116-0002
2-20-7 Arakawa Arakawaku Tokyo Japan

ISSN 2423-8376

# International journal of
# terrorism & national security

2019 4(2)

<Index>

J-INSTITUTE

2019 4(2) 1-6 Submission: 2019/11/10, Peer review: 2019/11/20, Accepted: 2019/11/20, Published: 2019/12/30

International Journal of Terrorism & National Security

Publication state: Japan
ISSN: 2423-8376

Publisher: J-INSTITUTE
Website: http://www.j-institute.jp

Corresponding author
E-mail: klitie@semyung.ac.kr

Peer reviewer
E-mail: terrorism@j-institute.jp

http://dx.doi.org/10.22471/terrorism.2019.4.2.01

# A Study on Response Measure against Drone TERROR

**Lee Jae-young**

*Semyung University, Jecheon, Republic of Korea*

## Abstract

*Purpose; Drone has been acknowledged for its application over various areas from agriculture, industry to info-communications and is rapidly being developed and commercialized. Due to the enactment of domestic Aeronautics Law, regulations on drones are eased, hence free flight without a separate approval has become available. Drone is easily purchasable at a low cost and adaptable for purposes through facilitated remodeling and control. Modern terrors are shifting into soft target terrors against many and unspecified persons via various attacking means easily acquirable, and drone terror is increasing in number all over the world. Drone terror is performed by direct attacks upon flights or significant infrastructures using drones controlled to reach a desired location and by explosion, dropping a drone with explosives on-board. No countermeasure and budget are prepared against dramatic increases of security violations by drones around high-security level national infrastructures in South Korea such as airports, powerplants and prisons, the existing security paradigm is not appropriate to deal with the drone terror risks. Therefore, this study suggests a new response measure against drone terrors.*

***[Keywords]* Drone Terror, 4th Industrial Revolution, Anti-Drone, IOT, UAV**

## 1. Introduction

A trailer of a movie to be released on November 2019 presented a drone terror scene. Multiple small drones in crowds flew, identified people with on-board cameras, shot firearms against identified people and caused an explosion by dropping their on-board explosives.

The terminology, the 4th Industrial Revolution, is used as a convergence of manufacturing and info-communication industries in Industry 4.0, and indicates more intellectual and innovative shifts of the society through the convergence of Information and Communication Technology, such as Internet of Things, Artificial Intelligence, Big Data and Mobile, into overall economy and industry. Drone, a major technology to lead the 4th industrial revolution, involves market volume and value rapidly expanding. Drones developed for military purposes were originally used as a missile targets, and now the application has been extended from reconnaissance and attack aircrafts to logistics, traffic control, crime prevention, disaster fire, agriculture, leisure and services. Consequently, production and sales of low-cost drones are keep increasing[1][2]. However, as drone technology develops and its cost gets lower, abusing cases of drones has occurred. Indiscriminate photographing with drones cause privacy infringement. Drones presents low likelihood of being detected, high location accuracy and facilitated production process. Such benefits of drones are increasingly abused in terrors throughout the world.

This study proposes a response measure to deal with drone terrors. This study consists of followings. Chapter 2 observes the definition and the risks of drone terrors. Chapter 3 illustrates foreign drone terror cases and their features and Chapter 4 suggests a practicable response measure against drone terrors after examining anti-drone technology. Then, Chapter 5 draws a conclusion.

## 2. Relevant Research

### 2.1. Definition and types of drone

Terror is defined as “Behavior terrifying enemies or opponents through violence[3]”. terror is differently defined by generations and presents different features by regions. Contemporary terror groups are hardly exposed, forms networks among groups internationally and commit terrors indiscriminately all over the world without any war front. The terror types are diversified into aircraft hijacking, poisonous or biochemical weapon terror and suicide bombing terror against many unspecified persons around aircrafts, subways, cars and city centers[4]. Terror groups committing terrors to achieve political and social objectives would naturally perform efficient and delicate tactics. Reasons of increasing soft target terrors lie in easy steps for an attack, terrifying the world into fear and difficulty in prediction[5][6]. Terror techniques are shifting into tools easily acquirable in daily lives as the means of attacks. By attacking the target at low cost, terror groups may overcome their insufficient finance and achieve maximization of strategic benefits[7]. Therefore, drones at low cost and easily acquirable, convertible for purposes and controllable are used as the mean for attacks.

Drone refers to aircraft or helicopter-shaped military UAV(Unmanned Aerial Vehicle / Uninhabited Aerial Vehicle) which can perform autonomous flight with guidance of radio waves without a pilot. Drones in the early 2000s were used as targets instead of enemy aircrafts for air force planes and anti-aircraft gun, and now are used as military weapons to attack such as reconnaissance, surveillance and anti-submarine attacks[8][9].

Lexical definition of drone terror is ‘the threat to perform illegal violence upon lives and properties, intimidating a specific member, government or the public to accomplish political, social, ethnical and ideological purposes by using flying air vehicles remotely or autonomously controlled via aerodynamic force, but without a person’[7].

Drone terror is largely segmented into two sections. First, it is to use drone as a direct mean of attack. This is the simplest way of drone terror, directly attacking infrastructures or people, or damaging aircraft engines as if a bird strike. Second, it is to utilize loading capability of drones. Using drones with high-performance camera to photograph in proximity to critical facilities, to assassinate key figures by loading firearms, explosives, biochemical substance and nuclear weapons or to induce terrors on significant facilities[7][10].

### 2.2. Risk of drone terror

Drone is evolving rapidly over time as a core technology leading the 4th industrial revolution[11]. Various applications such as courier, transportation, agriculture, measurement, marine structure, exploration and security are enabled and their consequent risk has increased. An anonymous IoT expert insisted production of a drone which are equivalent to the one used for the recent Saudi terror by remodeling a domestic commercial drone is available – “If you give me two hours, drones can be turned into a remotely controlled weapon. Drone parts including motors and frames are easily accessible in the market, hence it can be turn into a bomb above our heads carrying dangerous chemical substances through an illegal remodeling”[12]. For drones, acquisition cost is low, they are easily accessible both online and offline and remodeling and control are easy, therefore terrorist members with malicious intentions can abuse them for own purposes. In addition, domestic critical infrastructures are vulnerable to drone attacks Furthermore, the rapidly increasing security violations by drones around high-security level national facilities such as airports, powerplants and prisons are causing difficulties

**Table 1**. Foreign drone terror[7].

| | Location | Content | Characteristics |
|---|---|---|---|
| 2011.09 | The United States | UAV with C4 was planned to attack US Department of Defense and the Capitol, yet failed due to precognition by FBI | - Drone length 1.5~2m, Max speed per hour over 160km, 2.3kg explosives are to be on-board<br>- Follower of Al-Qaeda<br>- First attempt of UAV terror |
| 2015.05 | Japan | Opposing against nuclear powerplant reactivation, small drone with radioactive substance is dropped to the roof of Cabinet Office | - Radioactive substance, not firearms or explosives on-board<br>- Security vulnerability to small drones is exposed |
| 2016.11 | Iraq | Suicide drone attack by IS caused 4 soldiers and civilian casualties | - First case of IS attacking the West by drones<br>- Commercial micro drones are used for terrors |
| 2018.08 | Venezuela | Assassination attempt upon the president, Nicholas Maduro, by a drone with explosives | - First assassination attempt to a head of state by drones<br>- 2 commercial micro drones with 4kg explosives on-board<br>- Implication of terror risks by multiple drones |
| 2018.10 | France | Threat of drone terrors by IS in response to blindage construction around Eiffel tower by city of Paris | - Use of drones for the means of attack to spread social disorder and fear |
| 2019.09 | Saudi Arabia | Drone bombing attacks on two world’s largest oil production infrastructures of ARAMCO, a Saudi Arabian state-owned oil company | - Use of drones to terror against critical state infrastructures<br>- Use multiple small drones for application of a drone crowding<br>- 3~4kg explosives on-board |

from unprepared measures and budget, still the existing security paradigm is inappropriate to respond to drone terror risks. Drone, being an important mean of terrors, should be regulated as an unconventional tool of war, not as a mean to contribute to establishing prosperous societies, thus relevant regulations and preventive measures should be prepared[13].

## 3. Drone Terror Cases and Analysis

<Table 1> is a summary of contents and characteristics of foreign drone terror cases.

Observing foreign drone terrors, first commercial micro drones are used for terrors. Commercial micro drones can easily be purchased online and offline at a low cost. Furthermore, as if the drone terror in Japan, a drone was able to fly to Cabinet Office, and presents low likelihood of being detected, considering the drone was left for 13days over the roof. Second, loading function of drones is utilized. Drones can close-up critical infrastructures by mounting a high-performance camera, drop explosives at any desired location and crash towards a destination with dangerous substances such as radioactive material on-board. Moreover, compared to suicide bombing terrors, no sacrifice of an attacker is required for an attack. Third, in the case of drone terror in Saudi Arabia, if small drones are utilized in crowd, their efficacy can be maximized. Even if several drones are incapacitated by shotguns, it is not sufficient to defend against drone crowding, hence the drone terror may be successful.

## 4. Response Measure against Drone Terror

Having drone terror risks spread, ‘Anti-drone’ has caught an attention. Anti-drone is to incapacitate illegal drones causing problems. Anti-drone can be classified into two, the passive, regulating drones by laws and the active, performing direct measures to illegal drones. Passive measure is limited to restrictions on self-programming, safety management and laws, hence becomes invalid if illegal use of drones are enforced. Active measure is to detect illegal drones, capture them for incapacitation or crash them, yet damage to other equipment, facilities and people may be caused despite its preliminary prevention against illegal drone utilities[7][14][15].

Anti-drone is a defensive technology, including regulations and safety management, against illegal drones with the notion to perform defense and attack simultaneously, and is to effectively control operations and utilizations of the drones by real-time monitoring and interrupting flight of the illegal drones in a preliminary manner via all sorts of means including regulations, drones and radio waves, at the stages prior to take-off, flight and landing[14]. Anti-drone technology consists of 3 stages – detection, identification and incapacitation. Small object entering a specific area is detected, whether it is a drone is identified and if it is a drone, it is incapacitated to eliminate risks.

Technology to detect drones mainly uses sensors, and there are sensors of sound detection, direction finding, image detection and radar detection. Detection is largely separated into Active and Passive ways. Active method uses self energy-generating radar, an object is detected through reception of reflected signal from the object, when the radar sends out a radio frequency at a specific band. Radar detection ensures a stable performance regardless of climate, temperature, and day-and-night, and has an advantage of long maximum detection range. However, it is costly for production, purchase and introduction, issues of signal interruption with other systems should be considered as a self signal-generating unit, hence institutional approval and support by the government are required – allocation of frequency band for operation. Passive is to recognize characteristics of drones. It includes sound detection method detecting particular noise from propeller rotations during drone operations and direction finding method predicting locations of controller and drones by detecting signal directions of frequency being transmitted and received within control signal(2.4GHz band) and image signal(5.8GHz band) between the two entities. Direction finding method has an advantage to locate the controller unlike other measures, yet is ineffective in city centers where many WiFi are installed as its control signal and WiFi frequencies are the same. In addition, if drones perform autonomous flight using GPS, the method becomes ineffective, thus sound detection and image detection methods are additionally installed to complement the weakness[7][14][15].

Both Active and passive methods has own strengths and weaknesses, thus should be operated complementarily – radar detection for remote objects, direction finding, sound detection and image detection for any objects in blind spots – for effectiveness.

If a detected object is identified as an illegal drone, the drone should be plunged, destroyed or landed for incapacitation. Ways to incapacitate are jamming, destruction and capturing. Jamming is to release jamming signal into the most critical control signal band(ISM 2.4GHz) to have the drone control unavailable. However, drones performing autonomous flight with GPS signal would not be incapacitated despite of jamming and can continuously fly to its destination. Furthermore, ISM band is the frequency frequently used by the private, it may cause a damage to civilians. Hence, institutional support by the government is required for implementation of jamming units in terms of signal outgoing duration, signal output and operation area[11][15].

Ways to destroy drones are to physically destroy them, firing shotguns against approaching illegal drones, burning the drones by shooting razor beam and using another drone to crash into the illegal drone. Compared to jamming, they are more certain methods to plunge the drones, however risk of secondary damage arises and shooting a rapidly maneuvering drones with shotguns and razor beam is difficult[11].

Last method to incapacitate drones is to capture them. Training eagles, using drones with wire net and using wire net fired from the land are the methods to seize the illegal drones. However, to train eagles, the eagles may highly be injured, the drones with net are not easily applicable for drones maneuvering at high speed and the wire net fired from the land is only practicable when the illegal drones are located closely[11].

Jamming is the most effective way to incapacitate illegal drones. In addition, it is not directly to destroy the drones, hence likelihood of secondary damage from explosives is relatively low. However, jamming is currently illegal in South Korea under the Law of Frequency Management. It is defined illegal as it may paralyze entire local communication, jamming in a private sector to seize illegal drones is unavailable[16]. Domestic anti-drone technology level is at commercializing stage and the anti-drone system should be installed in major governmental infrastructures, however sales and use of jamming units are not available by the Law of Frequency Management, and further any unit testing trials for a research purpose has been defined illegitimate, thus huge restriction exists in anti-drone technology advancement and relevant industry development. Even if the law is amended and relevant units to jamming becomes usable, still, there are problems. Customization of drones with various functions is available and, in particular, illegal drones for terror would not use the commercial frequency, hence jamming to incapacitate them may results in lower efficiency. Consequently, to seize the illegal drones, adequately combined applications of jamming method, destroying methods with shotguns and razor beams and capturing methods using trained eagles and wire net would result in high efficiency.

## 5. Conclusion

Convergence of the cutting-edge information-communication technology and overall economy and industry since the 4th industrial revolution has made the society more intellectual and innovated. Drone, a core technology to lead the revolution, is rapidly evolving and its application range is expanding. Thanks to the advantages – technological development, lightening of parts and low acquisition cost – drone has been utilized in various industries and leisure activities. As drone technology develops, its abuses in terrors has increasingly occurred. Drones are difficult to be detected, has high location accuracy and is easy to be produced and controlled. To respond against drone terrors taking advantages of the benefits, various anti-drone technologies are being developed in different countries.

Anti-drone technology consists of 3 stages – detection, identification and incapacitation. radar detection upon approaching objects, direction finding, sound detection and image detection methods are used, whether the detected object is a drone is identified, then incapacitation is performed if it is a drone. Ways to incapacitate are jamming, explosion and capturing. Jamming the frequency between drone and controller is the most efficient, yet is illegal in South Korea under the Law of Frequency Management. Thus, measures from legislative and policy perspectives are required. However, problems still exist even if the measures are prepared from the views of law and policy.

The key to anti-drone technology is to detect, identify and incapacitate illegal drones. Anti-drone technology has been developed and applied in various countries, yet different strengths and weaknesses are presented in each technology, thus it is assumed that a completely safe and legitimate technology has not been developed. Accordingly, an objective for defending against illegal drones should be set and adequate technological combination is needed. Moreover, further development of anti-drone technology and its application against drone terrors are demanded.

# 6. References

## 6.1. Journal articles

[2] Lee JH & Kim HS. A Study on the Development of Safety Management Method for Toy-type Drones. *Journal of the Institute of Electronics Engineers of Korea,* 55(8), 110-117 (2018).

[4] Jung BS. Case Analysis of Drone Terrorism and Its Efficient Countermeasures. *Institute of Police Science*, 14(2), 147-176 (2019).

[6] Oh SY. A Study on Risks of Terrorism to Analyze Attributes of Domestic Terrorism Factors and Cases. *Korean Journal of Convergence Science*, 7(3), 112-120 (2018).

[7] Jung BS. Case Analysis of Drone Terrorism and Its Efficient Countermeasures. *Institute of Police Science*, 14(2), 149-176 (2019).

[10] Heo J & Jung YG. The Crime with Drone, the Crime Prevention Using Drone. *Korean Academy of Public Safety and Criminal Justice*, 26(3), 358-381 (2017).

[11] Song YS & Shim HS. The Drone Strikes Back: Around a Anti Drone System. *Joint Chiefs of Staff,* 75, 57-64 (2018).

[13] Jun YJ & Lee CB & Lee SH. A Case Study of Recent New Terrorism and Potential Patterns in South Korea. *Korean Security Journal,* 53, 9-34 (2017).

[15] Choi SH & CHae JS & Cha JH & Ahn JY. Recent R&D Trends of Anti-drone Technologies. *ETRI Electronics and Telecommunications Trends,* 33(3), 78-8 (2018).

## 6.2. Thesis degree

[14] IM YS. Exploring Response of Sports Safety Paradigm Change and Drone Terror Threat. Sungkyunkwan University. Doctoral Thesis (2018).

## 6.3. Books

[1] Lee A. Convergence Weekly Tip; Technology-Industry-policy. Convergence Research Policy Center (2017).

[5] Walter R. Origins of Terrorism. The Johns Hopkins University (1998).

## 6.4. Additional references

[3] https://dict.naver.com/ (2019).

[8] https://terms.naver.com/ (2019).

[9] https://namu.wiki/ (2019).

[12] http://www.donga.com/ (2019).

[16] http://www.busan.com/ (2019).

**Author**

**Lee Jae-young** / Semyung University Assistant Processor
B.A. Semyung University
M.A. Semyung University
Ph.D. Chungbuk National University

Research field
- A Study on Improvement of Device Removal Processes from ZigBee Network, Journal of Engineering and Applied Sciences, 13(1) (2016).
- A Study on Utilizing IoT for Preventing Approach Restraining Order Violation, International Journal of Police and Policing, 2(1) (2017).
- A Study on User Authentication and Key Agreement Protocol in Wireless Sensor Network, International Journal of Engineering & Technology, 7(2-12) (2018).

Major career
- 2012~2016. Semyung University, Assistant Processor in Department of Liberal Education
- 2016~2019. Semyung University, Assistant Processor in School of Information & Communication Systems
- 2019~present. Semyung University, Assistant Processor in Department of Liberal Education

2019 4(2) 7-14 Submission: 2019/11/10, Peer review: 2019/11/20, Accepted: 2019/11/20, Published: 2019/12/30

International Journal of Terrorism & National Security

Publication state: Japan
ISSN: 2423-8376

Publisher: J-INSTITUTE
Website: http://www.j-institute.jp

Corresponding author
E-mail: s092724@naver.com

Peer reviewer
E-mail: terrorism@j-institute.jp

http://dx.doi.org/10.22471/terrorism.2019.4.2.07

# Police Countermeasures on the Possibility of TERRORISM Using Drone in South KOREA

**Oh Sei-youen**

*Semyung University, Jecheon, Republic of Korea*

## Abstract

*The study suggests that South Korea is no longer free from drone terrors considering recent increase in terrors using drones, successive North Korea(DPRK) Unmanned Aerial Vehicle(UAV) crashes and unidentified UAV flight above significant government buildings in the past. Hence, this study would observe causes and countermeasures in relation to terrorism risk using drones in South Korea, recognize the terror risk using drones in South Korea through past advanced studies, statistical data and case studies, and propose the following effective countermeasures. Although terrors using drones in Korea has not occurred yet, considering its future occurrence risk, effective countermeasures from this study result may be summarized as followings.*

*First, Anti-Drone Terrorism Law should be enacted separately to prepare against any drone terrors in Korea.*

*Second, to be prepared against drone terrors in Korea, social security network via cooperation among significant national infrastructures, the Ministry of Land, Infrastructure and Transport, the Ministry of Defense and related organizations is required.*

*Third, Anti-drone System should be established to incapacitate illegitimate drones.*

*Fourth, internet websites offering knowledge to produce and renovate improvised explosive devices should be blocked and user authentication with real names is needed for any online drone purchases.*

*Fifth, as drones are privately purchasable online at a low cost, there is also a risk of terror by socially discriminated and prejudiced people such as foreign residents, minorities and the second generation of immigrants. Therefore, improvements in social perception and protection* on them are required.

[Keywords] ***Drone Terror, Police Countermeasures, Anti-Drone System, Utilize Unmanned Aircraft, Anti-Drone Terrorism Law***

## 1. Introduction

Since the drone(UAV: Unmanned Aerial Vehicle) bombing attack on two world-largest oil production units of ARAMCO, the state-owned oil company of Saudi Arabia on September 14th, 2019, the severity of terror and crime risk by drones has spread. In particular, noting the drone terror cases such as a DPRK small drone photographing the Blue House and military facilities and unidentified drones successively appearing near the 1st class national security facilities, including nuclear power plants in 2014 and 2017 – that is, drone terrors are no longer a foreign, but domestic issue committed by entities such as North Korea. Moreover, drones contribute to establishing a convenient and prosperous society as a core technology necessary in our community which would be converged with the overall economy and society in such a 4th revolutionary era – IOT(Internet of Things), AI(Artificial Intelligence) and Big Data. However, if such scientific technologies are abused by crime and terror groups, considerable damage to our society is anticipated to adversely be caused, yet our current drone detection and countermeasure system is still at an early stage. Characteristic changes in international terror, increased number of international drone terrors and increased number of infiltration conspiracy by DPRK via various small UAV development, as results of the recent 4th revolution, presents high drone terror risk in South Korea. In addition, if small and micro UAV development by DPRK is consistently performed and its technology advanced, drones may turn into mass destruction weapon which may load biochemical weapons for terrorism, hence strategies and defensive systems against terrors at national level should be prepared to cope with terrors by small UAV including drones.

Consequently, this study would analyze virtual potential risk of drone terrors assuming a more intensified and diversified form, a type of New-terrorism from the 4th revolution, suggest anti-terror strategies, and thoroughly prepare for possible drone terror risk.

## 2. Theoretical Discussion on Drone Terror

### 2.1. Concept and forms of drone terror

Drone is a flight vehicle navigable without a pilot which fulfills one of the following items stated by the decree of Ministry of Land, Infrastructure and Transport[1]. Federal Aviation Regulation(FAA) and National Aeronautics and Space Administration(NASA) refer a drone as Unmanned Aircraft(UA) and Unmanned Aircraft System(UAS)[2].

Unmanned Aerial Vehicle(UAV) or Unmanned Aircraft System(UAS) is generally flight vehicle navigating along the pre-installed programs via remote control from the land or autonomously navigating, voluntarily recognizing surrounding environment without a pilot, and is a flight vehicle with a full or partial capability of such a function[3]. Other than UAV, UAS is widely used, yet is an integration with another system with all equipment required for UAV flight system and its operation, hence UAV is used to refer the aerial vehicle and UAS is used to refer the entire system for UAV platform operation[4].

Thus, most military and European nations call it unmanned aerial vehicle[5]. while they recently generalized the term into drone.

Drone attack and terror methods by terrorists are widely divided into two. First, it is to use a drone as a direct mean to attack. This, as the simplest attack method, is to attack against facilities and human beings through its physical hits and crashing into aircraft engine as if a bird-strike has occurred. Second, using the loading function of drones, other than direct stroke, terrors on major government infrastructures or assassination of key figures are committed by loading firearms, biochemical substance and nuclear weapons on drones[6]. Recent drone attacks such as oil facility destruction in Saudi Arabia and president assassination attempt in Venezuela are the cases to utilize drones as direct means of terror.

### 2.2. Drone terror risk pursuant to changes in international terrorism condition

Recently occurring terror traits are indiscriminate, not selecting any symbolic facility or figure as a particular terror target, but expanding targets to irrelevant civilians and government multi-facilities, thus are difficult to be predicted nor dealt with. Attack means of such terrors has become much easily available by individuals through learning knowledge to build a drone with explosives loaded, unlike the existing methods – having usage methods of attack means and activities trained at terror camps – after activation of the Internet and SNS.

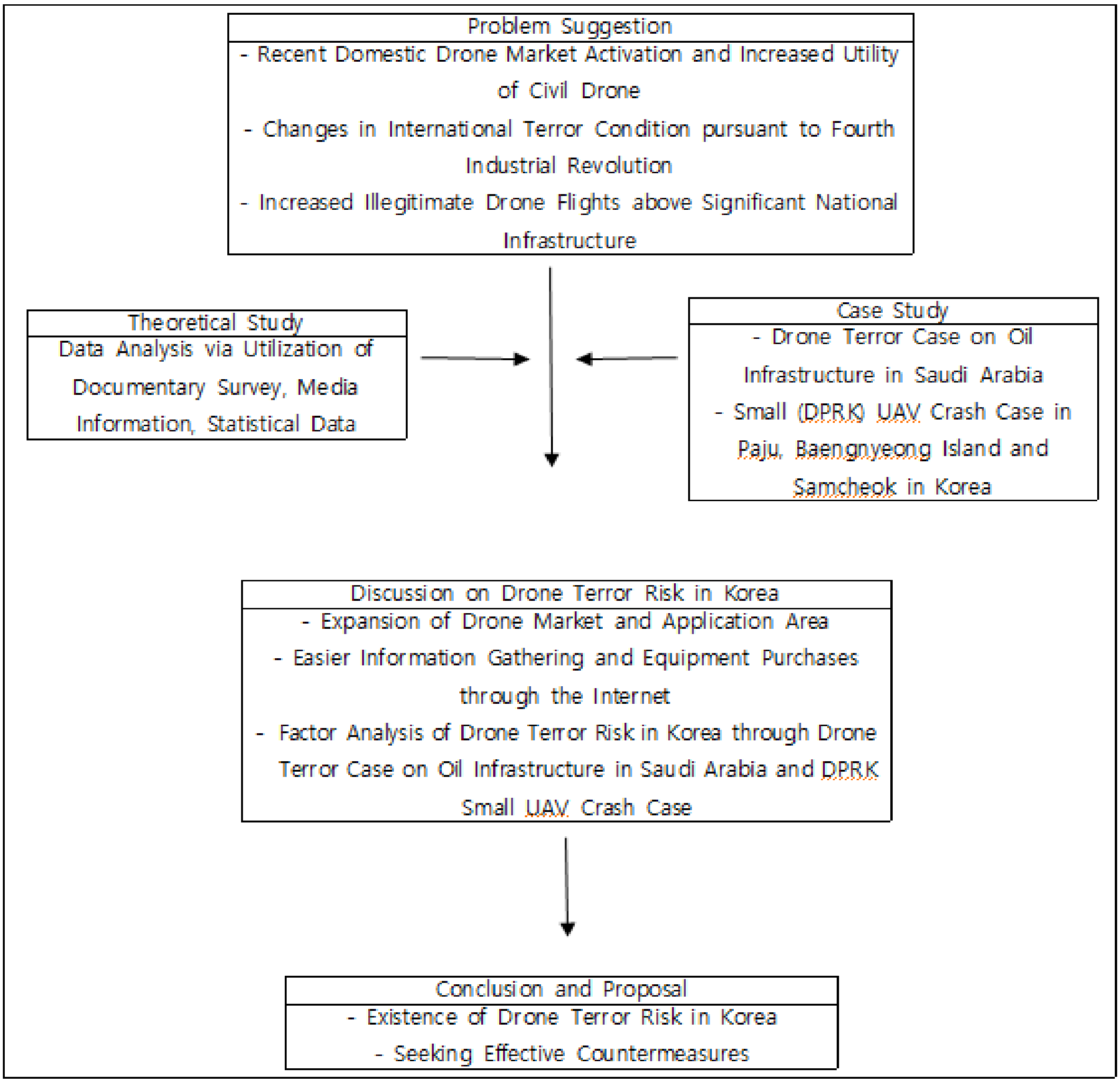
Features of such drone terrors is their availability of huge damage to major facilities with small number of drones as 3-4kg of explosives has become loadable on each drone like an UAV. If the explosives are biochemical or radioactive substance, the damage would be huge. If small UAVs navigate at low altitude in South Korea, as there is no detection radar to detect them, any suicide terror of drones with 1kg explosives or biochemical weapon would practicable in any degree[7]. Second, small detection drones are not likely to be noticed by detection radar, and if more than one drones with explosives are involved for an attack, the attack is difficult to be prevented and would cause huge damage. Third, any person can purchase a drone at a lost cost through the Internet, and its control is easier than other terror means, hence a terror may be committed not only by terrorist groups, but individuals. Fourth, as drone terrors have a benefit of no damage to terrorists, it would more diversely be utilized for high-tech terror, in the future.

Therefore, drone terrors, noting its low cost and easy purchase ability, yet maximized damages and the unsettled situation of anti-drone terrorism system to detect and incapacitate micro-drone terrors throughout the world including our society, have a huge likelihood to become the attack means for terrorists and extremists with social dissatisfaction.

## 3. Analysis of Possibility of Terrorism Using Drone in South Korea

### 3.1. Development process of discussion on drone terror risk in South Korea

**Figure 1.** Process of development of the paper.


Problem Suggestion
- Recent Domestic Drone Market Activation and Increased Utility of Civil Drone
- Changes in International Terror Condition pursuant to Fourth Industrial Revolution
- Increased Illegitimate Drone Flights above Significant National Infrastructure
Theoretical Study
Data Analysis via Utilization of Documentary Survey, Media Information, Statistical Data
Case Study
- Drone Terror Case on Oil Infrastructure in Saudi Arabia
- Small (DPRK) UAV Crash Case in Paju, Baengnyeong Island and Samcheok in Korea
Discussion on Drone Terror Risk in Korea
- Expansion of Drone Market and Application Area
- Easier Information Gathering and Equipment Purchases through the Internet
- Factor Analysis of Drone Terror Risk in Korea through Drone Terror Case on Oil Infrastructure in Saudi Arabia and DPRK Small UAV Crash Case
Conclusion and Proposal
- Existence of Drone Terror Risk in Korea
- Seeking Effective Countermeasures

At recent, successive application of drones such as the oil unit terror in Saudi Arabia by the Yemen rebel forces and explosives terror to assassinate Venezuela president, the international society is actively seeking for countermeasures against the risk of drone terror, a type of New-Terrorism Law. The characteristic changes of terrorism in the international society, successive falls of small UAVs launched from DPRK in 2014 and 2017, increased number of illegitimate aerial drones around major government infrastructures in South Korea, civil drone market growth and its expanded application areas are suggesting drone terror risk in the country, South Korea.

Therefore, to analyze statistical data in addition to documentary survey and media information in this study, based on environmental factors, discussion regarding drone terror risk in South Korea from case study analysis would be schematized as <Figure 1>

## 3.2. Drone terror case analysis

(1)Categorization of case analysis

Considering the no drone terror and damage history in South Korea yet, the category targets of drone terror risk in this chapter would involve comparative analysis upon UAV falls based on recently occurred foreign drone terror cases, thus to observe any future possibility of drone terrors in the nation and to seek for effective countermeasures.

(2)Case analysis

① Major case analysis of foreign drone terror

**Table 1.** Major case of foreign drone terror.

| Section | Time | Place | Contents | Features |
|---|---|---|---|---|
| Case 1 | 2011. 09 | U.S.A | Plan to attack the US Ministry of Defense and Assembly Hall by UAV with C-4 explosives attached failed due to preliminary detection by FBI | - UAV Length 1.5-2m<br>- Over Maximum Speed/hr 160km, 2.3kg Explosives on-board<br>- Follower of Al-Qaeda<br>- First Terror Trial by UAV |
| Case 2 | 2015. 05 | Japan | Drop of a small drone with radioactive substance to the rooftop of prime minster official residence to oppose reactivation of nuclear power generator | - Loading radioactive substance, not firearm and explosives<br>- Uncovering the security vulnerability against small drones |
| Case 3 | 2016. 11 | Iraq | 4 soldiers and civil casualties from suicide drone from IS | - First case, which IS attacked the West by drones<br>- Utility of commercial micro-drone |
| Case 4 | 2018. 08 | Venezuela | President assassination attempt by a drone with explosives attached | - First case attempted assassination on the chief of state by drones<br>- 4KG explosives loaded on commercial 2 micro-drones<br>- Suggested a terror risk by multiple drones |
| Case 5 | 2018. 10 | France | Threat by IS to commit drone terror in response to establishment of blind age around Eiffel Tower in Paris | - Use of drones for the means of terror attacks, spreading social disorder and fear |
| Case 6 | 2019. 09 | Saudi Arabia | Explosives attacks by drones on 2 world-largest oil production units owned by ARAMCO, the state-owned oil company in Saudi Arabia | - Use of drones for terrors on significant national infrastructures<br>- Applying drone swarm, using small drones<br>- 3-4kg explosives loaded |

Note: Jeong, BS. 2019: 163-164 For Reference Uses.

Analyzing the foreign drone terror cases in <Table 1>, first, drone has low level of being detected than other attack means, and while drones with 3-4kg explosives loaded and used for terrors are mostly cheap, its effect-to-cost is huge, hence is mainly used for facility destruction and key figure assassination. Second, loaded items on drones may be radioactive substance or biochemical weapon, other than explosives, thus can cause considerable human and property damages by attacks using a small drone. Third, drone swarm of small drones is used to attack against major government facilities of civil aviation oil-refinery. As such an attack by drone swarm employee low-price drones, it is difficult to tactically respond. Even if one drone is blocked, other drones still perform attacks, thus avoiding damages is impossible. Furthermore, as mentioned for drone swarm, cheap drones are used, thus using expensive weapons to deal with drone swarm faces limitation in the manner of cost-to-effect.

Consequently, locations of drones appearing near major government infrastructures such as airport and nuclear power plant are shared with the control tower real-time and if required, drones are incapacitated, then anti-drone system should be established to provide the location information of drone pilot to the police.

② Case analysis of drones(UAV) detection in Korea

**Table 2.** Drone detection cases in Korea.

| Section | Time | Contents and features |
|---|---|---|
| Case 1 | 2014. 03~04 | - Successive DPRK Drone Crashes in Paju of Gyeonggi-do Province, Baengnyeong Island and Samcheok of Gangwon-do Province<br>- Shooting Panorama of the Blue House and Military facilities<br>- Small digital camera installed<br>- Use of Camouflaged Drone with 2m width and 1m height |
| Case 2 | 2015. 06 | DPRK drone photographing 551 images of THAAD base in Seongju and military bases in Gangwon-do Province |
| Case 3 | 2019. 08. 12~13. | 3-4 small flight vehicles, suspected to be drones, appearing near Kori Nuclear Power Plant in Gijang-gun, Busan |
| Case 4 | 2019. 08. 29 | Drone appearing near Gamami beach and ports near Hanbit Nuclear Power Plant in Yeonggwang-gun, Jeollanam-do Province |
| Case 5 | 2019. 09.07 | Around 20 minutes of flight by an unidentified drone near Hanbit Nuclear Power Plant |

Note: http://news.chosun.com.

<Table 2> lists the recent drone appearances in South Korea, and probability of DPRK consistently preparing for mass destruction weapons such as biochemical and nuclear terrors is worried since 2014 and 2017, referring the fall of DPRK drone(UAV) with small digital camera equipped and photographing images around military bases and the Blue House. That is, DPRK is accepting its limitation in its sole utilization of conventional weapons and considering uses of mass destruction weapons[8], and its utility mean may be a drone. Till the recent, DPRK has continuously proceeded missile test launches, and North Korean weapons are considerable part of the main forces of Yemen Houthis rebel force is pointed out as the mastermind of drone attack on oil facilities in Saudi Arabia and of Iran[9] and DPRK is likely to utilize drones for the means of future terror attacks.

## 4. Effective Countermeasure Against Drone Terror

In recent international society, expanded drone terrors, increased number of unidentified drone flights and 3 falls of small UAVs launched from North Korea, in Baengnyeong Island, Paju of Gyeonggi-do Province, and

Samcheok of Gangwon-do Province indicate the likelihood of domestic drone terror risk

Hence, this study observes causal factors and countermeasures of drone terror risk in South Korea, recognizes the risk severity through the existing advanced studies, statistical data and case studies and suggests an effective countermeasure as following.

(1)Anti-Drone terrorism Law should be separately enacted to prepare for drone terrors. South Korea enacted an Anti-Terror Law in 2016, however the contents do not include any details for anti-drone terror countermeasure and prevention. Thus, Anti-Drone Terrorism Law including blocking illegitimate drones, regulatory measures to safely manage targeted facilities and means of terrors and increasing penalty for each illegal drone flight should be established and preparation for new terror attacks using 3D printers is required.

(2)To deal with drone terrors in South Korea, a social safety network establishment is necessary through an integrated response system with appropriate and relevant organizations. Hence, the related organizations such as military and civil groups should form an integrated response system, to collect, analyze and exchange of terror information via mutual connection, to prepare for actual situations via regular virtual simulations and to seek for countermeasures against future drone terrors[7].

(3)Anti-Drone system to incapacitate illegitimate drones should be formed. Observing flight case frequencies with illegal drone flights and penalty information, 4 cases in 2014, 17 cases in 2015, 25 cases in 2016 and 37 cases in 2017 occurred – increased by over 9 times for the past 4 years[10]. Unidentified drones around nuclear power plants were noticed 13 times since 2015, and over 10 cases were noted during only this year for illegitimate drone flight in the air over nuclear power plants in South Korea. However, no equipment to block illegal drone flights while they are approaching is prepared in South Korea hence, huge human and property damages are anticipated if a drone terror similar to the one in Saudi Arabia occurs. Therefore, a systematic Anti-Drone Protection System with functions to forcefully land illegitimate drone flights or to redirect the directions of the intruded drones

In China, to prepare for drone terrors, jamming rifle is used to block drone signals and using high energy laser, an Anti-Drone Protection System with a vehicle laser used for a rapid blockage against illegal drone flights is established in airline facilities[11].

(4)Analyzing recently occurred drone terror cases, rather than special and expensive drone units, easily acquirable commercial drone units online were used. Thus, using real-name user authentication of drone purchases online and blockage of internet websites where knowledge to produce and renovate improvised explosive devices are available should be performed.

(5)Most drone terrors are held by a terrorist or a group, considering the drone features which they are generally purchasable on the Internet and commercial drone variations are enough to practice terrors, people socially discriminated and prejudiced such as social misfits, second generations of immigrants and minorities may commit drone terrors, thus perceptional improvement and protection are needed for them[7].

## 5. Discussion

In accordance with the international changes by the 4th revolution, the means of terror attacks has shifted into various tools and equipment easily acquirable in daily lives, hence terrorists may maximize their terror damages while the cost of drones and small unmanned vehicles is small, and spread of terrors by the means including drones in international society and high terror risk in South Korea are plausible.

Particularly, drone terror by nK to South Korea is presented in addition to domestic infiltration conspiracies and successive weapon development tests.

However, drones are relatively cheap and easily controllable, yet is difficult to be detected and be traced, if drones are used for terror in South Korea, as its drone detection and response system is at an early stage, huge damage is anticipated. Hence, this study has been proceeded to offer basic information about drone terror risk in South Korea considering both internal and external conditions and an integration of effective countermeasures may be summarized as followings, as a result.

First, Anti-Drone Terrorism Law should separately be enacted to deal with drone terrors in South Korea.

Second, to prepare for the domestic drone terrors, a social security network with cooperation among related organizations such as major government infrastructures, the Ministry of Land, Infrastructure and Transport and the Ministry of Defense should be established.

Third, Anti-Drone System should be established to incapacitate illegitimate drones.

Fourth, real-name user authentication of drone buyers and blockage of internet websites offering knowledge to produce and renovate improvised explosive devices should be practiced.

Fifth, considering the low cost and purchasability by an individual online of drones, there is a probability of people socially discriminated and be prejudiced such as foreign residents in South Korea, minorities and second generation of immigrants may commit terrors. Hence, improvements in social perception and protection for them are required.

As above, drone terror risk in South Korea has been observed through documentary survey, statistics and case study analysis and suggested an effective countermeasure. Yet, in the current condition with no drone terror history in the country, assuming based on the illegitimate drone flights and foreign drone terror cases presents a limitation studying and suggesting an effective countermeasure. Therefore, in relation to the drone terror risk, further studies should be conducted in various methods and the countermeasures should adequately be prepared after revision of related bills from different countries to make them domestically practicable.

## 6. References

### 6.1. Journal articles

[2] Jung BS. Case Analysis of Drone Terrorism and Its Efficient Countermeasures. *The Korean Journal of Korean Police Studies Association*, 14(2), 142-176 (2019).

[4] Oh JH. Response Methods Against Acts of Terrorism That Utilizing Unmanned Aircraft. *Journal of Korea Security Science Association*, 30, 63-82 (2012).

[5] Park JH. Study on the Legal Issues on the Unmanned Aircraft System. *Journal of Northeast Asian Law Review*, 16(2), 79-104 (2015).

[6] Heo J & Jung YG. The Crime with Drone, the Crime Prevention Using Drone. *Korea Journal of Public Safety and Criminal Justice*, 26(3), 358-381 (2017).

[7] Oh SY & Lee JM & Park MG. Study on Occurance Possibility of Suicide Bombing using Utilize Unmanned Aircraft in Korea. *Journal of the Society of Disaster Information*, 10(2), 288-293 (2014).

[8] Park NK & Kang SW. A Study on Status Survey for the Improvement of Shelter Facilities for Residents. *Journal of Korea Society of Disaster Information*, 10(1), 91-97 (2014).

### 6.2. Books

[3] Jung DH. Utilizing Unmanned Aircraft. Imagination-communication (2006).

### 6.3. Additional references

[1] http://www.law.go.kr/ (2019).
[9] http://news.chsun.com/ (2019).
[10] http://www.newsis.com/ (2019).
[11] https://m.post.naver.com/ (2019).

**Author**
**OH Sei-youen** / Semyung University Professor
B.A. Daejeon University
M.A. Dongguk University
Ph.D. Dongguk University

Research field
- A Study on Crime Prevention of Dating Violence Based on IoT, International Journal of Pharmacy and Bio Sciences, Special Issue, March (2017).
- A Study in Virtual Educational Training System for Police with Augmented Reality Technology, Journal of Engineering and Science, 13(1) (2018).

Major career
- 2013~present. Semyung University, Assistant Professor
- 2013~present. Korean Police Studies Association, Research Director

2019 4(2) 15-22

Submission: 2019/11/10, Peer review: 2019/11/20, Accepted: 2019/11/25, Published: 2019/12/30

International Journal of Terrorism & National Security

Publication state: Japan
ISSN: 2423-8376

Publisher: J-INSTITUTE
Website: http://www.j-institute.jp

Corresponding author
E-mail: didsun9999@hnmail.net

Peer reviewer
E-mail: terrorism@j-institute.jp

http://dx.doi.org/10.22471/terrorism.2019.4.2.15

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

**Yang Seung-don**[1]

*Kimpo University, Kimpo, Republic of Korea*

**Park Woong-shin**[2*]

*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

* This work was supported by Kimpo College 2019's Research Fund.

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[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[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 volunterer 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 selfdetermination 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

[1] Park WS. Review of New Investigative Techniques for Regulating Child Pornography: Focusing on the Investigation of Child Pornography on the Dark Web. *Law Review*, 19(3), 51-83 (2019).

[2] Michael KB. White Paper: The Deep Web: Surfacing Hidden Value. *Journal of Electronic Publishing*, 7(1), 1-50 (2001).

[3] Michael C. A Public Policy Perspective of the Dark Web. *Journal of Cyber Policy*, 2(1), 26-38 (2017).

[5] David G & Michael R & Paul S. Onion Routing for Anonymous and Private Internet Connections. *Communications of the ACM*, 42(2), 1-5 (1999).

[7] Daniel M & Thomas R. Cryptopolitik and the Darknet. *Survival: Global Politics and Strategy*, 58(2), 7-38 (2016).

[9] Gabriel W. Going Dark: Terrorism on the Dark Web. *Studies in Conflict & Terrorism*, 39(3), 195-206 (2016).

[10] Dilipraj E. Terror in the Deep and Dark Web. *Air Power Journal*, 9(3), 121-140 (2014).

[23] John S. The Online Disinhibition Effect. *Cyber Psychology and Behavior*, 7(3), 321-326 (2004).

[24] Pawk WS & Yoon HS. A Study of Terror Concept. *Korean Terrorism Studies Review*, 6(2), 44-71 (2013).

### 5.2. Books

[6] Julia B & Tim B. The Rise and Challenge of Dark Net Drug Markets. Global Drug Policy Observatory (2015).

[12] Beatrice B. The Dark Side of the Web: ISIL's One-stop Shop?. Report of the European Union Institute for Security Studies (2015).

[14] Cath S. Cyber Crime and the Darknet. Sirius (2017).

[15] Europol. EU Terrorism Situation and Trend Report 2017 (2017).

[17] Nikita M. Terror in the Dark. The Henry Jackson Society (2018).

[19] Gabriel W. Going Darker: The Challenge of Dark Net Terrorism. Woodrow Wilson Center (2018).

[21] Beatrice B. The Dark Side of the Web: ISIL's One-stop Shop. Report of the European Union Institute for Security Studies (2015).

[25] Stuar H. Islamist Terrorism: Key Findings and Analysis, The Henry Society (2018).

## 5.3. Additional references

[4] https://www.wired.com/ (2014).

[8] https://metrics.torproject.org/ (2019).

[11] http://cjlab.memri.org/ (2014).

[13] https://news.naver.com/ (2015).

[16] https://motherboard.vice.com/ (2015).

[18] https://www.terrorism-info.org.il/ (2017).

[20] https://krypt3ia.files.wordpress.com/ (2014).

[22] https://translate.google.co.kr/ (2018).

**Lead Author**

**Yang Seung-don** / Kimpo University Professor
B.A. Soonchunhyang University
M.A. Dongguk University
Ph.D. Dongguk University

Research field

- Application Plan of U.S. Aviation Profiling for Prevention of Air Terrorism in Korea, Korean Security Review, 38 (2014).
- A Study on the Trend and Countermeasure of Cyber Terrorism, Review of Korean Terrorism Studies, 11(2) (2018).

Major career

- 2011~present. Korean Association of Terrorism Studies, Member
- 2015~present. Korean Association of Police Science, Member

**Corresponding Author**

**Park Woong-shin** / Dongseo University Visiting Professor
B.A. Sungkyunkwan University
M.A. Sungkyunkwan University
Ph.D. Sungkyunkwan University

Research field

- A Study on the Criminal Law of the Propaganda of Terrorism on the Dark Web, Journal of Criminal Law, 31(3) (2019).
- A Study on the Application of the Doctrine of Warrants on Wearable Police Camera, The Journal of Police Policies, 33(1) (2019).

Major career

- 2017~present. National Central Police Academy, Visiting Professor
- 2019~present. Dongseo University, Visiting Professor

2019 4(2) 23-33 Submission: 2019/11/10, Peer review: 2019/11/20, Accepted: 2019/11/25, Published: 2019/12/30

International Journal of Terrorism & National Security

Publication state: Japan
ISSN: 2423-8376

Publisher: J-INSTITUTE
Website: http://www.j-institute.jp

Corresponding author
E-mail: sinchuk.back@scranton.edu

Peer reviewer
E-mail: terrorism@j-institute.jp

http://dx.doi.org/10.22471/terrorism.2019.4.2.23

# The Role of Technology in Facilitating, Connecting, and Ending CYBERCRIME, Drug Trafficking, and Money Laundering

**Mohammed AlQahtani**[1]

*Florida International University, Miami, United State of America*

**Raymond Doug Partin**[2]

*Florida International University, Miami, United State of America*

**Back Sin-chul**[3*]

*University of Scranton, Scranton, United States of America*

**Jo Sung-gu**[4]

*Kyungwoon University, Gumi, Republic of Korea*

## Abstract

*This research investigates and shows how technology helped to facilitate and to connect three types of transnational crimes. More specifically, cybercrimes, drug trafficking, and money laundering. Moreover, technology has helped to facilitate cybercrimes by basically giving birth to them; without the evolution of technology, we would not have had cybercrimes. When ICTs(Information and communication technology) showed up, people all over the world can now have access to the internet which can make some of them vulnerable to cybercriminals. Examples of cybercrimes can include hacking, Ransomware, Identity theft, phishing emails, Internet Crime Against Children(ICAC), industrial espionage, and fraud.*

*As for drug trafficking, technology has helped to facilitate this type of cybercrime by basically giving dealers and consumers a safe atmosphere where they can make deals and payments from anywhere in the world without the need of physical appearance which makes them less exposed to getting arrested. Examples of electronic drug trading are the hidden market places in the darknet.*

*As for money laundering, technology has provided money launderers the ability to establish online offshore companies and banks that have fewer restrictions on money laundering; this method helps criminals to wash their money in countries with no or few laws that prohibit and investigate unknown income sources. Furthermore, technology has provided online banking which gives people the ability to make online transactions; cybercriminals can easily blend their illicit transactions with the illicit ones with less chance of getting noticed.*

*Other than facilitating those crimes, technology has also helped to connect those three types of crimes. Cybercriminals help drug dealers with coding and providing cyberspace, both cybercriminals and drug traffickers launder their money to have legit unquestionable income.*

*As for recommended policy implications, nations should keep updating their laws in order to properly prosecute those types of crimes, more education for law enforcement agencies should by implied as well along with more awareness to the public to avoid victimization.*

*[Keywords]* ***Cybercrime, Drug Trafficking, Money Laundering, Darknet, Transnational Crime***

## 1. Introduction

Everything evolves as times passes. Technology is central to human evolution; it has evolved over thousands of years and will continue to evolve until the end of the world. As technology has evolved, it has enabled the evolution of the world, improving and making life on this planet easier and faster. Whether it is physical technology, technological hardware that can be used as a mechanical instrument(e.g., machines, vehicles, cameras)[1][2], or digital technology information that is coded and programmed into software to work as part of a machine(e.g., artificial intelligence, applications, internet), the evolution of technology has made communication, business, traveling, security, entertainment, and the majority of human activity significantly more accessible and more efficient.

The evolution of technology has also benefited criminals and evolved the world of crime[3]. As the evolution of technology has transformed the world, crime and criminals have also evolved and transformed in type, methods, complexity, and adaptation to new prevention methods enacted by law enforcement. With the help of technology, traditional crimes can modernize and advance[3].

In addition to benefiting criminals and facilitating crime, technology has also played a role in fighting crime through its use by criminal justice departments. Law enforcement agencies across the globe have utilized technology to maximize security and minimize crime rates[3]. For example, through programs, machines, and other technology, law enforcement agencies have been able to improve their intelligence mechanisms, to scan for explosives and any law-violating items, and to ensure security while minimizing damages caused by criminals.

Although technology is an umbrella term, this research considers the evolution of technology as the independent variable, and specifically information and communication technology(ICT). ICT refers to any technology that helps to produce, store, transmit, communicate and disseminate information in all forms, including voice, text, data, graphics, and video[3]. Examples of ICT include both hardware(machines and devices) and software(e.g., applications, programs, malware).

Information and communication technology largely focus on the Internet. According to Nuth(2008), the Internet is the network of computer networks. At its origin, the Internet was merely a tool of communication to exchange messages between computers. However, with the evolution of technology, the Internet has evolved into the subject(place), object(target), and tool(instrument)[3]. When a computer connects to the Internet, it connects to millions, if not billions, of other computers located across the globe at a low cost[3]. Nuth(2008) argues that there is no such thing as territorial space when it comes to the Internet. In other words, people from all around the world can connect and surf the Internet however they want, with minimum physical restrictions.

Criminals have taken advantage of the Internet. As a tool for international connection, the Internet offers many opportunities for criminals to act upon, and a massive field to roam and practice criminal activity[3]. With the help of this technology, criminals can now communicate, plan, commit, and monitor their criminal acts with reduced risk of capture due to the absence of physical appearance[3][4]. The Internet draws the bridge for criminals to commit their crimes remotely and from the coziness of their desk chair. Nuth(2008) provides a basic example of how an individual or a group of criminals, either experienced or self-taught, can crash the European stock market and cause global chaos for many nations.

As it has helped criminals and crime, the evolution of technology has also helped law enforcement agencies in preventing, reducing, and minimizing the damage of crimes. Nuth(2008) argues that both sides have benefitted from technology. For law enforcement and criminal justice, both physical and digital technologies have been implemented in fighting the battle against crime and criminals. Nuth(2008) provides the example of a basic physical technology that has been implemented in many nations and has worked as a great deterrent for criminals: the installation of closed-circuit television surveillance systems(CCTV) in public or private spaces has helped in reducing crime rates in the United States and the United Kingdom.

Crime technology is an unwanted but unavoidable race[3]. Due to rapid adaptation by criminals and organized crime groups, law enforcement agencies and criminals are racing to surpass each other. Every new invention is followed by a newer one. For example, telephones and mobiles were first invented to communicate. Those devices were soon exposed to evolution and now can record conversations through electromagnetic impulses [3]. The endless cycle of technology evolution will never stop advancing, while criminals and law enforcement agencies race each other to adapt to the new mechanisms offered by such evolution[3]. However, Nuth(2008) emphasizes how technology can backfire on law enforcement agencies. He explains that when law enforcement agencies adopt new technology to help them fight crime, criminals can study this new technology, develop newer versions, and use it to their benefit to overcome the challenge posed by law enforcement. For example, when law enforcement agencies introduced DNA-testing technology, criminals took that technology and used it in their favor, adopting it to remove their DNA traces from the crime scene, or even replace their DNA with someone else's[3].

Cybercrimes, drug trading, and money laundering are the dependent variables for this research. This study demonstrates how technology can facilitate and connect these three types of transnational crimes. Cybercrimes refer to every crime related to the Internet(e.g., hacking, sabotaging, cyber terrorism, theft, identity theft), while drug trading covers the transition of traditional drug trading to modern and digital drug trading(i.e., via surfing the dark web, which offers the ability for sellers and buyers to browse, communicate, seal deals, and exchange payments). Drug trading also refers to hardware technology that helps drug traders in transporting their drugs with the use of technology(e.g., transporting drugs via drones from point A to point B). This research also demonstrates how technology has introduced more methods for criminals to launder their money(e.g., buying and selling programs' codes, electronic copies of games or music).

This research fills the gap in understanding the role of technology in the overlap between cybercrimes, drug trading, and money laundering. For example, cybercriminals can create their e-commerce store in the darknet. Darknet is an area of the Internet that is not shown to the public; it has a strong inscription that cannot be accessed with regular browsers. Browsers that provide users access to the darknet include a browser called TOR or the onion router, which was made many years ago by the United States Navy to allow them to encrypt their intelligence sharing with the anonymity it provides[4]. Through its anonymity and encryption, the darknet enables drug traders to make deals via the Internet and make profits that they can launder and wash via purchasing and selling digital goods.

This research also addresses some of the policies that have been implemented over the years to prevent cybercrimes, drug trading, and money laundering using the evolution of technology. It examines why such policy implementations are not working properly in preventing crimes. Also, the research suggests which type of those three crimes is the most serious and why. Finally, this research reviews previous studies regarding how technology can impede transnational crimes by merging it with new policies to fight those three types of transnational crimes and provides recent and historic examples for each variable and policy discussed.

Although the umbrella of transnational crimes covers many different types of crimes, the three types above of crimes were specifically chosen because the variables are logically related. Without the evolution of technology, cybercrimes would not exist, as the Internet is the origin. Without technology, digital and physical drug trading would evolve, and without both cybercrimes and drug trading, money laundering methods would not have expanded and evolved throughout the years.

## 2. Cybercrimes

Cybercrimes are one of the biggest threats currently facing the world. Cybercrimes caused losses that amounted to $400 billion in 2005, compared to the $17 billion loss from the 9/11 attacks[4]. Internet-facilitated crimes are limitless; new crimes are committed every minute around the world from different locations. The cyber world offers opportunities to everyone: criminals can continue their criminal activities, traditional crimes can advance and become cybercrimes, and non-criminals can learn how to be criminals with the push of a button[3]. Nuth(2008) also argues that the cyber world enables criminal offenses and makes them increasingly possible, creates new crimes, and transforms traditional crimes into advanced crimes.

Furthermore, McQuade(2001) writes that cybercrimes are very complex and mysterious to government officials, media, and society due to the involvement of advanced and complicated technologies with which many people are unfamiliar; the involvement of many suspects and victims, and the vast amount of damage and harm caused by and to them; the mixed varieties of traditional and new crimes; the lack of communication between law enforcement experts; and the ability of cybercrimes to occur from different geographical locations and different jurisdictions where law enforcement agencies can practice their authority. McQuade(2001) also suggests that adaptation to new technologies can generate crime waves, which in theory can be predicted and measured. Although these waves benefit transnational crime groups, terrorist groups, and cyber criminals, police and law enforcement agencies can sometimes use them in their favor to predict, prevent, and minimize the damage of certain cybercrimes. According to Nouh, Nurse, Webb, and Goldsmith(2019), there is an asymmetrical relationship between cyber criminals and law enforcement agencies, as law enforcement agencies face restrictions that do not allow them to collect data to investigate.

Cybercrimes and cybercriminals experience more benefits than traditional crimes. According to Li(2018), the sophistication and skills that cybercrimes require to offer many advantages to cybercriminals. For example, cybercrimes do not require physical appearance and can operate remotely across multiple time zones and jurisdictions, which makes it difficult for law enforcement to deal with those types of crimes[4]. Moreover, cybercrimes provide cybercriminals more anonymity. Cybercriminals operate from different locations around the world, and they can change their IP addresses and conceal them with a press of a button, making them effectively immune to detection and tracing[4]. Although it takes seconds to commit a cybercrime, cybercrimes can cause damages that last for weeks or even months. Once a network is infected with viruses, these viruses keep regenerating and spreading, causing more damages over time[4].

Furthermore, cybercrimes provide concealed victimization, as victims are attacked with little or no information on who attacked them. This concealment leads many victims to not report the crimes committed against them, which increases the dark figure of crime[4]. Kang(2018) argues that some victims are not willing to report and become hidden victims due to the ignorance of cybercrimes among police, limited accessibility of police and courts, and fear. Li(2018) found that as a result, only 1 in 100 cases was detected in the US, 1 in 8 was prosecuted, and 1 in 33 prosecutions resulted in prison time, and the chance of cybercriminals being sent to prison is 1 in 26,400.

Cybercrimes can be understood according to multiple criminological theories. According to McQuade(2001), theories and criminological schools from the 18th century can be applied to understand cyber criminals. For example, the classical school can explain cybercrimes by simply demonstrating the free will and the thrill-seeking actions accompanied by selfishness and evilness. Meanwhile, Sutherland's(1947) differential association theory explains how some cybercriminals learn the basics of technology and continue their way into criminality[2]. McQuade(2001) notes that even Cohen and Felson(1979) mentioned technology, exploring how motivated offenders can attack suitable targets using technology and committing cybercrimes to take advantage of the absence of protection.

Cybercrime has been defined in many different ways in the scholarly world. According to Nuth(2008), cybercrimes are any type of crime conducted on the Internet, which requires hardware or physical technology such as a computer. In their works, Brar and Gulshan(2018) both argue that cybercrimes are malicious activities that affect the three fundamental principles of network security: confidentiality, integrity, and availability. According to Brar and Gulshan(2018), confidentiality is threatened by attacks on private documents and passwords, integrity is threatened by attacks that aim to corrupt and destroy data, and availability is threatened by attacks that can immobilize or jeopardize the flow of data or information. Additional scholars such as Thomas(2018) define cybercrime as any offense enabled by technology. Meanwhile, Cordova, Alvarez, Ferrandiz, and Perez-Bravo(2018) define cybercrimes using the Oxford Dictionary of Law(2002), which defines cybercrimes as "any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them." Cordova et al. (2018) also expand upon this definition by stating that cybercrimes are any criminal act conducted in cyberspace, and they define cyberspace as the network that includes the Internet, telecommunication networks, computer systems, and embedded processors and controllers in critical industries[5].

Technology has facilitated cybercrimes because it gave birth to them. Nuth(2008) emphasizes one of many types of cybercrimes known as viruses. According to John(2006), a virus is malicious software that inserts its code and infects the area, causing damages. Nuth(2008) provides the example of a virus called "love bug." Love bug was sent as an attachment in the year 2000 via email. Many people received the email and clicked the attachment files that contained the virus, causing millions of computers around the world to be damaged and infected within hours. Many governments and companies were attacked by this virus, and the worldwide business community lost an estimated $6.7 billion in the first five days of the spread of the virus. Furthermore, Nouh et al.(2019) share that cybercrimes marked 50% of crimes committed in the United Kingdom in 2017 alone and that almost 68% of businesses located in the UK have been victims of cybercrimes and cyber-attacks.

Cybercriminals adapt and evolve along with the evolution of technology. According to Glenny(2008), cybercriminals used to commit cybercrimes to ruin someone's day in order to entertain themselves and enjoy a good laugh. However, the evolution of technology created many opportunities for cybercriminals to expand the field of their criminal activities[3]. With the huge dependence on technology and computers for everyday activities such as banking, texting, and sending and receiving emails, and the overall central role technology now plays in life, cybercriminals evolved from criminals who once just wanted to ruin someone's day, to criminals who want to benefit and act upon opportunities that the evolution of technology offers[3]. Cybercriminals are ultimately very fast to adapt. By the time a new technology emerges, cybercriminals will have already coded programs, made plans, and generated new ideas on how they can benefit from this opportunity[6]. Examples include cyber-attacks on governments to achieve political goals, cyber-attacks on banks and credit cards to achieve a financial goal, and cyber-attacks on individuals to blackmail or achieve a personal goal.

According to Brar and Kumar(2018), cybercrimes always attack three fundamental principles, known as the CIA(confidentiality, integrity, and availability). Confidentiality means that cybercriminals will attack data that are private and limited to authorized users only, including account passwords. Names for those attacks can be eavesdropping, snooping, or password attacks[7]. Integrity refers to the accuracy of the attack and its occurrence in a specific time to achieve a specific goal. An example is an attack that shuts down electricity in an area for a few hours, and names for such attacks include Salami attack, cross-site scripting, and session hijacking[7]. Finally, availability means shutting down the access of authorized users from the attacked network so cybercriminals can roam without interruptions. Examples include shutting down Internet connections in a specific bank to block the access for the cybersecurity team, which allows cybercriminals to roam freely. Such attacks are called DDoS attacks, UDP attacks, and HTTP attacks[7].

There are many types of cybercrimes committed by cybercriminals, and categories of cybercrimes differentiate in both goals and means. Previous research from Nuth(2008) and Brar and Kumar(2018) provide that many types of cybercrimes can be categorized into four main categories: entertainment, personal, financial, and political. Entertainment cybercrimes are any crimes to corrupt or ruin someone's property. This includes cyber-vandalism, which is any malicious destruction of property[3]. Personal attacks are any attacks that achieve personal goals for the criminals. These attacks can include many cybercrimes, such as cybertrespass, which means crossing unauthorized boundaries.

Further crimes that fall under the personal category are child pornography, cyber stalking, cyber bullying, spying, and revenge[3][7][8]. Financial-gain attacks include any cybercrime that achieves financial gain for the criminal. These attacks include credit-card theft, identity theft, fraud, electronic money laundering, and spam emails[3][7]. Finally, political cybercrimes are politically motivated crimes that aim to harm, sabotage, or cause financial damage. Examples include hacking and spying[3][7]. There are some cybercrimes that can be categorized in more than one category. For example, hacktivism (any network attacks that give access of private data and information to cybercriminals) can be used in any category of the above to achieve various goals that cybercriminals aim to achieve.

Cybercrime incidents happen globally, and the world has witnessed many of them. The first cybercrime case explored in this paper is the case, covered by Stevens(2011), of Joe, an Australian man who was arrested and sentenced for involvement in child pornography. Joe's computer was seized by the police, and they found images that included child pornography. Joe's life changed after his arrest: he was forced to sell his house to meet legal fees, he was prohibited from meeting his 8-year-old daughter without supervision, and he was forced to quit his job for "security reasons." The second case comes from the FBI: a $10 million hack in 1994 by a transnational gang. Led by a Russian computer programmer, gang members hacked bank accounts from the United States by obtaining IDs and passwords and transferred all funds overseas. Although many receiving bank accounts have been frozen by authorities, the heist continued for months, until Levin the programmer was sent back to the US and pled guilty. Bellisle(2017) also tells the story of a member of the Russian parliament who hacked more than 500 U.S. companies and stole millions of credit cards that he then sold to other websites. A further example comes from the Department of Justice(2018), which covered a notable case of cyberstalking. Joel Kurzynski was arrested and sentenced for cyberstalking by threatening, body shaming, and sending hate speech to two close people in his life. Also, in a case with the Department of Homeland Security(2012), a group of people hacked credit cards and increased their limit. While acquiring the PIN, the organized group burned the information into new cards and drained them at ATMs. This operation was happening in 24 countries, resulting in a $40 million loot from 34,000 ATMs. Finally, the news has recently covered many cyber-attacks targeting big brands and countries. For example, Adobe was attacked, and 150 million accounts were leaked[9]. Sony PlayStation network, Target, Yahoo, and Marriott were all also victims of cyber-attacks and had their costumers' information leaked or hacked[9]. South Korea and Russia, in particular, have been targeted for cybercriminals, as 100 million credit cards were stolen in South Korea and 1.2 billion logins from 420,000 websites were possessed by hackers in Russia[9].

## 3. Drug Trafficking

Drug trading and drug smuggling are the second types of transnational crime that has been heavily facilitated and improved with technology. According to Nuth(2008), technology enables traditional crimes to transform and adapt to technologies. Drug trading and smuggling, like other crimes, have evolved and adapted along with technology. A review of previous research and known cases reveals how both hardware technology and software technology have modernized the illegal drug industry.

The United Nations Office of Drugs and Crime(2010) defines drug trafficking as the global industry of illegal drugs that includes any cultivating, manufacturing, distributing, and sale of substances that are prohibited by laws. Although this definition is applied to traditional drug trafficking, the definition can also be applied to advanced drug trafficking with the way technology has evolved the illegal drug industry, as the same processes of trading and smuggling are relevant.

Technology-facilitated drug trafficking and smuggling use both physical or hardware technology and digital or software technology. Hardware-facilitated drug trading and smuggling refer to how traffickers and smugglers use technological machines and devices to seal their deals. These devices can include flying drones that carry the shipment and transport drugs in and out of any areas that include borders, walls, buildings, and fences[10]. Digital or software drug trading can be implemented by organized crime groups or dealers via the use of Internet and darknet, which provides suppliers the ability to advertise and show their products along with ratings and prices[11]. Customers can browse, ask, bargain, buy, and even share opinions with other costumers. All these deals happen with the click of a mouse from a computer connected to the Internet, without the need of leaving the house of even desk chair[11].

There have been many cases of drug trading and smuggling around the world in which criminals utilized technology to commit their crimes. For example, a 25-year-old man in 2017 was charged with drug-smuggling crimes in San Diego, where he smuggled more than 13 pounds of methamphetamine believed to be worth $46,000 using a drone that flew across the border[12]. According to Fiegel(2017), in 2012 alone, the US authorities seized 150 drones carrying two metric tons of marijuana, cocaine, and heroine. The drones mainly fly from Mexico to the United Stated carrying a variety of illicit drugs. Mexico upgraded the drone designs and increased the capacity compared to regular personal drones. Mexican drones now can carry and transport 60-100 kilograms(132-220 lbs.) of drugs in a single trip[13]. Drones offer organized crime groups and cartels less risk in drug trafficking. Firstly, they offer protection to employees and the whole group, as captured employees will be questioned by authorities[13]. Fiegel(2017) also notes that beyond transporting drugs, drones can work as a tool for surveillance that supports protecting areas and shipment. He offers the example of cartels that used drones to gather intelligence and scan the area to protect their $30,000,000 cocaine shipment going to Panama.

In addition to drones and hardware technology, drugs can also be traded online via the Internet. Augusto and Godoy(2015) reveal that the virtual drug black market can be accessed with fake IP addresses. For example, Silk Road referred to as “the Amazon of illicit goods,” attracts customers and suppliers from all around the world buying and selling illicit items such as body parts, organs, and drugs[14]. Weed, ecstasy, heroin, steroids, cocaine, and hash are all traded on the website with full anonymity for the administrators, consumers, and suppliers[14]. With the use of Bitcoin as the main currency of payment, all payment transactions are fully untraceable and anonymous[14].

Moreover, Rhumorbarbe, Staehli, Broséus, Rossy, and Esseiva(2016) claim that the darknet has more than 48,000 listings of people who claim that they sell drugs from 70 countries. The most commonly listed drugs are cannabis-related drugs, ecstasy, and cocaine. Buskirk, Naicker, Bruno, Burns, Breen, and Roxburgh(2016) argue that after monitoring 16 illicit marketplaces across the darknet, they found that cannabis, pharmaceuticals, MDMA, cocaine, and methamphetamine had the highest demand. Although many virtual illicit market places such as Silk Road and Silk Road 2.0 were shut down by authorities, illicit market places are still growing and generating[15]. Afilipoaie and Shortis(2015) outline the steps needed to purchase illegal drugs from the darknet. An individual should use TOR browser to hide his or her IP, acquire Bitcoin for a fully anonymous transaction, and communicate via PGP encryption(short for Pretty Good Privacy) to ensure privacy and security from third parties.

Technology-facilitated drug trafficking is directly connected to cybercrimes. Cybercrimes are any illegal act that occurs via or in cyberspace[5] and without cyberspace, drug suppliers and consumers would not be able to seal their deals and exchange payments. Technology gave rise to cybercrimes, and cybercrimes, in turn, gave rise to the darknet and illegal e-commerce websites, where technology-facilitated drug trafficking flourishes.

## 4. Money Laundering

Money laundering is the process of "washing" illegally obtained money to make it appear legal and legitimately obtained in order to avoid prosecution[16]. Money laundering is the third type of transnational crimes that have been heavily facilitated by technology, and its placement as third on the list mirrors the underground economy[11]. Every illegal act that has a financial goal will resort to money laundering in order to complete its mission. No matter the type of crime, money laundering will always play the last part in order to make the outcome legal. Both cybercrimes and traditional crimes utilize money laundering to complete their purposes.

Naim(2005) argues that new technologies have facilitated money laundering due to the lack of physical borders and low-priced bank transactions. He also argues that due to new technologies, many financial institutions can be a destination of funds. As technology renders borders useless, criminals engage many offshore firms to lauder their money remotely[11]. Albanese(2011) also notes that entertainment technology such as casino chips are heavily used by criminals to launder their money because gambling chips can be traded with cash. Also, Albanese(2011) states that criminals take advantage of money orders and checks by transferring their hard cash into official financial documents. Further types of money laundering facilitated by technology occur via cryptocurrencies or digital currencies.

Examples and cases of technology-facilitated money laundering are numerous, and many criminals have been globally prosecuted due to their involvement in laundering funds. For example, many online video games are involved in money laundering. According to Osborne(2019), cybercriminals steal credit cards and buy items in videogames such as Fortnite to launder their money. She shares that criminals buy V-Bucks that can be sold to the gaming community with lower prices, which provides criminals the perfect method to wash stolen funds. According to Hall(2015), discounted game codes are another method that criminals use to launder money stolen from credit cards. Hall(2015) argues that on websites such as Kinguin and G2A, people sell games at almost 80% discounts; however, the codes are obtained illegally and it is another method of laundering, which can be applied to anything in the e-commerce world. Due to the privacy that cryptocurrencies provide, criminals have been able to launder $1.2 billion between 2017 and 2018[28]. Ngetich (2018) highlights that with the help of Bitcoin, a Danish bank called Danske was able to lauder $234 billion between 2007 and 2015. Gola(2019) and Beedham(2019) found that 7,096 out of 417,465 money laundering cases in Japan involved Bitcoin.

Money laundering is directly connected to cybercrimes and drug trading. As previously mentioned, money laundering is the resort of almost every single crime driven by finances, particularly cybercriminals who are involved in scamming and identity theft for monetary gains. Meanwhile, online drug traders and traffickers also commit their crimes in cyberspace with the help of cybercriminals for money and subsequently launder money in order to achieve their financial goals. Therefore, the connection between cybercrimes, drug trading, and money laundering is fundamentally established with the help of technology. Beyond the facilitation of individual crimes, technology has connected the dots and established interdependency and symbiosis between the three types of transnational crimes.

## 5. Policy Implication

There have been many attempted policies to defend against the three types of transnational crimes, but most have not been effective. Regarding cybercrimes, Nouh et al. (2019) argue that cybercriminals adapt to new methods 200% faster than authorities. No matter how authorities try to defend against and investigate cybercrimes, they are restricted and limited to the data they can access, which results in an asymmetrical relationship against cybercriminals. Brar and Kumar(2018) also study how authorities focus on cybersecurity to defend data against cybercriminals. Due to the fast adaptation of criminals, cybersecurity will not be enough to counter cybercriminals, because cybercrimes are not single-angled. Furthermore, Thomas (2018) argues that even if authorities succeed in countering cybercriminals, authorities will not be able to arrest and prosecute offenders due to jurisdictional limitations, because cybercrimes are digital and not limited to physical borders.

Policies have also failed to counter technology-facilitated drug trafficking. In traditional drug trafficking, authorities always focus on the supplier. Although traditional drug trafficking requires physical appearance and physical effort, suppliers continue to multiply in numbers due to the high demand[16]. By default, cyber drug trafficking provides less risk and less effort to suppliers due to the lack of physical interaction, appearance, and borders. Unfortunately, authorities continue to target suppliers and ignore the bigger picture, which is approaching the issue through supply, demand, regulations, and completion[16].

Albanese(2011) argues that increasing efforts against money launderers will increase the number of transactions money laundered do to wash money. With the increase of transactions, fees increase; and when fees increase, money launderers earn more money, and the washing process continues[16].

Recommenced policy interventions against cybercrimes should focus more on awareness and education for law enforcement, potential offenders, and victims, and more on cooperation between law enforcement agencies, nations, and the private sector. Thomas(2016) argues that many law agencies' personnel are not properly educated and aware of cybercrimes, which makes victims more vulnerable to blackmailing and harassment. Also, Ron, Fuertes, Bonilla, Toulkeridis, and Javier Díaz (2018) note that nations such as Ecuador treat cybercrimes under civil law, which punishes cybercriminals with minor penalties if prosecuted. Criminalizing cybercrimes will not be accomplished without increasing awareness and education of cybercrimes' consequences. Li(2018) provides a critical point regarding defense against cybercrimes. He mentions that a few countries have updated their laws in order to criminalize the crimes that are facilitated by technology. Li (2018) also suggests that a collaboration between both the public and the private sectors should occur to protect against cybercrimes.

Furthermore, Nouh et al.(2019) state that sharing intelligence between local and international law enforcement agencies is key to minimize the effect of cybercrimes. As an example, the FBI hosted a campaign, the Cyber-citizen Partnership Awareness Campaign, to increase the education and awareness of children and their parents on how to use the Internet ethically and avoid criminality and victimization. Glenny(2008) also provides advice on how to avoid being a victim of cybercriminals. He warns youth not to download illegal music and pornography, because they are largely used as baits to lure young people and make them vulnerable to hacking. Kang(2018) also provides extensive advice on how people should protect themselves from cyber-attacks. After analyzing the Hollywood hacking campaign that targeted famous personalities, Kang(2018) warns not to get baited by "phishing" emails that tend to hack computers and access all data that users have in their computer or on their associated cloud storages. Recommended policy interventions against cybercrimes should be approached from the victims' side and not the offender's sides.

Regarding both physical and digital technology-facilitated drug trafficking, new policy interventions should focus more on the demand and regulations, and less on the supply.

Fiegel(2017) and Wolfe(2019) mention how drug cartels use the technology of drones to transport drugs and surveil the areas to execute their mission. The demand is high for drugs, and as Albanese(2011) argues, focusing only on suppliers while ignoring demand will increase the prices and make criminals make more money. Therefore, new approaches should focus on where those drones are going, as focusing on the demand will render the suppliers' operations useless. Meanwhile, limited existing research has specifically focused on how to counter digital drug trafficking. According to Albanese(2011), focusing on the demand and increasing internet use regulations is a better approach than targeting suppliers, as suppliers can be making deals from any point on the globe in different jurisdictions, which prohibits authorities from operating effectively. However, they can target the destination of the shipment within their jurisdiction and control the demand.

Recommended policy interventions for technology-facilitated money laundering have been previously raised by Naim(2005), Glenny(2008), and Albanese(2011). They all highlight that most money laundering occurs overseas from offshore companies, which will not happen if countries increase the sharing of their financial information. Such an approach also applies to digital money laundering that uses games' codes and cryptocurrencies. Increasing communication between nations and companies can, by default, increase the awareness of consumers on how criminals steal credit cards using cybercrimes and launder them in video games and cryptocurrencies. Also, technology can provide banks and authorities with anti-money laundering methods. According to Balooni(2017), technologies can provide financial institutions with large data memory that can store, render, profile, and detect huge numbers of electronic transactions occurring by the minute around the world. Technology is capable of undergoing tasks that humans cannot process, and tracking money laundering transactions in vast numbers is one of those tasks that technology can help us to overcome.

## 6. Conclusion

All cybercrimes, drugs trafficking, and money laundering are facilitated and connected by the evolution of technology. Technology gave birth to cybercrimes, cybercrimes are used as a portal for drug trafficking, and both crimes resort to money laundering to finish the job and loot their funds legally. Therefore, the recommended policies to counter the three types of crimes should include a focus on consumers, victims, potential offenders, and regulations to prevent the spark that ignites those crimes. Education, awareness, and international/private collaborations should be encouraged to share intelligence between jurisdictions and to warn the youth and the elderly in particular, who are not familiar enough with technology to understand how not to violate the law or be victimized. The best method to fight any type of transnational crimes is to approach and analyze the whole equation, which should involve supply, demand, regulations, and victims(if they are not victimless crimes).

## 7. References

### 7.1. Journal articles

[3] Nuth MS. Taking Advantage of New Technologies: For and Against Crime. *Computer Law & Security Review*, 24(5), 437-446 (2008).

[5] Cordova JGL & Álvarez PFC & Ferrandiz FDJE & Pérez-Bravo JC. Law Versus Cybercrime. *Global Jurist*, 18(1), 1-9 (2018).

[7] Brar HS & Kumar G. Cybercrimes: A Proposed Taxonomy and Challenges. *Journal of Computer Networks & Communications*, 12 April, 1-11 (2018).

[8] Stevens B. An Unrecognized Girardian Scapegoat?: Criminal and Social Consequences for Internet Offenders. *Colloquium*, 43(2), 183-196 (2011).

### 7.2. Books

[1] Opper J. Science and the Arts: A Study in Relationships from 1600-1900. Fairleigh Dickinson Univ (1973).

[11] Naim M. Illicit: How Smugglers. Traffickers,

and Copycats are Hijacking the Global Economy. Doubleday (2005).

[16] Albanese JS. Transnational Crime and the 21st Century: Criminal Enterprise, Corruption, and Opportunity. NY: Oxford University (2011).

## 7.3. Additional references

[2] McQuade, S. Technology-enabled Crime, Policing and Security (2001).

[4] Li B & Erdin E & Güneş MH & Bebis G & Todd S(n.d.). Traffic Monitoring and Analysis. Retrieved April 1 (2019).

[6] Glenny M. McMafia: A Journey through the Global Underworld. House of Anansi (2008).

[9] https://outpost24.com/ (2019).

[10] https://www.rotorandwing.com/ (2019).

[12] https://www.washingtontimes.com/ (2019).

[13] https://smallwarsjournal.com/ (2019).

[14] https://works.bepress.com/ (2019).

[15] Van Buskirk J & Naicker S & Bruno RB & Breen C & Roxburgh A. Drugs and the Internet (2016).

**Lead Author**
**Mohammed Alqahtani** / Florida International University Researcher
B.A. University of Miami
M.A. American University

Research field
- A Comparative Analysis of Volunteer Officers from the United States and the United Kingdom, International Journal of Police and Policing, 4(2) (2019).

Major career
- 2019~present. Florida International University, Teaching Assistant

**Co-Author**
**Raymond Doug Partin** / Florida International University Researcher
B.A. The University of Cincinnati
M.S. The University of Cincinnati

Research field
- A Comparative Analysis of Volunteer Officers from the United States and the United Kingdom, International Journal of Police and Policing, 4(2) (2019).

Major career
- 2018~present. Florida International University, Teaching Assistant

**Correspondence Author**
**Back Sin-chul** / University of Scranton Assistant Professor
B.S. Northeastern University
M.S. Bridgewater State University
Ph.D. Florida International University

Research field
- The Future of Cybercrime Prevention Strategies: Human Factors and a Holistic Approach to Cyber Intelligence, International Journal of Cybersecurity Intelligence & Cybercrime, 2(2) (2019).
- Low Self-control, Social Learning, and Texting While Driving, American Journal of Criminal Justice, 44(2) (2019).

Major career
- 2011~2012. Massachusetts State House, Legislative Aide
- 2019~present. University of Scranton, Professor

**Co-Author**
**Jo Sung-gu** / Kyungwoon University Professor
B.A. Kyungwoon University
M.A. Kyungwoon University
Ph.D. Kyonggi University

Research field
- Response of Korean Private Security against North Korean Cyber Terrorism, International Journal of Protection Security & Investigation, 2(2) (2017).
- Korea's National Security and Anti-terrorism Strategy - The Cases of Key Figure Assassination and the Direction of Protection Security Activities-, Korean Police Studies Review, 17(2) (2018).

Major career
- 2006~2009. Republic of Korea National Assembly, Secretary
- 2012~present. Kyungwoon University, Professor

2019 4(2) 34-40 Submission: 2019/11/10, Peer review: 2019/11/20, Accepted: 2019/11/25, Published: 2019/12/30

International Journal of Terrorism & National Security

Publication state: Japan
ISSN: 2423-8376

Publisher: J-INSTITUTE
Website: http://www.j-institute.jp

Corresponding author
E-mail: khs1030r@hanmail.net

Peer reviewer
E-mail: terrorism@j-institute.jp

http://dx.doi.org/10.22471/terrorism.2019.4.2.34

# A Framework for Developing MILITARY Safety Performance Indicators(MIL-SPI) Using the Balanced Scorecard

**Kwon Hyuck-shin**

*Seoul National University of Science and Technology, Seoul, Republic of Korea*

## Abstract

*The ROK Army has recently formed the safety professional organization ,whose function is implementing safety management policies, and providing safety support to field troops with the aim of establishing a new safety culture from the combat preparation perspective. The purpose of this study is to devise a framework for the development of the Army's safety performance indicators(SPIs) by applying the balanced scorecard(BSC) that is used as a performance management model in both public and private organizations.*

*SPIs provide objective countermeasures for the organization's performance with regard to safety. In particular, SPIs of government organizations are used in policies to prepare for and mitigate large-scale risks and significant economic losses from accidents by analyzing and evaluating information on the frequency of accidents and the amount of damage expected in the event of an accident.*

*This research, ultimately aimed at developing the Army's SPIs, has been carried out with the following procedures: 1)check the policy directions set by the current government and the Ministry of Defense related to safety, and summarize the mission and vision of the army; 2)the perspectives of the balanced scorecard designed for corporate organization have been adjusted to suit the military's safety management environment, and the objectives of safety management have been defined; 3)the objectives and performance goals of the safety management strategies pursued by the Army are selected from the adjusted BSC perspectives; 4)and finally, 34 SPIs and 8 key performance indicators(KPIs) have been selected to measure the achievement of performance targets by BSC perspectives.*

*The selected indicators will be useful safety management measures only after identifying the official statistical data to be used to measure them and developing scientific calculation formulas that have been validated through simulation tests. Also, each of the indicators should be combined with inspection, investigation and audit methods to provide more reliable information on safety outcomes to the Army as well as the public. The results of this study may be used as a research material in establishing a performance management system for safety management activities of military and public organizations.*

**[Keywords] *Military Safety, Balanced Scorecard(BSC), Key Performance Indicator(KPI), Safety Performance Indicator(SPI), Strategic Map***

## 1. Introduction

The ministry of national defense of the Republic of Korea is striving to meet the public's standards on safety and human rights at various areas and levels, and actively implement a national political agenda related to the safety of the current administration. In particular, the ROKA established and continues to operate the combat preparation safety team(CPST) since December 2018, for the purpose of fulfilling its duties as an organization responsible for soldiers and to implement life, human rights and safety, all of which are

*This research paper is a supplement to "A BSC Framework to Create Safety Performance Indicators for Military Safety Management; Focusing on the TRIANGLE Project of ROKA" which was announced at the 2019 Korean Society of Civil Engineers(KSCE) convention held in October 2019.

universal and contemporary core values of mankind.

The CPST has redefined its vision and missions under the control of the Army headquarters and is working on a TRIANGLE project consisting of 31 tasks in four areas. TRIANGLE is an acronym of the strategic objectives(Trust, Risk-zero, Innovation) and practice(Action, Network, Gear, Law, Education & training). The organization is the first in the ROK Army to be organized as a safety professional organization, and until the present, it has been making major efforts to establish its performance system by identifying its duties and functions, establishing related organizations, and setting up task lists. The organization, meanwhile, is at a stage where it needs to come up with a performance management system that will systematically and effectively manage its missions, visions, and strategic goals.

The aim of this research was to set up safety performance indicators(SPIs) essential for the establishment of performance management systems for the Army. The study was conducted on the basis of the balanced scorecard model by means of literature research, observations, and expert discussions on the CPST. The findings can further contribute to the improvement of the military's safety management systems and may provide the necessary framework for objectively measuring safety management performances.

## 2. Previous Research

### 2.1. Development of performance evaluation indicators for government agencies using the balanced scorecard

An organization's performance management system helps to achieve its mission, vision, or strategic goals systematically and effectively, and to measure and manage the organization's performance from a variety of perspectives[1][2]. Government organizations as well as private organizations have continually studied SPI development models to more systematically and objectively measure their safety performance. The performance indicator development models commonly used by public organizations are the balanced scorecard(BSC), input – process – output - outcomes(IPOO), and quality – cost – delivery - productivity(QCDP)[3][4].

The BSC model[5], developed by Nolan and Norton as a multinational performance measurement system, has also recently been used as a performance measurement system for government and public institutions[2]. The BSC is designed to allow enterprises to assess their performance from the balanced perspectives, including three non-financial perspectives(customers, internal processes, learning and growth) that have been overlooked. This is in contrast to the traditional manner of measuring their performances only from a financial perspective[5]. The model is also structured to balance long- and short-term goals, lagging and leading indicators, and internal and external views on performance[5].

The BSC is a compilation of indicators derived from the organization's strategies, which are used as a tool to communicate success factors and results to the organization's members and external stakeholders to achieve its missions and strategic goals[1]. Meanwhile, performance management systems of government agencies are difficult to use when quantifying the objectives of the organization, unlike those of private entities, and the needs of various stakeholders should be considered[6]. Therefore, the application of BSCs as performance management systems in the public sector requires flexibility to be modified to suit the purposes and characteristics of the public organizations.

### 2.2. The nature and validity of SPIs

From the perspectives of the BSC, all activities to achieve the organization's strategies are measured by key performance indicators(KPIs)[5][7]. KPIs are indicators included in SPIs, the database used to monitor and measure the performance of the health and safety sectors being pursued by the organization[8]. SPIs are a means of investigating and assessing the processes and operations of safety systems applied to the organization, and are the indicators that can explain the relationship between the accidents that occurred and the safety measures applied[9][10]. SPIs are data-based parameters used to monitor and measure safety performance. These indicators also provide objective countermeasures for the organization's safety performance with regard to safety[11]. SPIs usually provide more reliable safety results in conjunction with methods of inspection, investigation and audit.

The general criteria for selecting desired SPIs are: 1)the fewer SPIs, the better; 2)maintaining links with the key success factors(KSFs) in safety policies; 3)the past, present, and future of safety management are expressed in a manifest manner; 4)and development based on the needs of customers, shareholders and stakeholders[12]. The properly selected SPIs provide objective measures for the organization's safety performances and serves as a powerful motivator in promoting safety behavior among its members[4]. The goals and objectives of the KPI or SPI should be established on the basis of accurate investigation and readjusted if the safety management environment and strategy changes[12].

## 3. Research Methods and Procedures

This study was conducted to provide the framework needed for the Army to develop SPIs. For this study, the performance management model[1] presented by Niven was adjusted to match the characteristics and environment of the military, and the KPIs and SPIs of the Army were selected through the four-step process described in chapter 4. Also, related literature analyses, expert discussions, and intensive observations of military safety management sites were mainly used as ways to enhance the reliability and validity of these findings.

## 4. The Framework for the Development of Military SPIs

### 4.1. Identifying the army's missions, visions and strategies

The missions, visions, and strategies concerning the safety of the Army have been clearly identified as shown in <Table 1> by reviewing the government's agenda(guaranteeing military personnel's human rights and drastically improving service conditions). These agenda items are closely aligned and more specific to the following policy tasks: the five-year plan for state administration related to national defense(establishing a safe society to preserve the safety of the people); the Department of Defense's military culture innovation plan(establishing an open barrack culture trusted by the people); and the defense policies(healthy and safe barracks, human rights-guaranteed barracks, and barracks with firmly built military morale).

**Table 1.** ROK Army's mission & vision for safety management.

| | |
|---|---|
| Mission | Enhance combat readiness through systematic safety management. |
| Vision | We ultimately contribute to the nation by ensuring the lives, human rights and health of the Army soldiers, eliminating non-combat losses, and fostering all soldiers as safeguards. |

### 4.2. Adjustment of BSC perspectives

These perspectives are the areas of safety management that are essential to the systematic and balanced management of the

Army's progress toward achieving its safety visions and goals. The BSC perspectives, which were designed to fit the corporate organization, have been adjusted to take into account the characteristics of the military organization. As a result, the "internal process" perspective, along with the "learning and growth" perspective, was accepted as suggested by Niven, but "customers" of the remaining views were adjusted to "customers and stakeholders" and "financial" to "resources" as shown in <Table 2>.

**Table 2.** BSC perspectives and purposes.

| BSC | Purposes |
|---|---|
| Customers<br>&<br>Stakeholders | It provides military services that satisfies customers(military personnel and people) by guaranteeing the human rights and security of soldiers, ultimately enhancing the credibility of the nation's military, and improving the competitiveness of defense Organizations |
| Internal<br>process | Through safety management activities, it minimizes the loss of the human and material resources of the military to prevent non-combat loss(tangible elements) and recognizes the value of life respect to soldiers, thereby cultivating self-esteem and unity(intangible element) |
| Resources | Secure the necessary personnel, organizations, budgets, equipment and facilities for systematic safety management activities and utilize them efficiently |
| Learning<br>& growth | Innovate & systemize safety management programs to create safe military environments, strengthen internal safety infrastructures by accumulating intelligences on safety, and ultimately establish an interdependent safety culture |

### 4.3. Strategic mapping for safety management

Strategic mapping is a useful way to transform strategies into tangible goals and measurable indicators[8][13]. The map as shown in <Table 3> has been drawn up by setting 4 strategic goals and 12 performance tasks that the Army should focus on in order to achieve their missions and visions identified in the first phase under the coordinated BSC perspectives in the second phase. The strategic map is a schematic diagram of the relationship between the critical success factors(CSF) that the Army needs to achieve its mission. This map clearly shows members of the Army how the safety management tasks they perform relate to the Army's visions and strategies for safety.

**Table 3.** Safety management strategy map of ROKA.

| Mission | Enhance combat readiness through systematic safety management | | | |
|---|---|---|---|---|
| Vision | • Securing the lives, human rights and health of the Army soldiers<br>• Eliminating non-combat losses<br>• Establishing safeguards for all soldiers | | | |
| BSC perspectives | Customers & stakeholder | Internal process | Resources | Learning & growth |
| Strategic goals | Ensure the safety of soldiers, and enhance the credibility of the people | Develop safety-related laws and organizations, eliminate tangible and intangible risks and threats | Secure the necessary resources for safety | Establish the interdependent safety management system |

| | | | | |
|---|---|---|---|---|
| Performance tasks | 1. Increase of customer satisfaction<br>2. Setting up an Improved culture of life<br>3. Establishment of an equal gender culture | 4. Development of institutions & doctrines<br>5. Optimization of safety organizations<br>6. Risk assessment, safety diagnosis & training<br>7. Establishment of accident response system | 8. Securing of professional manpower<br>9. Securing of safety facilities, equipment, supplies & budgets<br>10. Establishment of a safety collaboration network | 11.Strengthening safety leadership<br>12. Creating a climate of safety |

### 4.4. Creating KPIs & SPIs for the ROKA

KPIs and SPIs shown in <Table 4> are indicators of the performance of activities being undertaken to achieve the Army's safety management strategies. KPIs are also a means to assess the status of changes or to evaluate the degree of performance achieved by CSFs or targets. Performance goals and indicators that faithfully reflect the organization's missions and characteristics serve as guidelines for a detailed action plan to achieve the organization's strategies. In addition, well-established BSC effectively describe the organization's strategies through measuring indicators linked to strategic objectives. Indicators can be divided into performance motivators(leading indicators marked in blue) and outcome indicators(lagging indicators), which should be chain-linked to account for causalities between each other. The criteria applied in selecting KPIs are:1)conformity with the objectives of the BSC perspective; 2)representativeness of safety management activities by perspective; 3)the possibility of measuring performance; 4)and the possibility of clearly describing the process. <Table 4> summarizes the results developed in consideration of the nature, function and criteria of the performance indicators.

General organizations separate safety and health indicators from the selected KPIs and develop them into SPIs. However, the KPIs of the CPST are all analyzed to be SPIs because the organization is dedicated exclusively to the safety of the Army. Therefore, among the performance management tasks for the safety and health of the Army, indicators for one-off projects in the CPST have been divided into KPIs, with the remaining indicators selected as SPIs.

**Table 4.** Military safety performance indicators & key performance indicators.

| BSC | Safety performance indicators(leading indicator, lagging indicator) |
|---|---|
| Customers & stakeholder | 1-1 Reliability of military safety<br>1-2 Service satisfaction with safety management service<br>1-3 Suicide incidents occurred(persons) |
| | 2-1 Suicide prevention education completion rate(%)<br>2-2 Securing rate of suicide prevention counselors & instructors(%)<br>2-3 'Green Camp' operation rate(%)<br>2-4 Operation rate of “Field Support Team” of combat preparation safety team(%) |
| | 3-1 Number of incidents of sexual violence(case)<br>3-2 Percentage of education completed to improve gender awareness(%)<br>3-3 Number of gender equality consultants secured and their operational performance(%) |
| Internal process | 4-1 Safety SOP and process maintenance rate(%)<br>4-2 Number of adoption of safety systems and doctrinal development proposals(case) |
| | 5-1 Operational performance of safety organization |

| | |
|---|---|
| | 6-1 Safety assessment implementation rate for training sites(%)<br>6-2 Implementation of special health examination for workers in hazardous environments and implementation rate of health education(%)<br>6-3 Environmental measurement implementation rate for hazardous environment workplace(%)<br>6-4 Regular inspection rate for major management accident-related facilities and equipment(%)<br>* ammunition storages, oil storages, cooking areas, shooting ranges, training ranges, etc |
| | 7-1 Integrated accident response training rate(%) |
| Resources | 8-1 Securing professional qualifications and utilization rate of safety managers and staff for safety diagnosis(%) * trainee safety manager, suicide prevention institution, professional counselor, lifeguard |
| | 9-1 Secure safety protector and utilization rate(%)<br>9-2 Safety-related budget execution rate(%) |
| | 10-1 Network composition and collaboration rate with external safety specialized agencies(%) |
| Learning & growth | 11-1 Safety leadership diagnostic index |
| | 12-1 Safety information provision and utilization rate(%)<br>12-2 Identifying and reporting rates for near misses(%)<br>12-3 Utilization of safety culture content(%) |
| KPIs | 4-1 Enactment of the basic law on military safety management<br>4-2 Enactment of the army safety management regulations |
| | 5-1 Organization for safety precautions<br>5-2 Operation of the joint safety monitoring unit |
| | 9-1 Development of an accident information database<br>9-2 Development of smart safety management programs<br>9-3 Development of new concepts of shooting ranges<br>9-4 Establishing safety standards for shooting ranges by firearm and shell type |

## 5. Conclusions

This study was conducted to measure the outcomes of military safety management activities actively promoted by the combat preparation safety group, which the ROK Army launched to establish the safety culture in terms of combat readiness. A total of 34 SPIs have been selected from four perspectives as a result of the study using the BSC model, and eight of these indicators have been adopted as KPIs.

The indicators presented in this study will have to go through the process of analysis by professional research organizations in the future to determine whether they are key success factors in achieving the missions and visions of the CPST, and as a result, those that are selected as KPIs for the Army will require set goals in order to be achieved. The goals set out in these processes will be allocated to the relevant units and departments, and the operational organizations assigned to achieve the goals will go through the process of selecting the items to be promoted and then develop detailed plans. In addition, in order to ensure objectivity and fairness, it is required to find and apply official statistical data to be used for each indicator or index, and the scientific calculation formula must be developed and verified through simulation tests.

## 6. References

### 6.1. Journal articles

[2] Kim EH. A Study on Development of Key Performance Indicator Using BSC for Public Service: A Case of Elderly Welfare Service. *Korean Public Administration Quarterly*, 22(2), 349-375 (2010).

[3] Chung KS. A Model for the Development of Performance Indicators by I-O System Approach and Integration with BSC. *Journal of the Korean Production and Operation Management*, 2(4), 399-415 (2011).

[4] Chung KS. A Comparative Study among KPI Developing Methods. *The Korean Society for Quality Management*, 46(4), 863-876 (2018).

[5] Kaplan RS & Norton DP. The Balanced Scorecard: Measure that Drive Performance. *Harvard Business Review*, 83(7), 71-79 (1992).

[6] Jang DH & Shin Y. Introducing the BSC as an Evaluation Methodology for Local

Enterprises: Based on the Results of the Awareness Studies of the Urban Development and Facilities Management Operations' Evaluation Teams. *The Korea Local and Administration Review*, 20(1), 191-219 (2006).

[7] Kaplan RS & Norton DP. Using the Balanced Scorecard as a Strategic Management System. *The Harvard Business Review*, 85(7-8), 150-161 (2007).

[9] Kim J & Francine S. Guidance on Developing Safety Performance Indicators. *Process Safety Progress*, 28(4), 362-366 (2009).

[10] Louvar J. Guidance for Safety Performance Indicators. *Process Safety Progress*, 29(4), 387-388 (2010).

## 6.2. Thesis degree

[11] Seol JW. A Study on Risk Based Audit Methods using Process Safety Performance Indicator. Kwangwoon University, Doctoral Thesis (2019).

## 6.3. Additional references

[1] Niven PR. Balanced Scorecard Step by Step: Maximizing Performance and Maintaining Results. John Wiley & Sons (2002).

[8] Yoon SJ & Kim GS. Application Strategies on the BSC Model of Public Performance Evaluation System. Korea Institute of Public Administration (2005).

[12] Brown MG. Keeping Score: Using the Right Metrics to Drive World-class Performance. Quality Resources (1996).

[13] Kaplan RS & Norton DP. Strategy Maps-Converting Intangible Assets into Tangible Outcomes. Harvard Business School (2004).

**Author**

**Kwon Hyuck-shin** / Seoul National University of Science and Technology Researcher

B.A. Chonnam National University

M.A. Kyunghee University

Ph.D. Seoul National University of Science and Technology

Research field

- The Study on CEO Leadership Characteristics in Public Firm based on Korean Style Leadership Framework: The Case of Cho, Hwan-ik in KEPCO, Journal of Creativity and Innovation, 10(4) (2017).
- Creating Sustainable and Climate Shared Value in Public Institution: Lessons from a Case of Korea Army Cadet Military School, Sustainability, 11(14) (2019).

Major career

- 2014~2016. The 31st Infantry Division, Commanding General
- 2017~2019. Army Cadet Military School, Commandant