A Cyber Command and Control Framework for Psychological Operation Using Social Media

Kyoungmin Kim[1], Junwoo Seo[1], Mookyu Park[2], Moosung Park[3] and Kyungho Lee[2]
[1]*Seoul, Korea University, Department of Cyber Defense(CYDF), Republic of Korea*
[2]*Seoul, Korea University, Institute of Cyber Security & Privacy(ICSP), Republic of Korea*
[3]*Seoul, Agency for Defense Development(ADD), Republic of Korea.*
richard2104@korea.ac.kr

***Abstract*— Global threats, international terrorist groups and North Korea, paralyze political decisions by attacking and neutralizing the credibility of the main policy makers in the state and simultaneously manipulate the public opinion, which results in distrust and disconnection between each other. These threats use social media as their biggest core routine to conduct such attacks. This paper presents a series of processes and frameworks on how a commander should make a decision when performing a cyber psychological operation using social media. Based on the Endsley model, which is a situational awareness model, the paper compares the strengths and weaknesses of the three social media operations (IGMO, DeSMO, OSMO) performed by the military and proposes a guideline for performing an operation.**

***Index Terms*— Command&Control(C2); Cyber Psychological Warfare; Information Operation; Situational Awareness; Social Media Operation.**

I. INTRODUCTION

Global threats, international terrorist groups and North Korea, use various tools to strengthen their influence worldwide. Social Media, due to its convenience, are increasingly used by the global threats to accomplish their purposes and spread their message [1]. For example, Al-Shabaab used Twitter during its attack on the Westgate Shopping Mall, and the terrorist group Islamic State of Iraq and Syria (ISIS) uses social media when releasing threatening videos of beheadings. These attacks, also called as cyber psychological warfare, refer to the planned use of propaganda or any other instruments that affects the views, feelings, attitudes, and behaviors of the target country and group to achieve the attacker's policy goals in cyberspace. Specifically, cyber psychological warfare is getting more and more popular due to the anonymity of cyberspace, and the widespread ripple effects that overcome spatio - temporal constraints. International terrorist groups have shown cyber psychological warfare to propagate the brutal scenes of terrorist acts such as destruction of enemy facilities and suicide bombing and murder of prisoners, publicizing their activities and rallying support. They see their mission as not only simply creating terror among its foes, but also delivering their messages [2]. Recent cyber psychological attacks have been accelerated by the rapid spread of SNS (Social Networking Service) such as Twitter, Instagram, Facebook and YouTube. SNS has become a very effective means of multimedia communication that transmits news at the speed of light. It enables distribution of almost real-time information to a wide variety of unspecified persons as well as SNS users. Due to these strengths, 90 percent of terrorism on the Internet takes place using social networking service [3]. As the social media power and efficacy proved, the military begins to study whether it could be used as a tool of cyber psychological warfare.

In a study by Clay Shirky from the New York University, Shirky said discussion of the political impact of social media has focused on the power of mass protests to topple governments [4]. Furthermore, in a study by Umong Sethi from the Indian Army, Sethi said that monitoring of the social media over time is a useful tool to gather information regarding various trends and undercurrents among the target audience to counter insurgency and terrorist situations [5]. According to these studies, social media operations can have value at the operational and tactical levels, and directly contribute to the effectiveness of Cyber Intelligence, Surveillance, and Reconnaissance (also called Cyber ISR) and Cyber Operational Preparation of the Environment (Cyber OPE). For example, by gathering direct content and metadata, the operator can get to the specific software and hardware configuration or physical location of the target [6]. Social media can also provide a useful attack platform as an alternative Command and Control (also called C2) [6]. Taking advantage of these strengths, social media can be a key means to hold dominant position during warfare. However, there is no process for cyber psychological warfare using social media directly. This paper presents a set of standards and frameworks for the military commander to decide what kind of social media operation (SMO) should be taken when conducting cyber psychological warfare. To illustrate this process, the paper used the Endsley Model, which has long been the military command and control decision-making body.

II. BACKGROUNDS

This section describes the background to the two most important concepts in this paper, the Endsley model and the Factor Analysis of Information Risk (FAIR) methodology. The Endsley model serves as a main framework proposed in the paper, and the FAIR methodology is used to support the Endsley model.

A. Endsley Model

The three-step model of situational awareness was initially developed to understand air operations, but it could be extended to other areas such as power generation, petrochemicals, nuclear power, and command and control. Endsley's model describes the SA state and describes three

stages of SA formation: perception, comprehension, and projection[7]. As shown in Figure 1, the Endsley model is divided into three stages.

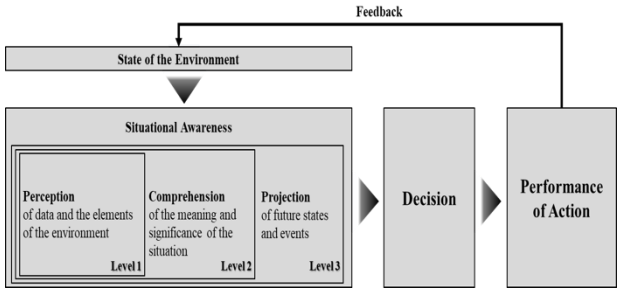

Figure 1: The Brief figure of Endsley's Situational Awareness Model

1) Level 1 SA: Perception of Data and the Elements the Environment

This is the lowest level of situational awareness and it relates to the pilot's awareness of aircraft instrumentation, aircraft behavior, terrain, air traffic control, and other aircraft information in the sky. At this stage, no interpretation of the data is performed and only the initial receipt of information in its raw form is represented. If the data could be extracted at this stage, the operator will be able to see the status of the specific variable but will not be able to consolidate the data.

2) Level 2 SA: Comprehension of the Meaning and Significance of the Situation

If the data can be integrated and synthesized to understand the relevance of the pilot's work, comprehension can be derived from the perception of the elements. The comprehension phase (e.g. the time and distance to the remaining fuel, the tactical status of the threats, the mission status, etc.) is necessary for the understanding of the importance of factors and their progress. In this way, the pilot can determine if there is an intended outcome in his action. Endsley argued that the level of achieved understanding represents the pilot's expertise. Individuals with less skilled can achieve a lower level 2 SA, despite achieving the same level 1 SA as a skilled opponent.

3) Level 3 SA: Projection of Future States and Events

This is the highest level of situational awareness and relates to the ability to predict the future of environmental elements (e.g. potential aircraft collision predictions). The accuracy of predictions depends largely on the accuracy of Level 1 SA and Level 2 SA. Projections of anticipated future situations give pilots sufficient time to resolve conflicts and develop action plans to achieve them.

B. Factor Analysis of Information Risk (FAIR)

FAIR is the standard quantitative model for information security and operational risk [8]. It is both a taxonomy of the information risk factors and a risk management framework [9]. Additionally, FAIR provides a method for measuring the factors that are related to an information risk. Figure 2 explains the relationship of the factors.

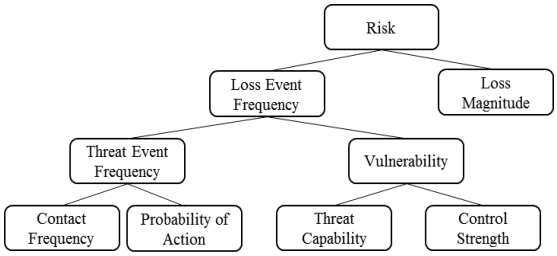

Figure 2: Factoring Diagram of FAIR Model

FAIR emphasizes the risk as an uncertain property, which should focus on how probable is a given event. Specifically, risk is comprised of the probable frequency and probable magnitude of future loss. In other words, it is about how frequently loss is likely to happen and how much loss is likely to result.

To estimate the degree of the risk, FAIR model describes four stages. In each stage, several risk factors and concepts are included.

The first stage of risk is identifying Scenario Components: the asset and the threat agents. According to the Introduction to Factor Analysis of Information Risk, the asset is defined as any data, device, or other component of the environment that supports information-related activities, which can be illicitly accessed, used, disclosed, altered, destroyed or stolen, resulting in a loss. Further, it is claimed that the threat is anything that can act against an asset in a manner that can result in harm. Drawn from this definition, this study specified the asset as military confidential documents and the threat agents as technical hackers, which is not an insider or a spy.

The second stage is evaluating the Loss Event Frequency(LEF). LEF is the probable frequency, within a given time-frame, that the loss will materialize from a threat agent's action. LEF is composed of two factors called the Threat Event Frequency(TEF) and the Vulnerability(Vuln). TEF, which is the probable frequency that threat agent will act in a manner that may result in a loss. It is comprised of the Contact Frequency(CF) and the Probability of Action(PoA). Furthermore, Vuln, which is the probability that a threat agent's actions will result in a loss, is comprised of the Threat Capability(TCap) and the Difficulty(Diff).

Table 1
Table of Risk Generation

		Risk				
	SV	H	H	C	C	C
	H	M	H	H	C	C
PLM	Sg	M	M	H	H	C
	M	L	M	M	H	H
	L	L	L	M	M	M
	VL	L	L	M	M	M
		VL	L	M	H	VH
				LEF		

The third stage is evaluating the Probable Loss Magnitude (PLM). PLM is the concept of loss that materializes directly as a result of the event.

The final stage is deriving and articulating risk. Risk is simply derived from LEF and PLM, which are estimated in the previous stages. Table I is used for articulating risk qualitatively. "C" stands for "Critical", "H","M" and "L" is "High", "Medium", "Low" respectively. Additionally, "SV: stands for "Severe", "Sg" is "Significant".

III. Related Works

A. The Social Side of 'Cyber Power'? Social Media and Cyber Operations [6]

This paper categorized military social media operations into three types: information-gathering (IGMO), defensive social media operations (DeSMO), and offensive social media operations (OSMO).

According to the paper, Information Gathering Media Operation(IGMO) focuses on passive information-gathering. It can be used for monitoring adversary activities and for targeting. Through IGMO, military and intelligence agencies monitor and document social media activities passively, rather than interacting with known social media actors. IGMO deals with two types of data: direct data collection and metadata. Direct data collection is the content displayed on social media, and the metadata reveals important details such as the location of target, the time that the target is active and many others.

On the other hand, Defensive Social Media Operations (DeSMO) is more active than IGMO. DeSMO can be used as counter- messaging or counter-propaganda. DeSMO does not play a direct role in terms of cyber operations. However, it is recognized as a key component of the deradicalization campaign.

Offensive Social Media Operation (OSMO) is more aggressive than the broadcasting or counter-narrative tool, which is the role of the existing SMO. Specifically, OSMO covers information gathering, information campaigning, providing accurate cyber effects, responding to the social media features of the opponent, degrading, denying or destroying.

B. Data to Decisions for Cyberspace Operations [10]

The paper describes the data driven decision-making functions needed to effectively perform cyber operations. According to the paper, in cyber operations, big-data collection is the key factor. Based on the collected data, there are three categories of decision-making: automatic, assisted and discovery.

Automatic decisions are made by an automated system that analyzes data in real time for the purpose of responding to changes in the state of the network. It is determined by the data collected by the network sensor or device within a few seconds. (e.g. Intrusion Detection System, Firewall, et cetera)

Assisted decisions determine the identification of cyberspace events, the threat vectors used, and the determination of the technical impact of the incident on support using analytical tools and decision support tools.

Discovery Decisions is a decision to manually analyze larger amounts of data. There are activities such as determining the impact of a mission, the attributes of enemy action, and the identification of hostilities.

Previous studies above analyze the strengths and weaknesses of social media operation and the categories of data-based decision-making. Data collection, linked as IGMO, is important for the appropriate decision-making; hence, how the commander conducts these operations becomes important. This paper combines the above social media operations with the Endsley Model to provide guideline on how to conduct the operation.

IV. Proposal Method: Endsley's Situational Awareness Model

This section describes a proposal method to explain the process of determining social media operations. In this paper, the three types of social media operations (IGMO, DeSMO, OSMO) is defined as the commander's final goal. With this goal, the paper presents the guideline for the commander to make decision, based on the Endsley Model. Figure 3 shows a process used in this paper. The paper focuses on situational awareness section for proper decision-making. Situational awareness is a three-stage process, with the following components: (1) Perception of data and the elements of the environment (2) Comprehension of the meaning and significance of the situation (3) Projection of future states and events [7]. Therefore, a commander acting in the environment should first gather observable information; selectively attend to the information that is most relevant to the task at hand; integrate incoming information with existing knowledge and make it understandable in light of the current situation; and finally, predict changes in the environment and subsequently the changes of incoming information [11].

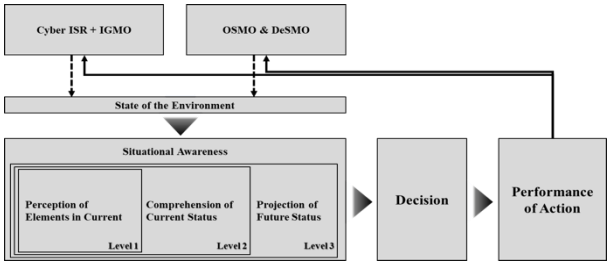

Figure 3: Endsley Model and Social Media Operation

Table 2
Strength and Weakness of IGMO

Strength	Score (%)
The extent and usefulness of the collected information to the army (Level 2)	Our army's utility to lose with false information of the enemy (Level 2)
A small information risk exposure of our military by conducting IGMO (Level 1)	The possibility of social media platform blocking SMA (Level 3)

V. Social Media Operation

This section describes how each level of the Endsley Situation Awareness Model will be applied to social media operations and the factors that the commander must consider when determining the SMO.

A. Situational Awareness in Social Media Operation

1) Perception (Level 1 SA)

The first step to achieve SA is to recognize the data as well as the status and attributes of relevant elements in the social media environment. The data mentioned here are the data acquired through the IGMO. This paper assumes that IGMO is a task that is always performed and that it determines whether IGMO needs further execution in the decision-making stage. As mentioned previously, *data* obtained through IGMO are divided into direct content and metadata.

The *relevant elements* of the social media environment are

classified as social media platform (SMP) and social media account (SMA). The *status* of SMP is expressed by the degree of activation. The degree of activation can be determined by the number of active users, the average number of connections between users, and the average logged -in time of users. For example, Facebook has 845 million active users, the average Facebook user has 130 friends and the average visit to Facebook lasts for 23 minutes. The *attributes* of SMP are directly related to the purpose of average users using SMP. For example, Linkedin is often used for business purposes as compared to other SMPs. The attribute is determined by two factors, the first of which is the SMP policy that limits the format of the data. Facebook, for example, has no limitation on the format of data. Twitter, however can only deliver information in 140 characters. With these limitations on the format of data, people use the platform differently, and the attributes of the platform also change. The second attribute of the SMP is the difference in information retention policy. The *attributes* of the platform depend on the degree of regulation of the user's information.

If the SMP was a macroscopic concept, the SMA is a microscopic concept. As described above, the *status* of SMA is also expressed as the degree of activation. The degree of activation in SMA can be determined by the number of links (followers), number of posts, and number of Likes (Retweet) per day. The *attributes* of SMA is related to the purpose of the account using SMP.

2) Comprehension (Level 2 SA)

The next step in SA formation is synthesizing the separated Level 1 SA elements through pattern recognition, interpretation, and evaluation processes. This level incorporates the information that was segregated in Level 1 to understand the impact on the military's goals and objectives. In other words, it analyzes collected social media information and finds meaningful information.

For instance, based on the direct content, one can analyze the characteristics of the SMA's writing or analyze the psychological and sociological meaning of the content. In addition to quantitative pattern recognition algorithms, the ability of the commander to recognize the situation is also important when analyzing the data.

3) Projection (Level 3 SA)

The third level of SA includes the ability to project the future behavior of an element in the environment.

Thus, in addition to the information analyzed through Level 2 SA Comprehension, further considerations include how the SMP and SMA will be used by the enemy and whether the benefits gained prior to Level 2 are sustainable elements in the future.

B. Factors to Consider when a Commander Decides Social Media Operation

Below is a list of criteria that can be used in the situational awareness phase to determine each SMO.

1) IGMO

As mentioned above, IGMO assumes to be a frequently performed task. The data collected through the IGMO applies to Endsley's situational awareness. At this time, according to SA Level 1 and 2 mentioned above, it is necessary to confirm whether it is perceivable information. The IGMO should be performed consistently because it is a component of the effective Cyber ISR in the social media operation.

The factors that the commander should consider in order to determine the IGMO are listed in Table 2. For each factor, the magnitude can be determined qualitatively by the commander. IGMO should be implemented if their merits and risk totals are positive.

Each element has a level of Endsley model. This allows us to compare the strengths and weaknesses of IGMO in light of Endsley's situational awareness.

2) DeSMO & OSMO

status of relevant elements

SMP \ SMA	Very Low	Low	Moderate	High	Very High
Very High	M	H	VH	VH	VH
High	L	M	H	H	H
Moderate	VL	L	M	M	M
Low	VL	L	L	L	L
Very Low	VL	VL	VL	VL	VL

Figure 4: Status of Relevant Elements

Based on the methodology of Factor Analysis of Information Risk (FAIR), the paper designed a criteria table to help the commander qualitatively judge which SMO to carry out. To determine whether enemy's OSMO is threatening or ally's DeSMO is effective, the commander should first consider the status of SMP and SMA. The commander can divide the status of SMP and SMA based on qualitative criteria as shown in Figure 4 and jointly consider them based on the status of relevant elements.

VI. CONCLUSION

This paper introduces a set of guidelines and procedures for the types of social media operation to be used by a commander. By introducing the framework of the social media operation for the first time, the commander can learn a series of processes to reasonably manage the social media operation. Specifically, we defined information at each state which are related to the Endsley's model so as to be specialized in social media operation and explained how the three levels of situational awareness are applied. This paper also takes into consideration that the social media has a disadvantage of giving unintended benefits to the enemy because of the bidirectional property. Therefore, if the commander is concerned about the current state and the projection of future status using the framework, the bidirectional property could be considered as it allows for the calculation of the utility and the damage of the enemy and the military. Using the Endsley model and the FAIR model, it can be applied not only to the Situational Awareness but also to the Battle Damage Assessment of the Social Media Operation. However, this paper does not fundamentally solve the doubts that the effects of SMO are marginal [6]. First, SMO's benefits are not universal. According to other studies, SMO only works on conflict areas that have a high degree of connectedness and social media activity. The positive view of this limitation is that the problem will be solved in the near future when the social media becomes universal as the spread of social media

becomes rapid due to the increased desire for IT worldwide. In addition, it should be performed in the real time considering the sophisticated and continuous monitoring is required due to the entangled social media network. Finally, continuous monitoring and countermeasures are needed in order to operate it effectively.

ACKNOWLEDGMENT

This work was supported by Defense Acquisition Program Administration and Agency for Defense Development under the contract. (UD060048AD)

REFERENCES

[1] Farwell, James P.," The media strategy of ISIS. Survival", 2014, 56.6: 49-55.

[2] Jenkins, Brian Michael.,"Is Al Qaeda's Internet Strategy Working?", 2011.

[3] Weimann, Gabriel.," New terrorism and new media", Washington, DC: Commons Lab of the Woodrow Wilson International Center for Scholars, 2014.

[4] Shirky, Clay, " The political power of social media: Technology, the public sphere, and political change", Foreign affairs, 2011, 28-41.

[5] Sethi, Umong," Social Media-A Tool for the Military", Centre for Land Warfare Studies, 2013.

[6] Herrick, Drew, " The social side of 'cyber power'? Social media and cyber operations.," In: Cyber Conflict (CyCon), 2016 8th International Conference on. IEEE, 2016. p. 99-111.

[7] Endsley, Mica R.," Toward a theory of situation awareness in dynamic systems", Human factors, 1995, 37.1: 32-64.

[8] Fair Institue. (2017). [Online]. Available: http://www.fairinstitute.org/

[9] Jones, Jack," An introduction to factor analysis of information risk (fair)", Norwich Journal of Information Assurance, 2006, 2.1: 67.

[10] Stone, Steve, "Data to Decisions for Cyberspace Operations", Military Cyber Affairs, 2015, 1.1: 6.

[11] Munk, Sandor," Situational awareness (data) bases in military command and control", Information Technology, 2004, 3.3: 373-385.