Exploratory Research for the Response of the Dark Web and TERROR Crime

Yang Seung-don¹
Kimpo University, Kimpo, Republic of Korea

Park Woong-shin²*
Dongseo University, Busan, Republic of Korea

Abstract

Everyone knows that the Internet is widespread, but it’s more extensive than you know and contains information you don’t know. This is not because you are not familiar with ICT. It’s an area that can’t be found on its own, and this is the dark web.

This study examined the relevance of various terrorist crimes on the dark web, especially air terrorism. In other words, starting with a review of the structure of the Internet, including an understanding of the dark web, the terrorist trends of recent years have been examined. Lastly, three major countermeasures were proposed.

As a result of the study, the first is to stop terrorist criminals from acquiring the violent means through the Dark Web, and the second is to stop the spread of political, religious and ethnic purposes, which are important elements of terrorist crime. Finally, the value of freedom of expression that can arise through this was once again enhanced. The first thing to consider when considering a terrorist crime is to acquire the means to commit such a terrorist crime on the dark Web. And there is a need to create a department dedicated to the development of a social consensus on the social risks of terrorist crimes (including aviation terrorism) on the Deep Web and the Dark Web. Furthermore, the penetration of Internet-savvy terrorists into the dark Web will facilitate international countermeasures to find solutions to counter illegal and evil activities, but it should not undermine the freedom of legal and legitimate expression.

[Keywords] Deep Web, Dark Web, Terror Crime, Freedom of Speech, Act of Instigation to Terrorism

1. Intro

The Internet we rely on every day consists of three areas. It is a surface web that is commonly accessed by Naver, Daum, and Google, a deep web that is not covered by the surface web, and finally a dark web. The dark web is an area that is intentionally concealed as part of the deep web and cannot be accessed by ordinary Internet access programs. An area that exists online but cannot be accessed unless an exact Uniform Resource Locator (URL) is used.

Of course, this dark web itself is a value-neutral area, so there is no direct link to crime. The various forms of positive websites that exist on the dark web prove this. However, due to the closeness and difficulty of access to the dark web itself, criminals have begun to parasitize on the darkly. Especially, not only are there various forms of illegal trading, but also active crimes are taking place at the Dark Web Marketplace where they are gathered. While the forms of crime on the dark web are indescribably diversified, this town is particularly interested in reviewing the status of terrorist use of the dark web. Of course, crimes that can occur on the dark web are so diverse that crimes on the dark web should not be assumed solely as terrorist crimes. In particular, the issue of distributing child pornography on the dark Web, which has
shocked the nation recently, is no less serious than a terrorist crime. However, in this study, we want to focus on the problem of the use of the dark web by terrorists. In general, the greatest characteristic of dark web crime can be seen as anonymity and liquidity\cite{1}, as the type of crime that best suits these characteristics can be seen as terrorist crime.

In this study, we will examine the true nature of the dark web and its relevance to air terrorism in particular, and suggest possible countermeasures against air terrorism based on the dark web. To that end, first seek a general understanding of the dark Web and look at terrorist criminals' tendency to avoid the dark Web, which has been intensifying since the 2016 Paris attacks in France. In addition, we will review the types of terrorist crimes that can occur on the dark web.

2. The Dark Web, the New Crime Gateway

2.1. Surface web, deep web, and dark web

2.1.1. What is the surface web?

The Internet we use every day consists of two main areas. It is the surface web and the deep web. The surface Web, the most familiar Internet area for ordinary users, includes information accessed using standard search engines such as Naver and Google. Information obtained from these sites is presented to the searcher without any restrictions. Assuming the Internet is a giant iceberg, the top of the iceberg that most people can see is the surface web that can be searched by search engines like Naver and Google. However, most of the Internet is below metaphorical sea levels, is unsearchable, and is not accessible to the general public. And this hidden part of the Internet is the Deep Web.

2.1.2. What is the deep web?

In the early days of the Internet, there was so little information available that it was easily indexed and easily accessible to users. However, things have changed with the increase in Internet use. As a result, information indexing on the Internet was based on queries entered in search engines. Traditional search engines were able to search for static pages, but they were inefficient in searching for dynamic pages. Static pages are linked to other pages of the Internet. Dynamic pages, on the other hand, are linked to specific webpages and can only be retrieved through target queries or keywords. This created a gap between the Internet's static and dynamic web pages and began to widen over time. Thus, in 1994, Dr. Jill Ellsworth used the phrase "invisible web" to express "invisible" information in queries against existing search engines used in that period\cite{2}. Later, in 2001, Web scientist Michael K Bergman coined the term 'Deep Web' in a paper titled "Deep Web: Surfacing the Hidden Value." His definition of the term "deep web" was no different from Elsworth's term "invisible web," but his main purpose was to find automated ways to identify deep-web sites and direct them to questions to see pages invisible on the surface Web. He also aimed to quantify the size of the Deep Web and characterize the quality of content on the Deep Web. Because Bergman's paper was the first extensive study of invisible deep-web and also became widely known in the Web research community, the term deep-web is widely known as the "invisible web," which refers to the unindexed source of the web. Therefore, the term deep web is defined as follows.

- Information on the Internet(Web pages, documents, files, images, etc.) can be found in the
  - Not accessible through direct query of existing search engine.
  - Can only be accessed through target query or keyword.
  - In case it is not indexed or cannot be indexed by an existing search engine.
  - Protected by security mechanisms such as login ID, password, membership registration and fees.

Simply put, information on the Internet that cannot be accessed directly through a
traditional search engine but requires a targeted approach can be defined as a 'deep web' or 'unseen web' or 'hidden web'.

2.1.3. What is the dark web?

The dark web exists in the deep web. While the Deep Web and the Dark Web sometimes look the same, the Dark Web is much more inaccessible, mostly unregulated, and means a smaller portion of information stored on the Internet[3]. A hidden area that can be accessed through a special program(ex. TOR) that supports encryption. It is understood that Deep Web accounts for about 90 percent of content on the Internet, while DarkNet accounts for about 0.01 percent. Recently, a study found that the amount of information circulating on the dark Web increased to 30,000 in 2015 from about 10,000 websites in 2014[4]. Just like the Deep Web, there is no figure for the exact quantity of information or information distributed on the dark Web.

Access to the dark web requires a unique program that supports encrypted channels. This hides the computer's IP address in various layers of encrypted web traffic, such as onions. Encrypted data travels through randomly selected computers via a network known as relay computers and is displayed past the junction point called nodes. Each node is displayed only in the following sequence of systems, and the last node is displayed when the message arrives at the intended destination, thereby maintaining user anonymity[5]. Users who access Darknet through programs such as TOR using this technology can remain anonymous and free from surveillance by third parties.

2.2. TOR - a means of accessing dark web

In order to access the dark web, there are also Internet Project(I2P) and Freenet(Invisible Internet Project), but the most widely used method is to access through TOR. TOR itself is a value-neutral program that is not relevant to criminal behavior. The TOR was produced in mid-1990 by the Defense Advanced Research Projects Agency, which was originally designed to ensure the safe Internet use of U.S. troops stationed abroad[6]. However, as the use of the TOR soon proved to be the use of the U.S. military, the U.S. unveiled it free of charge in the early 2000s. This meant that the anonymity of individuals using TOR was guaranteed, so it was also aimed at promoting information access by people who wanted access to information that was either heavily censored online or locally illegal.

TOR transmits information as it moves data through various "network relays" run by distributed service computing called volunteerer computers around the world[7]. These tor provide very high anonymity by anonymizing websites and operators who have visited, hiding the user's identity and location. This trait has made TOR very popular among darknet users, which is still progressive. The fact that the number of users with direct access to the TOR network increased from about 2 million in 2015 to about 4.5 million in 2018 shows an increasing use of TOR[8].

2.3. Status of crimes on the dark web – dark web marketplace

As its size and usage increase, the dark web offers a variety of services to users. The nature of the services offered on the dark web is a threat to the real world. Most services are illegal, from drugs, weapons and assassins to pornography and money laundering. While these services are prohibited in reality, the anonymity and liquidity provided naturally by these dark Web sites increases the amount of online use. More and more users are attracted to the fact that they can use these services anonymously for their own benefit.

And these forms of crime, the Silk Road, alpha Fey, such as Market, Market Place in mostly made in tail. In other words, it is understood that the online platform was created on the dark web for criminal purposes.

3. Recent Trends of Terrorist Criminals – Evacuation to the Dark Web

3.1. Radicalization of terrorism crime and propaganda

3.1.1. The spread of radicalization in the dark web
Terrorists by taking advantage of the various online platforms in the late 1990s been. In other words, conventional terrorist criminals have anonymously spread their political ideologies and purposes to the general public through websites and SNS accounts.

These activities on the surface web were soon proved to be too dangerous for them, as activities on the cotton web could be monitored and tracked by the intelligence and investigative agencies. In addition, posts related to terrorist crimes is can be deleted by private companies of the area, such as Google. In response, terrorist criminals gave up on scalability and chose to gain anonymity. In other words, instead of giving up many potential customers available on the surface web, they chose anonymity through the dark web to achieve their goals and began to prevent the arrest of human members and the closure of organizations[9]. As such, the Dark Web is like a treasure trove that enables secure communication for terrorists, shares their knowledge and instructions, posts training manuals, and enables online recruitment, planning and behavioral control[10].

For example, an unidentified radical jihadist posted an e-book on the Internet called "How to Survive the West – Mujahideen Guide," where the main theme was to use TOR when searching online for topics on jihadism[11]. The European Union Institute for Security Studies (EUISS) announced that ISIL's activities on the surface are now closely monitored, and many government efforts to eliminate or filter extremist content have forced jihadists to seek new online safe havens[12].

Furthermore, this trend has become more widespread since the November 2015 Paris attacks by IS. In other words, since the 2015 attacks in France, hundreds of IS-related websites have been shut down by an atypical hacker group Anonymous, and in response, IS's media channel Al-Hayat Media Center has posted links to new dark websites in forums related to IS.

The best examples of such terrorist crimes using the dark Web to radicalize ordinary people and turn them into terrorist criminals are the cases of Kim in Korea voluntarily joining ISIS[13] and the case of Tower Hamlets v. B. in Britain. These events are dramatic examples of whether a person who is not yet mature in judgment could have easily become radicalized through propaganda on the dark web[14].

### 3.1.2. Propaganda diffusion in the dark web

Those who support terrorist crimes share related content on various SNS platforms as part of efforts to maximize the impact and relevance of related organizations and support terrorist crime groups. Of course, it is true that ISPs and general Internet service companies have tried to prevent the spread of profunda postings, and that these efforts have reduced terrorist crime postings on the surface Web[15]. But this is on the surface of the Web and, ironically, this effort has prompted terrorists to hide in the dark. And given the characteristics of encrypted chat applications or darknet, such as telegrams, it is rather natural for terrorist criminals to pay attention to them. For example, ISIS' Al Hyatt Media Center has posted posts related to the group, with detailed explanations on how to get to the new dark Web site[16]. The posts reflected what had already been posted on other IS sites, which is believed to have been a reaction to the diminished driving force caused by the intelligence and investigative agencies' monitoring of tracking.

However, profiling for terrorist criminals excludes conversion for their political purposes and their membership adoption[17]. Religious conversion and joining terrorist groups are effective only when they are conducted on the public, including intelligence and investigation agencies, but this is because, paradoxically, the possibility of tracking them by intelligence and investigative agencies increases.

### 3.2. Recruitment and education of potential criminals

The recruitment of members of terrorist crime groups does not necessarily have to be done through the dark web. Although initial contact to recruit more members is possible
even on surface web-based platforms, it is currently happening through dark web where anonymity is guaranteed due to the risk of exposure to information and investigation agencies. However, there are not many confirmed cases of terrorist recruitment through the dark web. Recently, a BBC reporter in Britain attempted to infiltrate a terrorist organization in 2015. A BBC reporter who wanted to infiltrate the terrorist group tweeted that he contacted Junaid Hussain in 2013 to discuss joining the terrorist group. After Junaid Hussain was later killed in 2015 in a secret operation by intelligence authorities, he contacted another unnamed recruit and attempted to disguise himself as a cryptographic messenger via the Darkweb. The recruiters then taught not only recruitment but also active terror crimes in London, an example of empirical evidence that terrorist groups are hiring more members through the dark web[18]. In addition, the training and training of the members who have been filled through the preceding procedure are similar. In other words, while the methodology for carrying out terrorist crimes is also possible through the surface web, in the reality of continuous deletion of government and private domains, criminals who do not acquire them can obtain them from the dark web. As such, the Dark Web does not require a physical location for plotting crimes against terrorist crime groups, allows members of the organization to carry out crimes through training or experience, and exists as a target for overcoming intelligence and investigation agencies.

3.3. Financing of terrorist crimes

The key issue in responding to terrorist crime on the dark web is terrorism funding. Internationally, terrorist funds are not only regulated by the Convention on the Suppression of the Financing of Terrorism, but are also regulated by law enforcement authorities, including the Financial Intelligence Unit (FIU), at the level of individual countries. Recently, however, there has been a vacuum in the existing anti-terror system, which is attributable to the activation of Bitcoin and other cryptocurrency currencies. Of course, when Satoshi Nakamoto, founder of Bitcoin, the flagship of cryptocurrency, invented bitcoin in 2008, it would not have been what it originally. However, terrorist crime and the dangerous synergy effect of the dark web are becoming a reality. Cryptographic money, which has the same value as cash, is widely used not only for ordinary criminal crimes, but also for terrorism crimes, especially for the collection of terrorist funds, transfer of funds, and illegal purchase of weapons[19]. What makes this stark is the posting titled "Bitcoin Wa Sadaqat al-Jihad," which was posted online in 2014[20]. It urged the use of cryptocurrency such as bitcoin as a means of bypassing Western financial systems, which promote economic support for jihad and restrict donations to it through restrictions on the financial system. In addition, in 2015, Singapore’s security company S2T found concrete evidence that a terrorist organization known to be associated with IS and operating in the Americas was recruiting bitcoin, as well as that some of the perpetrators of the November 2015 terrorist attacks in Paris, France, prepared the crime through donated bitcoin. Against this backdrop, the European Union's Institute for Security Studies has published a study showing that people who sympathize with terrorism are believed to be using Bitcoin to transfer terrorist funds, and that IS' activities on the dark web will result in greater economic capacity as well as greater efficiency in organizational operations[21]. In November 2017, relatively recent fundraising activities began on the Web site of Akhbar al-Muslimin, a news channel in the Muslim world, and in December 2017 Zoobia Shahnaz, a U.S. citizen, was convicted and sentenced to 20 years in prison[22]. She was accused of transferring $85,000 in bitcoin to four companies - Chase Bank, TD Bank and American Express and providing aid to IS and other terrorist groups.

What can be seen in these cases is that continued evidence of terrorists' use of the dark Web and cryptocurrency has been accumulating, especially recently this trend has surfaced on the surface. And the above cases and other findings mean that the use of cryptocurrency is widespread, not only in terrorist crime organizations, but also in organizations and individuals supporting them.
3.4. Conclusion

As reviewed above, terrorists are moving away from conventional surface-web-based activities and extending their radius of activity to the dark Web. The Internet provides easy, cheap access to a wide range of information and guarantees minimal anonymity. Here, the Dark Web takes a step further and has a strong anonymity at its core. Under these circumstances, it is natural for criminals, including terrorism, to pay attention to the dark Web. This anonymity, in particular, has significantly lowered the bar for transgressions compared to other legal and social norms, which may be why the Internet domain[23], including the dark Web, has become a hotbed of crime. While large-scale terrorist crimes have certainly declined since 2001 as a result of global anti-terrorist attacks, I believe that reviewing the types of terrorist crimes committed on the dark web in the continuous occurrence of small or medium-sized terrorist crimes or their attempted acts will be important in terms of prevention of terrorist crimes in advance. In particular, it can be seen that the type of terrorist crime on the dark web is not only about preventing the spread and spread of terrorist crimes, but also about joining and training potential actors who carry out terrorist crimes themselves. The problem is that responding to crimes on the dark web can be a double-edged sword. This is due to the fact that TOR, the main access tool for the dark web, has a value-neutral nature. In other words, responding to terrorist crimes on the dark web (including the Internet) is in a difficult situation where it is necessary to find the best way to realize the ideal inherent in democratic values of freedom of expression and personal rights while curbing inappropriate Internet use by terrorists.

4. Outro

Below, I would like to conclude by suggesting the possibility of terrorist attacks based on the dark web and policy countermeasures against them.

4.1. Deterrent against obtaining the means of terror crime

The first thing to consider when considering a terrorist crime is to acquire the means to commit such a terrorist crime on the dark Web. In fact, investigators found that the gunman, who was used in the 2016 gun attack in Munich, Germany, purchased the weapons from the dark Web. For example, a site called EuroGuns is an online dark web platform that deals with various arms sales. For example, the AK-47, an assault rifle used by the Kouachi brothers in the 2015 Charlie Hebdo terrorist attack in France, sells for $550. In addition, several documents, such as terrorist handbooks and explosives guides, were available for purchase on Alpha Bay. And the means of terrorist crimes by terrorist criminals include not only guns, explosives, but also forged documents and passport supplies. For example, the Fake Documents Service provided "high quality fake passports, driver's licenses, identification cards, stamps and other products" to customers for use in countries such as the United Kingdom, the United States, Australia and Belgium.

These examples show the need for prevention strategies and tracking of items that could be a means of terrorist crime on the dark web. Since it is virtually impossible to block access to the dark web, developing tracking technology for those who purchase these items from the dark web is necessary. For example, U.S. intelligence agencies are developing and using new investigative techniques to track down terrorist criminals on the dark Web. Network Initiative Techniques (NIT), which are mainly used by the prosecution and the Federal Bureau of Investigation, MEMEX techniques that are commonly used by the prosecution and the Department of Defense, and XKeyscore, which is used by the National Security Agency (NSA). However, even if they are given a court warrant, it is difficult for the investigation to be carried out beyond the scope of the warrant, or the relevance of the criminal charges, in that these methods are online. In addition, public consensus is needed in that it could lead to controversy over the surveillance society, which could infringe upon the people's right to self-
determination of personal information. Terrorists by taking advantage of the various online platforms in the late 1990s been. In other words, conventional terrorist criminals have anonymously spread their political ideologies and purposes to the general public through websites and SNS accounts.

4.2. A deterrent to the propaganda of terror crime

The most distinctive feature of terrorist crime is its political, religious and ethnic purpose[24]. This is distinct from the subjective component of a terrorist crime of intent. According to a recent study, more than one-third of a total of 269 religious terror attacks surveyed in 2018 were affected through the Internet, including the dark Web[25].

In Korea, there was an incident in July 2019 when an active duty soldier tried to join ISIS due to the extremist movement of IS through the Internet and password application. And the case of Tower Hamlets v. B in the UK reviewed earlier could be assessed as a similar event.

There is an abstract danger that a particular purpose, such as this excessive component of terrorist crime, is spreading on the Internet, including the dark web, and it is necessary to block the spread of these extremist ideas in our reality that these abstract risks actually change to specific risks. Of course, under the current law, the Korea Communications Commission can order ISPs to delete certain sites and block access after deliberation by the Korea Communications Standards Commission to regulate the dark Web. However, since harmful information is assumed on the surface web, there is a limit to blocking terrorist-related information circulating on the dark web. Thus, there is a need to create a department dedicated to the development of a social consensus on the social risks of terrorist crimes(including aviation terrorism) on the Deep Web and the Dark Web.

4.3. Consideration of freedom of expression

In order to respond to terrorism on the dark web, one must consider harmonizing the principle of proportionality with the unredeemable value of freedom of expression. In other words, despite the recent recognition that the dark Web is deeply connected to crimes, including terrorist crimes, it should consider that it itself is value-neutral and provides an advantage in the spread of journalists, civic groups and democracy. Thus, the penetration of Internet-savvy terrorists into the dark Web will facilitate international countermeasures to find solutions to counter illegal and evil activities, but it should not undermine the freedom of legal and legitimate expression.

5. References

5.1. Journal articles


5.2. Books


5.3. Additional references


