Flexible and Enhanced Cyber Threat Intelligence: Research on Advanced Analysis Methods

Won-Chul Kim[1], Ki-Woong Park[2]*

[1] SysCore Lab., Sejong University, Republic of Korea
[2] Department of Computer & Information Security, Sejong University, Republic of Korea
atc1827@gmail.com, woongbak@sejong.ac.kr

Abstract

To minimize damage from cyberattacks, it is important to collect and analyze various types of threat information prior to inferring the attacker's intent.

The intensity and persistence of a cyberattack are often driven by attacker's motive; understanding this motive enables a more efficient response, helps narrow down potential attackers, and supports proactive defense.

This study explores methods for classifying attack groups and inferring their intentions by measuring the similarity of Indicators of Compromise (IoCs) and Tactics, Techniques, and Procedures (TTPs) based on attackers' characteristics, resources used, attack techniques, and socio-economic damage analysis.

This study identifies the strengths, weaknesses, and limitations of existing attack group classification methods, derives core elements for analyzing attack intent, and proposes a combined approach that integrates IoC and TTP similarity-based comparison with damage analysis methods. This approach enables the inference of attack intent even in the early stages of a cyberattack.

We present a method for inferring attackers and their intent by analyzing targets and observed attack damage during the early to middle stages of an attack.

Keywords: CTI, IoC, TTPs, Cyberattack groupings, Cyberattack intent

1 Introduction

The internet provides anonymity and secrecy, enabling attackers to reach their targets.

Unlike individual hackers of the past who acted to showcase their abilities, today's attackers are more organized, with a significant increase in state-sponsored hacking group activity [1].

The 2020 SolarWinds hacking incident serves as a prime example. A hacking group known as "Cozy Bear," believed to be linked to Russia, inserted malicious code into the update process of SolarWinds, an IT monitoring software, allowing them to infiltrate over 18,000 organizations, including the U.S. government agencies, major corporations, and research institutions. This attack was not merely cybercrime but represented a form of cyber warfare driven by geopolitical tensions and political motives. Cyberattacks can be categorized by various actors, including state-sponsored cyber warriors engaged in cyber warfare, individuals or organizations motivated by financial gain, hacktivists expressing political grievances, and terrorists aiming to instill public anxiety [2-5].

Cyberattack groups operate with varying purposes; therefore, proactive response requires rapidly inferring both the responsible group and their intent.

Understanding an attacker's intent enables proactive responses and informed strategic decision-making.

In the early stages, the focus was on analyzing hacking techniques to detect and block cyberattacks, rather than identifying attack groups and their intentions. This led to the development of signature-based detection methods [6-11].

Signature-based detection methods rely on values including resources used in attacks (e.g., IP addresses, domains, URLs), hash values of malicious code, and specific code strings. These attributes are treated as characteristics of attackers or attack groups and are used to classify attacks from the same source by comparing them with past incidents.

Values such as IP addresses and domain used in this context are referred to as indicators of compromise (IoC) [12] and continue to be utilized for identifying attackers or attack groups.

IoC analysis employs case-based reasoning (CBR), a traditional investigative technique that predicts the outcomes of new cases by referencing past incidents.

Case-based reasoning relies on a similarity metric to measure the degree of resemblance between past cases and current cases [13-14].

Researchers have studied methods for identifying the same attacker or attack group by analyzing reused attack resources or measuring similarity. Additionally, many studies have focused on comparing other IoCs, such as hash values of malicious code, types of APIs used, programming languages, and development environments, to attribute attacks to specific actors.

However, advances in IP technologies and development environments have enabled attackers to intentionally mislead or conceal IoC values, hindering the identification of attackers or groups.

With the recent emergence of Advanced Persistent

*Corresponding Author: Ki-Woong Park; Email: woongbak@sejong.ac.kr
DOI: https://doi.org/10.70003/160792642025112606010

Threat (APT) [15] attacks, carried out covertly and continuously, attackers and groups are increasingly using anti-forensic techniques to deliberately deceive analysts, making attacker classification more challenging [16].

To counter APT attacks, frameworks such as the cyber kill chain and Tactics, Techniques, and Procedures (TTPs) have been developed to identify the stages of cyberattacks, the technologies and procedures used at each stage, and the associated tactical objectives [17].

According to the Pyramid of Pain [18], altering or deceiving TTPs is more costly for attackers than manipulating or concealing IoCs, making TTPs more difficult to change. Ultimately, understanding attack intent allows decision makers to establish effective response strategies based on high-level cyber threat Intelligence (CTI) [19]. Therefore, accurately identifying the attack intent of cyber-attackers or groups enables efficient responses and facilitates proactive defense by enabling attack prediction.

However, with advancements in information technology (IT) environments, attack techniques and tools have become more standardized, and attackers are increasingly using automatically generated malware, making it difficult to distinguish unique characteristics. Consequently, research has shifted toward comprehensive analysis to extract correlations and identify attack intent, rather than responding to each attack individually [20].

CTI has emerged as a key technology for collecting large volumes of cyber threat information, performing correlation analysis, and supporting strategic decision-making by understanding insights into the intent and significance behind attacks [21-23].

CTI analysis typically focuses on technical, operational, and tactical levels; however, addressing strategic CTI requires the ability to infer attack intent. To this end, research has explored methods such as analyzing socioeconomic damage to better understand attacker's objectives [24].

In this study, we compared and analyzed existing methods for classifying attackers and groups, conducted the strength and weaknesses of each method, identified their limitations, and proposed a new method for inferring attack intent.

The remainder of this paper is organized as follows: Section 2 derives the advantages, disadvantages, and limitations of existing attack group classification methods, CTI analysis, and threat intelligence sharing approaches.

Section 3 presents a new framework for inferring attack intent during the early and middle stages of a cyberattack, building on the strengths and limitations identified in Section 2. Section 4 discusses the study's limitations and concludes with directions for future research.

2 Related Works

2.1 Attack Group Classification Method

In the past, proactive responses to cyber-attacks primarily focused on identifying attackers or attack groups, rather than analyzing their underlying intentions.

A review of existing research on cyber-attack group identification categorizes these efforts into six perspectives:

(1) Attacker Features: Classifying attackers based on personal characteristics

(2) Resource: Identifying attack groups through similarities in attack resources (e.g., IP addresses, URLs, domains) used by attackers.

(3) Techniques: Classifying attackers based on similarities in attack techniques, such as malware API usage patterns and frequently used keywords).

(4) TTPs: Grouping attackers by the similarity of TTPs used to reach their targets.

(5) Harm: Assessing classification based on the impact of cyberattacks, including financial loss, information theft, or system disruption.

(6) Attack Intent: Identifying the underlying intent behind a cyberattack can help infer the responsible attack group.

The classification methods mentioned above will be discussed in detail in the following chapter.

2.2 Attacker Features

In 2014, Kapetanakis proposed a method for characterizing attackers using eight attributes, including "technology" and "gender" [13]. This study utilizes attacker profiling techniques, considered a subset of CBR, to identify characteristics of attackers involved in security incidents. As shown in Table 1, the eight observable characteristics are technical proficiency, risk avoidance, educational background, gender, predefined objectives, speed, errors, and forensic prevention measures.

Table 1. Attacker features and observability

Feature	Observable
Skill	No
Education	No
Risk	No
Gender	No
Goal	No
Speed	Yes
Mistakes	Yes
Anti-forensics	Yes

In this study, three attacker characteristics— such as speed, were observable from the defender's perspective, while the remaining five— such as technical skill, were difficult to determine through direct observation. Therefore, our research focused on identifying attackers using only observable characteristics.

2.3 Resources used in the Attack

This study infers attack groups by classifying them based on the similarity of attack resources, (such as IP addresses, URLs, domains) used during cyberattacks, as part of an IoC-based analysis [25].

Figure 1 shows how IoC-based analysis extracts IoCs from cyberattacks and compares them with previously analyzed attacker profiles and open-source Intelligence (OSINT) [26] data to identify attackers or groups.

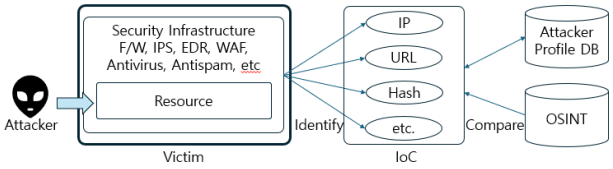

Figure 1. Overview of IoC-based cyber-attack groupings

In 2015, the Cyber Security Research Team at the Korea Internet & Security Agency (KISA) [27] proposed that identifying similarities in domains used during attacks can help attribute incidents to the same attacker or attack group, thereby enabling proactive responses to cyberterrorism conducted by groups with shared objectives [25].

2.4 Attack Techniques

As described in Section 2.3, IoC-based analysis methods examine malware to extract API usage patterns and frequently used phrases for identifying attackers or groups. In a 2015 study by KISA, similar approaches were applied to classify the attackers or groups. However, a 2014 study by Kim Wan-ju et al. identified attack groups by integrating OSINT with multiple digital clues, including EML files, attachments, and malware, used in attacks. They proposed a framework to monitor the reuse of identified attackers and attack resources, enabling the prediction of future attacks and facilitating proactive responses [28].

In 2013, Mohaisen et al. classified malware groups based on API behaviors observed during malware execution to identify common attackers [29-33]. They also analyzed botnet command-and-control channels to examine attack resources controlled by the same attacker [34-35] and studied spam emails to detect botnet groups infected with the same malware [36-38]. Additionally, Cova, Chen, Chang, et al. identified and analyzed "drive-by downloads" as a primary method of web-based malware distribution [39-42].

2.5 TTPs-Based Analysis

The MITRE ATT&CK® framework was developed to model the tactics and techniques of cyber attackers. Since the release of version 1 in 2018, it has undergone continuous updates, with version 17.1 available as of April 2025 [43].

The MITRE ATT&CK® Matrices are divided into three categories: Enterprise, Mobile, and ICS. As shown in Table 2, the Enterprise category comprises 14 tactics and 245 attack techniques.

Table 2. Enterprise category's tactics and techniques

ID	Tactics	Techniques
TA0043	Reconnaissance	10
TA0042	Resource development	8
TA0001	Initial access	11
TA0002	Execution	16
TA0003	Persistence	23
TA0004	Privilege escalation	14
TA0005	Defense evasion	45
TA0006	Credential access	17
TA0007	Discovery	33
TA0008	Lateral movement	9
TA0009	Collection	17
TA0011	Command and control	18
TA0010	Exfiltration	9
TA0040	Impact	15

Attackers can relatively easily modify elements of the attack infrastructure, such as hashes, IP addresses, and domains. However, modifying TTPs is a costly and complex process. For this reason, in 2022, a cyberattack group classification technique using the MITRE ATT&CK® model was studied. This study utilizes the existing MITRE ATT&CK model to extract TTPs at the cyber-attack incident level and classifies attack groups by analyzing the learned TTP patterns [44].

This study is significant because it utilizes TTPs, which are more difficult to falsify than IoCs and applies AI technology to learn from them. However, while attack objectives can be identified at each attack stage, limitations remain in fully understanding the overall intent behind the attack.

2.6 Harm-Based Analysis

In 2017, researchers analyzed the impact of cyberattacks from both economic and political perspectives [45].

Figure 2 shows a model for analyzing attack intent using a damage-based analysis method. When an attack occurs, the resulting damage is assessed to determine whether it affects the attacker's reputation and benefits (①, ②) or the victim's reputation and losses (③, ④). The attack is then categorized into one of three types: this represent the form of the attacker/group (ⓐ Individual, ⓑ Organization, ⓒ Country). Subsequently, the damage results are analyzed to infer the underlying motivation for the attack. (1) Belief, (2) Desire, (3) Politics, or (4) Economy. If two attack intentions are identified, they are compared to determine the final attack intent and classify the attack type accordingly.

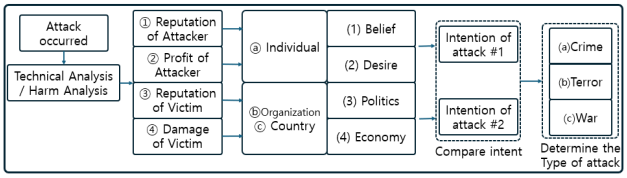

Figure 2. Model for analyzing the intent of cyberattacks

In the above study, the assessment of attack damage did not consider the scale of the attack or type of target, relying instead on a simple comparison. This limitation reduces the accuracy of identifying attack intent, which can vary significantly depending on the extent of the damage.

For example, if the impact information leakage can vary significantly depending on whether the target is an

individual, organization or country. Therefore, accurately assessing the damage requires first determining the target type and the scale of the impact.

Similar research conducted in 2021 utilized social issues to predict cyberattacks and proposed a framework for proactive response [46]. Analysis of APT attacks reveal that most attackers commonly use phishing and drive-by compromise techniques to gain initial access to their targets.

These two techniques are often targeted at employees of the victim organization or third-party individuals with access privileges, often exploiting current social issues for access.

A notable example is the COVID-19 pandemic, during which attackers sent emails containing information about virus spread and prevention, targeting individuals sensitive to these topics to steal personal and financial information.

Another example is the Sony Pictures Entertainment hacking incident in November 2014. The release of a comedy film depicting the assassination of Kim Jong-un likely provoked North Korea's leadership, making it reasonable to infer that North Korea was responsible for the attack.

2.7 CTI (Cyber Threat Intelligence)-based Analysis

Figure 3 shows the J. Bianco Pain Pyramid, which is composed of various indicators commonly used in cyberattacks [18].

As one moves up the pyramid, the cost to the attacker increases. IoCs, such as hash values, can be easily changed. In contrast, TTPs at the top of the pyramid are much harder to change, as they represent the attacker's capabilities and tactics, developed through significant investments of time and resources to achieve their objectives.

To implement proactive defense against cyberattacks, it is crucial to quickly analyze the high-level indicators at the top of the pyramid to identify the attacker's intent.

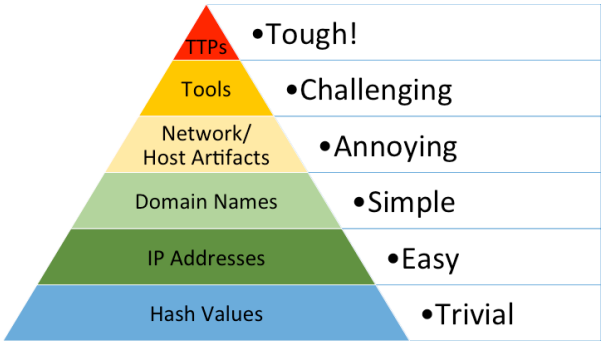

Figure 3. Pyramid of Pain

CTI refers to the comprehensive process of collecting and analyzing information across all levels of the pyramid of pain, with the goal of obtaining high-level intelligence from the top of the pyramid [12].

As shown in Figure 4, CTI outlines four subcategories of CTI, defined according to the level and persistence of knowledge-based information [47].

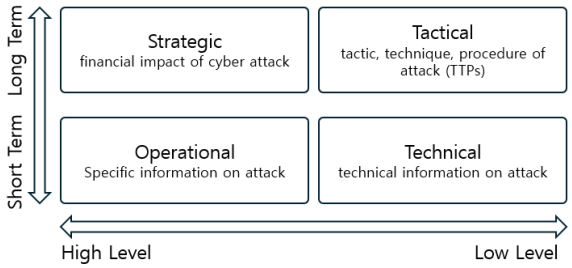

Figure 4. CTI classification

Among the four CTI categories, strategic CTI involves analyzing information obtained from various sources over an extended period through correlation analysis to derive results. Particularly, understanding the attacker's intent and classifying attack groups are considered top-level CTI tasks, which are analyzed in conjunction with the three lower CTI levels: tactical, operational, and technical, as well as shared CTI data.

Section 3 presents a model for the rapid acquisition of strategic CTI.

3 Proposed Scheme

3.1 Core Elements for Analyzing Cyber Attack Intent

To understand attack intent, it is important to identify who (attacker) attacked whom (target) and how the attack was carried to achieve the attacker's objectives. In this study, we first derive the key elements related to attack intent and characterize their properties to facilitate effective analysis.

The following describes each element related to attack intent:

(1) Attack Group: Attackers can be classified into individual hackers, hacker groups, cyberterrorist organizations, state-sponsored terrorist organizations, and entities involved in cyber warfare. Many national and private cybersecurity organizations identify and label these groups, such as APT28, Lazarus, and APT38, for monitoring and threat intelligence purposes. State-sponsored groups often have unique mission characteristics and profiling them can help identify emerging cyberattack actors. For example, North Korean attack groups primarily target South Korea rather than China or Russia in their cyberattacks. Additionally, when a state-sponsored attack is aimed at acquiring cryptocurrency, it is generally attributed to North Korea.

(2) Targets: Attackers may select either specific or broad targets depending on their intent. These targets can include government agencies, military organizations, companies, media outlets, and individuals. The attributes of the selected target often provide insights into the attacker's area of interest. For example, an attacker of a military-related website may suggest an attempt to gather military intelligence or analyze defense trends. Similarly, targeting an election agency could indicate an attempt to exert political influence in favor of the attacker's benefit.

(3) Social Context: Understanding whether an attack is linked to specific political, social, or economic issues

is essential at interpreting intent. Cyberattacks conducted at the national level are likely associated with significant events. For example, hacking incidents occurring just before an election may be interpreted as attempts to influence the results. A 2017 report states that according to a report released by U.S. intelligence agencies, Russian President Vladimir Putin personally ordered hacking to help Donald Trump win the presidential election and to undermine Democratic candidate Hillary Clinton [48].

(4) Attack type: Cyberattacks can be classified as cybercrime, cyberterrorism, or cyberwarfare. Identifying the type of attack helps determine the likely perpetrator by aligning the nature of the incident with typical attacker profiles.

Cybercrime is typically conducted by individuals, criminal organizations, or hacker groups, targeting individuals, businesses, and financial institutions. The primary goals include financial gain, fraud, or the theft of personal and sensitive information. Cyberterrorism is conducted by terrorists, hacktivists, or ideologically motivated actors. Its aims include instilling fear, creating social disruption, and conveying political messages by targeting appropriate targets. Cyber warfare is conducted by nation-states or state-affiliated organizations to achieve political gains or to support physical warfare by targeting key institutions and facilities of enemy nations.

(5) TTPs: Attack methods are primarily described using TTPs based on MITRE ATT&CK. Specific behaviors such as malicious code and repeated, patterned tactics, can help identify the attacker and their operational methods. TTPs vary depending on the attacker's intent; for example, attacks aimed at information gathering, destruction, manipulation, or disruption each exhibit distinct characteristics that can be used to infer attacker's intent.

(6) Propaganda: Attack groups may use technical methods such as website defacement, deepfake videos, and encrypted messaging platforms like Telegram to convey messages and conduct propaganda activities. These campaigns can allow insights into the attacker's intent and identity. Cyber psychological warfare and information warfare are clear examples as they aim to spread propaganda and cause confusion within the target country.

(7) Impact: The form and scale of damage caused by a cyberattack can identify important clues about the perpetrator and the intent behind the attack. Notably, the scale of a cyberattack is a multifaceted indicator that accounts for physical, economic, and social impacts, the technical complexity of the attack, and the strategic importance of the target, it does not simply refer to the extent of "significant damage." Additionally, the broader implications for national security and the global economic and social environment must also be considered.

The elements used to analyze the cyberattack intent, as described above, are summarized in Table 3.

Among these, the attack group and target are especially critical for identifying the attacker's intent. In particular, the attack group is a priority element, as it can be inferred from other elements. Additionally, understanding the extent of damage, particularly the scope of the attack, further informs the determination of the attack's intent. Therefore, to effectively identify intent and enable a proactive response, it is crucial to identify the attack group, attack target, and scope of damage as early as possible.

Furthermore, the elements used to analyze attack intent are closely interrelated and must be assembled like pieces of a puzzle; only by combining them can the attack intent be accurately inferred. Figure 5 illustrates the relationship between attack intent and its core elements, showing how each core element complements the others in the inference process.

Table 3. Core elements for analyzing cyber-attack intent

Elements	Meaning	Intent inference method
Attack Group	Hackers, terrorists, state-sponsored organizations, etc.	Attack Type/Damage/Intent Inference
Target (Victim)	Individuals, organizations, unspecified groups, countries, etc.	Predict attack groups, damage, and intent
Attack Type	Cybercrime/Terrorism/War	Inferring attack groups/intentions
TTPs	TTPs, malware functionality, presence of repetition/patterns	Attack Group/Damage Prediction
Harm	Nature of leaked/tampered information, form of damage, scope of damage	Inferring attack group/intent after damage analysis
Propaganda	Attacker's intended message, propaganda/promotion	Message analysis, prediction of attack group/target/intent
Social Context	Political/social/economic issues related to the timing of the attack	Inferring attack group/intent based on issues

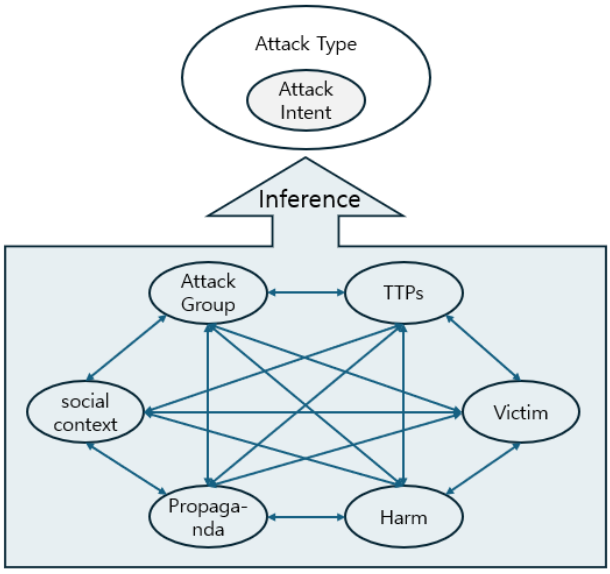

Figure 5. Core elements and attack intent

3.2 Elements Related to Attack Intent

3.2.1 Attack Group Classification Method

There are five primary methods for classifying attack groups. ① Attacker Characteristics: This method involves identifying attacker characteristics using techniques similar to criminal profiling in conventional investigations. However, unlike physical crimes, cyberattacks occur covertly within the unique and anonymous environment of the Internet, making it significantly more challenging to identify an attacker's characteristics. ② IoC-Based Analysis: This refers to various resources used by attackers in their attacks. These include malicious files (such as hash values, file names, and file paths), network information (such as malicious IP addresses, domains, and URLs), system registry changes, and log file analysis results. Defenders can obtain intrusion detection information (IoC) through their own security infrastructure (FW, IPS, anti-virus, etc.) and respond accordingly or share it with other organizations. Conversely, defenders can obtain IoCs from threat information-sharing organizations or partner companies and utilize them to respond promptly to emerging threats. If an attacker reuses the same resources in multiple attacks, defenders can often link the activity to a known group based on previous incidents. While attackers may employ deceptive tactics to obscure their identity, this approach enables immediate response, thereby making this approach widely adopted.

③ Attack Techniques: By analyzing the malware, tools, and techniques used by attackers at each attack stage, defenders can classify threat attackers based on similarities with past incidents, similar to approach ②. While some technical information may help in identifying specific attackers or groups, the widespread use of shared attack tools and open-source attack code has reduced the reliability of these correlations.

④ TTPs-Based Analysis: While organizations with specialized in-house teams can conduct TTP analysis independently, most rely on cyber threat intelligence reports from government agencies or private cybersecurity companies for preventive measures. Because TTPs often exhibit distinct characteristics and methods of specific attack groups, they are useful for classifying attack groups and providing long-term intelligence.

⑤ Social Context/Harm-Based Analysis: This method involves analyzing the political, social, and economic context surrounding an attack, along with the resulting damage, to help identify the responsible group. It is directly linked to the attacker's tactics and facilitates an understanding of their attack intent. However, obtaining a clear and accurate understanding of the damage is essential, as this information is critical for identifying attacks to specific groups.

In summary, analysis methods that focus on identifying the attacker or group, such as ①, ④, and ⑤, yield more valuable, long-term insights that enable proactive defense responses. In contrast, ② and ③ emphasize technical characteristics suited for immediate response during active incidents but are vulnerable to attacker deception. Based on the comparative analysis of attack group classification methods, this study recognizes the need for further research to improve method ⑤, which is partially valuable for identifying an attacker's intent and behavioral patterns in the early stages of an attack. Additionally, there is a need to explore ways to integrate this method with other analytical methods to improve overall effectiveness. Figure 6 provides a conceptual overview and comprehensive explanation of the attack group classification methods.

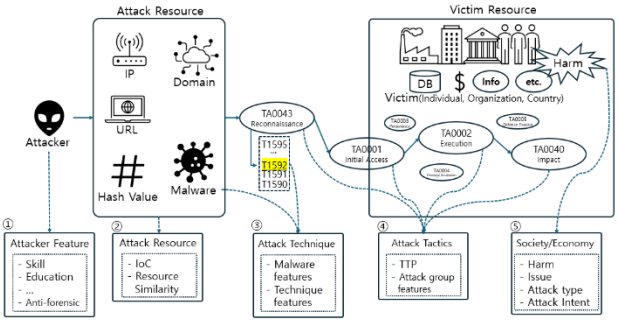

Figure 6. Attack-group-classification method

3.2.2 Analysis of Attack Targets

To infer attack intent, it is essential first to identify the attack targets and the extent of the damage, as these factors provide clearer insights compared to others. Methods for distinguishing attack targets include: ① Technical analysis: logs, malware, forensic analysis, ② Document/Behavior-based: phishing emails, time zones, message analysis, ③ Organization Structure-based: internal user roles, partner analysis, ④ CTI/External Information Utilization: TTPs, IoC, dark web information, and methods for sharing information between relevant agencies. Notably, information sharing between relevant agencies plays a crucial role in accurately identifying both the target and scope of an attack.

3.2.3 Analysis of Attack Harm

Methods for assessing attack damage include: ① Range: Check the number of targets and the extent of regional spread (e.g., 100 companies affected, spread to

20 countries), ② Strength: System paralysis, complete data deletion, etc. (e.g., ransomware causing a hospital to be paralyzed for three weeks), ③ Duration: whether the attack was a one-time event or involved long-term infiltration (e.g., months of covert infiltration (SolarWinds)), ④ Target Importance: Whether government agencies or critical infrastructure are targeted (e.g., attacks on the Department of Defense or power plants), ⑤ Influence: Chain reactions, social disruption, loss of trust (e.g., emergency services disrupted due to communication network outage), ⑥ Technical Complexity: Whether zero-day exploits or ICS attacks are used (e.g., Stuxnet, Industroyer).

3.3 Classification and characteristics of attack intent

To rapidly identify attack intent, it is necessary to examine the characteristics of various attack intents. Attack intent can be divided into domains such as belief, desire, politics, and economy, as proposed by Park Sang-min (2017). Alternatively, more specific intents, such as self-aggrandizement or the pursuit of corporate profit, can also be considered. In this study, we propose the following classification of cyberattack intent based on these broad categories:

1. Espionage: Activities aimed at stealing confidential, technological, or strategic information from foreign governments or companies. These are primarily conducted by national intelligence agencies or APT groups.

2. Disruption/Destruction: These attacks aim to cause chaos within institutions or societies by paralyzing systems, interrupting essential services, or destroying data. Typically executed by hostile nations or cyber military organizations.

3. Financial Gain: Attacks motivated by monetary profit, including ransomware attacks, theft and sale of sensitive data, and credit card fraud. These are commonly conducted by cybercrime organizations and independent hackers. In some exceptional cases, such as North Korea, sponsored cybercrime is also observed.

4. Political or Social Messaging (Hacktivism): These attacks are aimed to promote political protests, support social movements, or spread ideological messages. They are primarily carried out by hacktivist groups, such as Anonymous.

5. Military Advantage: These cyberattacks are conducted alongside physical warfare, including information and psychological warfare conducted before and after armed conflict. Their primary target is military communication networks and ICS. Conducted by state-sponsored cyber units.

6. Influence operations: These operations aim to spread social disruptions by spreading false information, manipulating public opinion, and interfering in elections. They are typically conducted by psychological warfare units and intelligence agencies.

7. Retaliation/Revenge: Cyberattacks driven by a desire to punish or seek revenge against a nation or organization, often taking the form of retaliatory actions between hostile organizations or nations.

8. Sabotage: Cyberattacks intended to gain a competitive benefit by destroying a competitor's systems, operations, or reputation. These attacks are often carried out by industrial spies or hackers hired by competing companies.

9. Technical experimentation or reputation/challenge: These attacks are conducted by individual hackers or groups seeking to demonstrate their technical capabilities, or build a reputation within the hacking community. This category includes actors such as script kiddies or white-hat hackers.

In this study, we aim to establish the relationship between these nine types of attack intent and their defining characteristics, to implement a structured attack-intention analysis model.

3.4 Proposed Attack Intent Analysis Model

3.4.1 Core Element Setting Values

The possible values of the core elements used in the attack intent analysis are listed in Table 4. The target is represented by a combination of one value from the unspecific/specific category and one from individual, Organization, or Country. For example, UI represents an unspecified individual.

Harm refers to the detailed elements discussed in Section 3.2.3 and is categorized as high, medium, or low. Higher values indicate a greater likelihood that the cyberattack is state-sponsored or motivated by significant gain.

Attack Group is inferred using the classification method discussed in Section 3.2.1 and can be classified as one of the following values: Individual, Organization, or Country.

The social Context is first classified into Wartime or Peacetime, and each category is further linked to issues with military, political, economic, and social contexts. For example, WM refers to cyberattacks related to military issues during wartime.

Propaganda shares the same value as Social Context.

The attack type takes one of three values: war, error, or crime.

Table 4 presents the core elements and possible settings for each.

Table 4. Core elements setting values

Target		Harm Range ~ Complexity	Attack group	Social context		Propaganda	Attack type
Unspecific	Individual	H (High)	Individual	Wartime	Military	Military	War
	Organization	M (Medium)	Organization		Politics	Politics	Terror
Specific	Country	L (Low)	Country	Peacetime	Economy	Economy	Crime
					Social	Social	

Each core element may be assigned a value based on the analysis results, or it may remain unassigned. These elements are linked together like pieces of a puzzle, aligned according to their matching values.

Table 5 presents example values for Attack Intent, Target, and Harm in the model proposed in this study. These values are adapted from Casey's 2016 study, "Understanding Cyber threat Motivations to Improve Defense," which presented some of the attack groups and motivations.

As shown in Table 5, when the attack group is state sponsored, the target is typically a specific government agency or military facility, resulting in SO and SC, with a high Harm value.

Table 5. Setting core elements by attack group

Attack group	Attack intent	Target	Harm
Civil activist	Hacktivism	UI	L
Radical activist	Hacktivism	UI	L
Anarchist	Hacktivism	UI	L
Script kiddie	Reputation/Challenge	UI, SO	L
Thief	Financial Gain	UI, SI, SO	L
Corrupt government official	Financial Gain	SI, SO	L
Data miner	Espionage	UI, SI, SO	M, L
Disgruntled employee	Financial Gain	SO	L
Competitor	Sabotage	SO	L
Internal spy	Financial Gain, Espionage	SO	M, L
Legal adversary	Influence Operations	SI, SO	L
Sensationalist	Hacktivism	UI	L
Mobster	Financial Gain	SI, SO	M, L
Terrorist	Disruption/Destruction, Retaliation/ Revenge, Hacktivism	UI, SI, SO	H, M
Vendor	Financial Gain	SO	M, L
Government Cyberwarrior	Disruption/Destruction, Retaliation/ Revenge, Military Advantage, Espionage	SI, SO, SC	H
Government spy	Espionage	SI, SO, SC	H

Conversely, when the attack group is an individual, there is usually a high "financial gain," the target type is mainly "individual," and the overall harm result is "low."

Given the strong correlation between the attack group, target, and Harm elements, this framework aims to analyze each core element and infer the Attack Intent by integrating and complementing these components.

3.4.2 Attack Intent Analysis Framework

Attack intent analysis involves inferring the nature of an attack by combining core elements in a complementary manner, like assembling pieces of a puzzle. As shown in Figure 7, the analysis begins by detecting the initial attack indicators, followed by identifying the attacker group and target, along with analyzing the damage. While some aspects may yield immediate results, covert and persistent attacks often involve limited information, necessitating repeated and iterative analyses.

The attacker group was inferred based on the detailed elements discussed in Section 3.2.1. Additionally, the attack target and resulting damage were also deduced. The inferred results matched the values defined in Section 3.4.1.

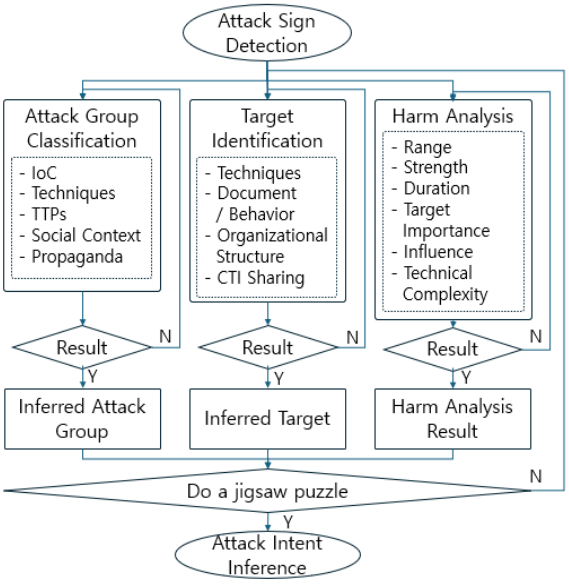

Figure 7. Attack-intent analysis framework

Based on the analysis of the attack group, target, and hand analysis results, the attack type and intent are inferred by piecing together each element, much like solving a puzzle. For example, if the attacker is identified as an individual, the target is a country, and the tactics are highly complicated, the inference is commonly incorrect. Therefore, the analysis of each core element is repeated from the beginning until a consistent set of highly correlated values is obtained, at which point the inference can be considered accurate.

The model shown above offers the advantage of inferring each key element using only the information available at the initial stage of an attack. Although the initial values of some elements may lack precision, they can be crosschecked against other key elements to improve accuracy. Furthermore, as time progresses and additional information is gathered, the model's inferences become increasingly reliable.

4 Conclusion

In this study, we selected key elements related to cyberattack intent and successfully inferred intent by leveraging the complementary relationships among these elements. By presenting an analysis model based on these essential components, we demonstrated the possibility of inferring attack intent during the early and middle stages of a cyberattack.

Further research is needed to develop implementation methods for real environments, such as calculation formulas to quantify the detailed elements of Harm-Based Analysis. Additionally, more research is required to identify "attack intent" using the STIX format [5], a standardized framework for cyber threat intelligence.

Classifying cyberattack groups requires continuous development to evolving attack techniques. As the core elements for analyzing cyberattack intent become more specified and are implemented as training data for AI models, significant advancements in the field can be expected.

Additionally, we confirmed that 'attack intent' linked to TTPs, which are challenging for attackers to replicate consistently.

The proposed framework can enhance the accuracy of attack group classification by incorporating TTPs to capture attribute values related to attack intent and damage assessment.

Further research is needed to utilize the STIX format, a future standard for cyber threat intelligence, to support the identification of "attack intent." The classification of cyberattack groups requires ongoing development to keep pace with evolving attack techniques. Once the proposed framework is implemented, continuous learning of attack group behavior is expected to enable more effective monitoring of changes in their characteristics.

Acknowledgments

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) (Project No. RS-2023-00228996, 20%; RS-2024-00438551, 20%; IITP-2025-RS-2021-II211816, 10%), the National Research Foundation of Korea (NRF) grant funded by the Korean Government (Project No. RS-2023-00208460, 30%), and the Ministry of Culture, Sports, and Tourism (MCST) and Korea Creative Content Agency (KOCCA) grant (Project No. RS-2025-02221620, 20%).

References

[1] K. W. Park, *When 'Cloud' and 'Zero Trust' meet*, December, 2024. https://www.boannews.com/media/view.asp?idx=135400

[2] K. G. Kim, F. A. Alfouzan, H. K. Kim, Cyber-Attack Scoring Model Based on the Offensive Cybersecurity Framework, *MDPI Applied Sciences*, Vol. 11, No. 16, pp. 1-21, August, 2021. https://doi.org/10.3390/app11167738

[3] M. Martineau, E. Spiridon, M. Aiken, A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature, *MDPI Forensic Sciences*, Vol. 3, No. 3, pp. 452-477, September, 2023. https://doi.org/10.3390/forensicsci3030032

[4] T. Casey, M. Rosenquist, P. Koeberl, *Understanding Cyberthreat Motivations to Improve Defense*, Intel Security and Privacy Office White Paper, February, 2016.

[5] B. Jordan, R. Piazza, T. Darley, *STIX Version 2.1*, OASIS Standard, January, 2021.

[6] C.-I. Fan, H.-W. Hsiao, C.-H. Chou, Y.-F. Tseng, Malware Detection Systems Based on API Log Data Mining, *2015 IEEE 39th Annual Computer Software and Applications Conference*, Taichung, Taiwan, 2015, pp. 255-260. https://doi.org/10.1109/COMPSAC.2015.241

[7] D. Uppal, R. Sinha, V. Mehra, V. Jain, Exploring Behavioral Aspects of API Calls for Malware Identification and Categorization, *2014 International Conference on Computational Intelligence and Communication Networks*, Bhopal, India, 2014, pp. 824-828. https://doi.org/10.1109/CICN.2014.176

[8] C. H. Choi, H. S. Lee, I. H. Jung, C. G. Yoo, H. S. Yoon, Statistical Analysis of EML Header for Cyber Attacker Tracing, *Proceedings of Korea Institute of Military Science and Technology annual conference*, Jeju, Republic of Korea, 2017, pp. 1141-1142.

[9] C. H. Choi, H. S. Lee, I. H. Jung, J. H. Park, H. S. Yoon, E-mail Clustering for Cyber Attack Attribution, *Proceedings of Korea Institute of Military Science and Technology annual conference*, Jeju, Republic of Korea, 2018, pp. 1289-1290.

[10] N. Villeneuve, J. Bennett, *Detecting APT Activity with Network Traffic Analysis*, Trend Micro Incorporated Research Paper, December, 2012. https://documents.trendmicro.com/assets/wp/wp-detecting-apt-activity-with-network-traffic-analysis.pdf

[11] G. Zhao, K. Xu, L. Xu, B. Wu, Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis, *IEEE Access*, Vol. 3, pp. 1132-1142, July, 2015. https://doi.org/10.1109/ACCESS.2015.2458581

[12] Y. Kazato, Y. Nakagawa, Y. Nakatani, Improving Maliciousness Estimation of Indicator of Compromise Using Graph Convolutional Networks, *2020 IEEE 17th*

Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2020, pp. 1-7. https://doi.org/10.1109/CCNC46108.2020.9045113

[13] S. Kapetanakis, A. Filippoupolitis, G. Loukas, T. S. Murayziq, Profiling cyber attackers using case-based reasoning, *19th UK Workshop on Case-Based Reasoning (UKCBR 2014)*, Cambridge, UK, 2014, pp. 1-10. http://gala.gre.ac.uk/id/eprint/14950

[14] J. L. Kolodner, An introduction to case-based reasoning, *Artificial intelligence review*, Vol. 6, No. 1, pp. 3-34, March, 1992. https://doi.org/10.1007/BF00155578

[15] B. E. Binde, R. McRee, T. J. O'Connor, *Assessing Outbound Traffic to Uncover Advanced Persistent Threat*, SANS Technology Institute, May, 2011. https://doi.org/10.13140/RG.2.2.16401.07520

[16] S. Rekhis, N. Boudriga, A System for Formal Digital Forensic Investigation Aware of Anti-Forensic Attacks, *IEEE Transactions on Information Forensics And Security*, Vol. 7, No. 2, pp. 635-650, April, 2012. https://doi.org/10.1109/TIFS.2011.2176117

[17] A. Berady, M. Jaume, V. V. Tong, G. Guette, From TTP to IoC: Advanced Persistent Graphs for Threat Hunting, *IEEE Transactions on Network And Service Management*, Vol. 18, No. 2, pp. 1321-1333, June, 2021. https://doi.org/10.1109/TNSM.2021.3056999

[18] D. J. Bianco, *The Pyramid of Pain*, https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html, April, 2014.

[19] S. Saeed, S. A. Suayyid, M. S. AI-Ghamdi, H. AI-Muhaisen, A. M. Almuhaideb, A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience, *MDPI Sensors*, Vol. 23, No. 16, pp. 1-27, August, 2023. https://doi.org/10.3390/s23167273

[20] K. H. Son, B. I. Kim, T. J. Lee, Cyber-attack group analysis method based on association of cyber-attack information, *KSII Transactions on Internet and Information Systems*, Vol. 14, No. 1, pp. 260-280, January, 2020. https://doi.org/10.3837/tiis.2020.01.015

[21] G. Husari, E. Al-Shaer, B. Chu, R. F. Rahman, Learning APT chains from cyber threat intelligence, *HotSoS'19: Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security*, Nashville, Tennessee, USA, 2019, pp. 1-2. https://doi.org/10.1145/3314058.3317728

[22] J. Surma, Cyber Threat Intelligence Systems: problems and challenges, *Collegium of Economic Analysis Annals*, No. 54, pp. 267-274, 2019. http://rocznikikae.sgh.waw.pl/p/roczniki_kae_z54_20.pdf

[23] M. Conti, T. Dargahi, A. Dehghantanha, Cyber Threat Intelligence: Challenges and Opportunities, in: A. Dehghantanha, M. Conti, T. Dargahi (Eds.), *Cyber Threat Intelligence. Advances in Information Security*, Springer, 2018. https://doi.org/10.1007/978-3-319-73951-9_1

[24] P. A. Watters, S. Mccombie, R. Layton, J. Pieprzyk, Characterising and predicting cyber Attacks using the Cyber Attacker Model Profile (CAMP), *Journal of Money Laundering Control*, Vol. 15, No. 4, pp. 430-441, October, 2012. https://doi.org/10.1108/13685201211266015

[25] H. S. Cho, S. G. Lee, B. I. Kim, Y. S. Shin, T. J. Lee, The Study of Prediction of Same Attack Group by Comparing Similarity of Domain, *2015 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, Republic of Korea, 2015, pp. 1220-1222. https://doi.org/10.1109/ICTC.2015.7354779

[26] L. Schwartz, *Amateur open source researchers went viral unpacking the war in Ukraine*, Rest of World, March, 2022. https://restofworld.org/2022/osint-viral-ukraine/

[27] KISA (Korea Internet & Security Agency). https://www.kisa.or.kr

[28] W. J. Kim, C. W. Park, S. J. Lee, J. S. Lim, Methods for Classification and Attack Prediction of Attack Groups based on Framework of Cyber Defense Operations, *Journal of KIISE (Korean Institute of Information Scientists and Engineers)*, Vol. 20, No. 6, pp. 317-328, June, 2014. https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART001881715

[29] A. Mohaisen, O. Alrawi, Unveiling zeus: automated classification of malware samples, *WWW'13 Companion: Proceedings of the 22nd International Conference on World Wide Web*, Rio de Janeiro, Brazil, 2013, pp. 829-832. https://doi.org/10.1145/2487788.2488056

[30] T. J. Lee, J. Kwak, Effective and Reliable Malware Group Classification for a Massive Malware Environment, *International Journal of Distributed Sensor Networks*, Vol. 12, No. 5, pp. 1-6, May, 2016. https://doi.org/10.1155/2016/4601847

[31] F. Haddadi, A. Nur Zincir-Heywood, Botnet behaviour analysis: How would a data analytics-based system with minimum a priori information perform, *International Journal of Network Management*, Vol. 27, No. 4, pp. 1-20, July/August, 2017. https://doi.org/10.1002/nem.1977

[32] G. A. N. Mohamed, N. B. Ithnin, SBRT: API Signature Behaviour Based Representation Technique for Improving Metamorphic Malware Detection, *International Conference of Reliable Information and Communication Technology 2017: Recent Trends in Information and Communication Technology*, Johor Bahru, Malaysia, 2017, pp. 767-777. https://doi.org/10.1007/978-3-319-59427-9_79

[33] W. Han, J. Xue, Y. Wang, L. Huang, Z. Kong, L. Mao, MalDAE: Detecting and explaining malware based on correlation and fusion of static and dynamic characteristics, *Computers & Security*, Vol. 83, pp. 208-233, June, 2019. https://doi.org/10.1016/j.cose.2019.02.007

[34] G. Gu, J. Zhang, W. Lee, Botsniffer: Detecting botnet command and control channels in network traffic, *Proceedings of the Network and Distributed System Security Symposium*, San Diego, California, USA, 2008, pp. 1-18.

[35] M. Feily, A. Shahrestani, S. Ramadass, A survey of botnet and botnet detection, *2009 Third International Conference on Emerging Security Information, Systems and Technologies*, Glyfada, Athens, Greece, 2009, pp. 268-273. https://doi.org/10.1109/SECURWARE.2009.48

[36] H. S. Choi, H. W. Lee, H. J. Lee, H. G. Kim, Botnet detection by monitoring group activities in DNS traffic, *7th IEEE International Conference on Computer and Information Technology (CIT 2007)*, Aizu-Wakamatsu, Japan, 2007, pp. 715-720. https://doi.org/10.1109/CIT.2007.90

[37] P. Sroufe, S. Phithakkitnukoon, R. Dantu, J. Cangussu, Email shape analysis for spam botnet detection, *2009 6th IEEE Consumer Communications and Networking Conference*, Las Vegas, NV, USA, 2009, pp. 1-2. https://doi.org/10.1109/CCNC.2009.4784781

[38] T. J. Lee, H. S. Cho, H. R. Park, J. Kwak, Detection of malware propagation in sensor Node and botnet group clustering based on e-mail spam analysis, *International Journal of Distributed Sensor Networks*, Vol. 11, No. 9, Article No. 530250, September, 2015. https://doi.org/10.1155/2015/530250

[39] M. Cova, C. Kruegel, G. Vigna, Detection and analysis of drive-by-download attacks and malicious JavaScript code, *WWW'10: Proceedings of the 19th international conference on World wide web*, Raleigh, North Carolina, USA, 2010, pp. 281-290. https://doi.org/10.1145/1772690.1772720

[40] K. Z. Chen, G. Gu, J. Zhuge, J. Nazario, X. Han, WebPatrol: Automated collection and replay of web-based malware scenarios, *ASIACCS'11: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, Hong Kong, China, 2011, pp. 186-195. https://doi.org/10.1145/1966913.1966938

[41] G. Wang, J. W. Stokes, C. Herley, D. Felstead, Detecting malicious landing pages in Malware Distribution Networks, *2013 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Budapest, Hungary, 2013, pp. 1-11. https://doi.org/10.1109/DSN.2013.6575316

[42] J. Chang, K. K. Venkatasubramanian, A. G. West, I. S. Lee, Analyzing and defending against web-based malware, *ACM Computing Surveys (CSUR)*, Vol. 45, No. 4, pp. 1-35, August, 2013. https://doi.org/10.1145/2501654.2501663

[43] MITRE ATT&CK®. https://attack.mitre.org/

[44] C. H. Choi, C. H. Shin, S. U. Shin, Cyber attack group classification based on MITRE ATT&CK model, *Journal of Internet Computing and Services*, Vol. 23, No. 6, pp. 1-13, December, 2022. https://doi.org/10.7472/jksii.2022.23.6.1

[45] S. M. Park, J. I. Lim, Study On Identifying Cyber Attack Classification Through The Analysis of Cyber Attack Intention, *Journal of The Korea Institute of Information Security and Cryptology*, Vol. 27, No. 1, pp. 103-113, February, 2017. https://doi.org/10.13089/JKIISC.2017.27.1.103

[46] K. Jang, K. H. Nam, *Study on framework to respond to social issue-based APT attack*, Master's Thesis, Konkuk Univ, Seoul, Republic of Korea, 2021.

[47] S. H. Gong, C. H. Lee, *Study on Cyber Threat Intelligence Analysis Method*, Master's Thesis, Seoul National University of Science and Technology, Seoul, Republic of Korea, 2018. https://snut.dcollection.net/public_resource/pdf/200000011087_20251028210536.pdf

[48] J. Marks, *Intel Report: Russian Government Aimed to Help Trump with Hacks*, Nextgov, January, 2017 https://www.nextgov.com/cybersecurity/2017/01/intel-report-russian-government-aimed-help-trump-hacks/134412/?oref=ge-homepage-noscript-river&__hstc=121679188.39bdf48f259dd57ad58973e620b4621f.1752624000280.1752624000281.1752624000282.1&__hssc=121679188.1.1752624000283&__hsfp=2324370431

Biographies

Won-Chul Kim received the B.S. and M.S. degree in computer science from Kyonggi University, South Korea, in 1998. He is currently working toward the Ph.D. degree in the Department of Computer and Information Security, University of Sejong, South Korea. His research interests include CTI (Cyber Threat Intelligence), Cyber Threat Analysis and machine learning.

Ki-Woong Park received the B.S. degree in computer science from Yonsei University, South Korea, in 2005, the M.S. degree in electrical engineering from the Korea Advanced Institute of Science and Technology (KAIST) in 2007, and the Ph.D. degree in electrical engineering from KAIST in 2012. He received a 2009–2010 Microsoft Graduate Research Fellowship. He worked for National Security Research Institute as a senior researcher. He has been a professor in the department of computer and information security at Sejong University. His research interests include security issues for cloud and mobile computing systems as well as the actual system implementation and subsequent evaluation in a real computing system.