report in 2015 entitled "The Impact of the Dark Web on Internet Governance and Cyber Security (www.cigionline.org/sites/default/files/gcig_paper_no6.pdf). These recommendations include

- Profiling of users on the Dark Web as well as their activities;
- Semantic analysis to track future illegal activities and malicious actors;
- Hidden service monitoring of new sites for ongoing later analysis; Social site monitoring to spot message exchanges containing Dark Web domains;
- Monitor user data by looking for connections to non-standard domains.

2.2. Techniques

Internet users reveal a lot of information in which users can be tracked via their online activities (Kriechbaumer & Nath, 2015). The following techniques/methods/practices enabling the tracking and identifications of users using the internet are discussed by Kriechbaumer and Nath:

- The content: posted information on social media sites that are using non encryption methods or emails sent who has access to the relevant network.

- IP Address: every device needs one to communicate with the internet; however it can be challenging with dynamic IP addresses as IP are shared or reallocated as users connect and disconnect, however ISP and Web site operators record the IPs.
- Cookies: small text files uploaded by a website to a user's device when browsing the internet and used to store or get information of users' activities. This can be passed on to a third party i.e. for advertising purposes.
- Browser fingerprint: some browsers have fingerprinting features that recognise users returning to a website.

Online anonymity systems are developed to execute multiple entry points via a service provider, or an organisation providing a service preventing the capturing and fingerprinting of users online behaviour. Thus some of the online anonymity systems technologies are listed below (Kriechbaumer & Nath, 2015):

- The TOR (The Onion Router) consists of two main parts namely, approximately 6000 computers forming a global network of nodes, secret entrance nodes called "bridges" (which is difficult to block) and free software running on users' computers to access the nodes. The data is encrypted in multiple layers, from the origin through the nodes - of which one layer of encryption is removed between the nodes until the destination. Each node is aware of the node before and after it, but not the other nodes. Any single node is known to at most two other nodes and unknown to the remaining 5997 nodes; TOR thus hides the IP and other identifiers of a general user of the internet. TOR software is available on the internet as well as for mobile phones. TOR thus allows users to access the internet anonymously and publish anonymous Web sites as TOR Hidden Services (THS) referred to as ".onion". To access THS is not simple because it is not indexed. TOR does have search engines such as "ahmia.fi" but some THS can be accessed through TOR on the open Web (Surface web) by replacing .onion with "tor2Web.org" (Kriechbaumer & Nath, 2015). Neither owners nor content is listed in the THS URL; it will be a bunch of numbers and alphabetical letters that does not make sense as described in section 1.1. Not all THS are published and they change rapidly, thus analysis is a snapshot in time. Note that approximately 45000 unique .onion addresses are created every day (TorMetrics)
- The Invisible Internet Project (I2P) is similar to TOR, but is designed for using hidden Web sites. There is a definite shift towards I2P, due to it offering a range of improvements such as integrated secure email, file storage and file sharing plug-ins, integrated social features e.g. blogging and chat facilities (Walsh, 2015).
- FreeNet is a tool used for sharing files anonymously by splitting the file into encrypted blocks and storing it at other FreeNet users. The Freenet Project offers similar functionality as TOR and I2P but it also allows for the creation of private networks which can only be accessed by people who have been manually placed on a 'friends list' (TurboFuture, 2015).
- FAI (Free Anonymous Internet) is based on "blockchain" technology (hardened against tampering); it is similar to a social media homepage, which allows users to exchange information anonymously (Walsh, 2015) (Walsh, 2015).
- ZeroNet is a new system which is based on torrent technology, combined with Bitcoin encryption (TurboFuture, 2015)

Due to the above, a deduction can be made that cyberterrorists are using anonymity systems to communicate and launch cyberterrorist attacks. However, terrorist groups like to claim responsibility for attacks. Cyberterrorists will also use THS to share information without revealing their location/name/and content (using codes or different languages), but the Surface Web offers other stealth open communication that terrorists can use (Kaplan, 2009):

- Steganography: hidden messages in videos on multimedia platforms such as YouTube or a posted video on social media i.e. blogs; and
- "Dead dropping": saving information in email drafts in an online email account that can be accessed by anyone in possession of the password.

Hence by using online anonymity systems for cyber counter terrorist operations, it allows the operation to hide specific IPs and access hidden potential cyberterrorist sites or others sites of interest, thus enabling covert online surveillance. However, this task is not as easy as browsing and the collection of information. Online anonymity systems either direct users to automatically download botnets, adult content contraband or weapons which ascribe to about 44% of sites, while the other 56% of sites are for politics, academic research and other topics (Kriechbaumer & Nath, 2015). There are also other techniques that can be used for traditional intelligence collection, for instance the creation of whistle blower sites using THS to expose cyberterrorist or criminal activities which are encrypted and anonymous. Using different tools and techniques, it will allow cyber counter terrorist operations to reach different depths of the Deep Web. Custom built crawlers using linked crawl techniques and APIs can be used to access the hidden website listings which are not indexed (Sui, Caverlee, & Rudesil, 2015). Note that there are also plenty of pay-to-use data bases in which cyberterrorists can store information, and access is only through subscription, creating legal challenges for law enforcement and military especially due to privacy.

The following techniques can be used to de-anonymising online anonymity systems users (Kriechbaumer & Nath, 2015):

- Exploit technical limitations: Online anonymity systems do trade-offs between security and usability for the user's experience to be enhanced.
- Exploiting users mistakes: "Human is the weakest link" users using the same persona or fake persona or make distinct comments on both hidden services and the open Web that allow them to be identified by non-technical means.
- Normal covert intelligence gathering: Who is associated with whom on social media both in hidden chat services and the Surface Web?
- Sites of interest: When looking for links to a cyberterrorist a starting point would be weapon sites, religious extremist sites, political radicalism sites and hate speech sites.

3. Military Cyber Counter Terrorist Operations

The terrorist threat will be determined by a higher strategically level of national security in which counter intelligence will play a vital part. Gaining knowledge about the adversary will lead to collecting information and defining the target (cyberterrorist organisation) and his infrastructure using the Cyberterrorist Kill Chain methodology (see Figure 1) directed to the Deep and Dark Web. Similarly, the terrorist organisation which has a specific ideology to launch a terrorist operation can possibly use cyberterrorists to launch cyber-attacks against National Critical Infrastructure (NCI), Critical Information Infrastructure (CII), Social Media (SM) and Media as well as other cyber sites to inflict destruction for the effect of fear and terror, through the Deep and Dark Web. Once data of cyberterrorist actions or plans are extracted from cyberterrorists' hidden sites or their devices are being manipulated, this information will be analysed and targeted terrorists will be identified for military counter terrorist force structure elements to apprehend and capture. The cyber response will, however, be determined as part of the military counter terrorist operation. The apprehension of cyberterrorists is not limited to nations' borders. The concept of augmenting the military counter terrorist operation with the use of cyber counter terrorist operations is depicted in Figure 2.

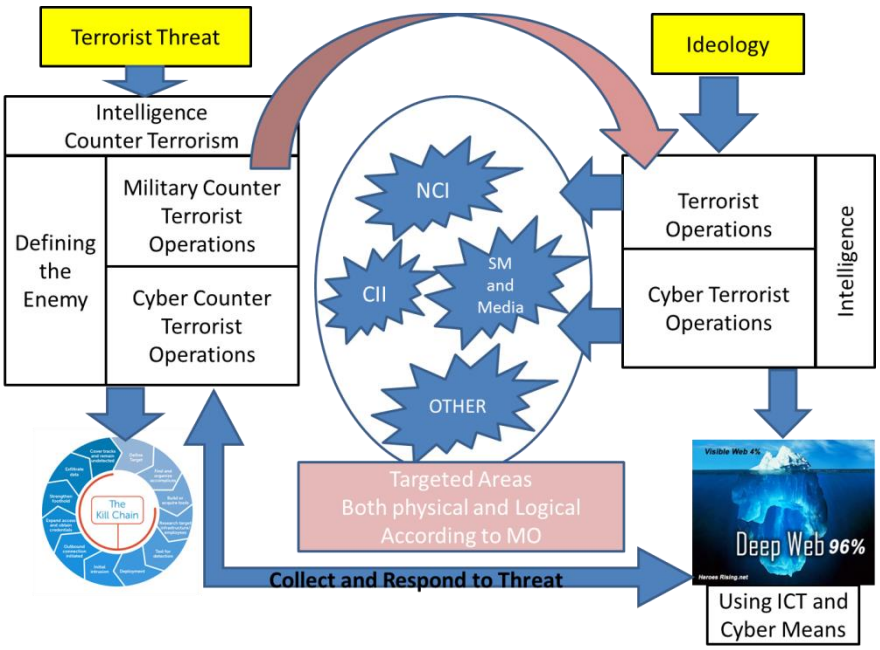


Figure 2: How Cyber Counter Terrorist Operations interlinks with military counter-terrorist operations

A military cyber counter terrorist operation will be co-ordinated in conjunction with a military counter terrorist operation. Thus, from a national security level the collection and monitoring of a cyber environment for situational awareness, for any nation state, to have a picture of the security environment is imperative. The legality of this is not covered in this paper. Military Intelligence through its processes will make use of the cyber environment to collect cyber information and to convert it into cyber intelligence. The cyber intelligence will assist in giving certain indicators of a terrorist threat, thus this intelligence will be combined with the physical counter terrorism intelligence to identify

the threat and targets. With this in mind the Kill Chain methodology adaption for stage 1, as discussed in Figure 1, can be seen as been utilised on different levels of military operations, namely strategic, operational and tactical for military cyber counter terrorist operations. The focus will then shift to different levels to target the different levels of terrorist operations, be it an organisation, group or individual. The focus for a cyber counter terrorist operation will be dependent on the different levels of a military counter terrorist operation. The latter three stages in the Cyberterroism Kill Chain methodology can thus be executed to exfiltrated data of cyberterrorists and terrorist activities.

4. Conclusion

In this paper the authors explored the use of Deep and Dark Web to assist military counter

terrorist operations. It has been found to be feasible means regardless of one's interpretation of what cyberterrorism is. The Deep and Dark Web has been used successfully in other areas of law enforcement (Cook, 2016). This is to be seen as an intelligence function for collection and processing of information, especially within the Dark Web. The level of response will depend on the level of threat to possibly launch offensive actions within the cyber domain. The authors also adapted the Cyber Kill Chain methodology to present an approach on incorporating cyber counterterrorism within traditional counterterrorism operations, and presented a rudimentary approach. Future research should be done on the cyberterrorist's psyche and Deep Web crawlers.

5. References

Bennett, C. (2015, October 2). White House brings counterterrorism strategy to cyber. Retrieved August 2016, from The Hill: http://thehill.com/policy/cybersecurity/232318-white-house-brings-counterterrorism-strategy-to-cyber-threats

Biddle, P., England, P., Peinado, M., & Willman, B. (Unknown). The Darknet and the Future of Content Distribution. Retrieved March 2016, from https://crypto.stanford.edu/DRM2002/darknet5.doc

Brennan, J. (2012, March 12). UNITED STATES COUNTER TERRORISM CYBER LAW AND POLICY, ENABLING OR DISABLING? Retrieved March 2016, from https://www.google.co.za/?gws_rd=cr,ssl#q=UNITED+STATES+COUNTER+TERRORISM+CYBER+LAW+AND+POLICY%2C+ENABLING+OR+DISABLING%3F

Collin, B. (1997). The Future of Cyberterrorism. Crime and Justice International, 15-18.

Computer Science and Telecommunications Board, N. (1991). Computers at Risk: Safe Computing in the Information Age. National Academy Press.

Cook, J. (2016, 08 14). Here are the methods police use to catch 'deep web' drug dealers. Retrieved September 28, 2016, from Business Insider, UK: http://uk.businessinsider.com/methods-that-police-use-to-catch-deep-web-drug-dealers-2016-8

Dictionary Free, t. (Unknown). www.thefreedictionary.com/cyber-terrorist. Retrieved March 2016, from The Free Dictionary: www.thefreedictionary.com/cyber-terrorist

HiddenWiki, t. (2013, May 3). What is the Hidden Wiki? Retrieved August 2016, from HiddenWiki.net: http://www.thehiddenwiki.net/

Hutchins, E., Cloppert, M., & Amin, R. (2011). Intelligence-Driven Computer Network Defense. Leading Issues in Information Warfare & Security Research, 1.

Iconix. (n.d.). Kill Chain. Retrieved August 2016, from iconix: http://sp-guard.iconix.com/kill-chain/

Jalil, S. A. (2003). Countering Cyber Terrorism Effectively - Are we ready to Rumble. Retrieved March 2016, from https://www.giac.org/paper/gsec/.../countering-cyber-terrorism.../105154

Kalomni, R. (2012, June). Dark Net How To Get Started. Retrieved March 2016, from http://www. askthe computer guy.com

Kaplan, E. (2009, Jan 8). Terrorists and the Internet. Retrieved September 28, 2016, from Council on Foreign Relations: http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005

Krasavin, S. (Unknown). What is cyber terrorism? Retrieved March 2016, from Computer Crime Research Centre: http://www.crime-research.org/library/Cyber-terrorism.htm

Kriechbaumer, T., & Nath, C. (2015, March). The darknet and online anonymity no 488. Retrieved August 2016, from www.parliament.uk: http://researchbriefings.files.parliament.uk/documents/POST-PN-488/POST-PN-488.pdf

Mirriam Webster, t. D. (n.d.). Terrorism. Retrieved from Mirriam Webster Dictionary: http://www.merriam-webster.com/dictionary/terrorism

On the Net Gang, t. (2013, 08 12). Cyber Kill Chain: Hope or Hype? Retrieved from On the Net Gang.

Pellerin, C. (2015, February 11). New Threat Centre to Integrate Cyber Intelligence. Retrieved August 2016, from U.S. Department of Defense: http://www.defense.gov/News/Article/Article/604093

Rouse, M. (2010, May). TechTarget. Retrieved August 2016, from Cyberterrorism: http://searchsecurity.techtarget.com/definition/cyberterrorism

Schmidt, K. (2013). Cyber Kill Chain: Hope or Hype? Retrieved March 2013, from On The Net Gang: http://www.onthenetgang.com/2013/08/cyber-kill-chain-hope-or-hype.html

Stewart, S. (2015, October 22). Stratfor. Retrieved August 2016, from Security Weekly: The modern terrorist will be able to do more damage with a keyboard than with a bomb.

Sui, D., Caverlee, J., & Rudesil, D. (2015, Oct). The Deep Web and The Darknet. Retrieved August 2016, from https://www.wilsoncenter.org/publication/the-deep-web-and-the-darknet

TechTarget, t. (n.d.). Cyberterrorism. Retrieved from TechTarget: http://searchsecurity.techtarget.com/definition/cyberterrorism

TorMetrics. (n.d.). Retrieved August 2016, from Unique .onion addresses: https://metrics.torproject.org/hidserv-dir-onions-seen.html

TurboFuture. (2015, April 18). Retrieved August 2016, from A Beginner's Guide to Exploring the DarkNet: https://turbofuture.com/internet/A-Beginners-Guide-to-Exploring-the-Darknet

Vocabulary.com Dictionary, t. (2016). Cyber-terrorist. Retrieved March 2016, from Vocabulary.com: https://www.vocabulary.com/dictionary/cyber-terrorist

Walsh, D. (2015, February). How to access the Deep web or DarkNet - A Beginners Guide. Retrieved March 2016, from http://cryptorials.io/how-to-access-the-deep-web-or-darknet-a-beginners-guide/

Website Magazine, t. (2014, July 22). Do you know how big the internet really is? Retrieved August 2016, from Website Magazine: http://www.websitemagazine.com/content/blogs/posts/archive/2014/07/22/do-you-know-how-big-the-internet-really-is-infographic.aspx

Weimann, G. (2005). Cyberterrorism: The Sum of All Fears? Studies in Conflict & Terrorism,, 28, 129-149.

Weimann. G. (2015). Going Dark: Terrorism on the Dark Web. Studies in Conflict & Terrorism, 39(3), pp. 195-206.

Wikipedia, t. (unknown). Counter-Terrorism. Retrieved March 2016, from Wikipedia: https://en.wikipedia.org/wiki/Counter-terrorism