Multi-lateral Cybersecurity Cooperation for Military Forces in the Digital Transformation Era

Hyun Kyoo Park[1(✉)], Wootack Lee[2], Zinkyung Ha[2], and Namhee Park[2]

[1] Petabi Corp., Seoul, Republic of Korea
hyunkyoopark@petabi.com
[2] Ministry of National Defense, Seoul, Republic of Korea
{tackl23, namhee}@mnd.go.kr, hazin@korea.kr

Abstract. Most organizations including armed forces continuously invested on security solutions such as security information and event management, next generation firewall and intrusion prevention systems to improve their cybersecurity capabilities. Even though most legacy monitoring tools can detect cyber threats, the warfighting and business information systems remain vulnerable to modified or unknown threats since those are evolved continuously in a covert manner.

At the Seoul Defense Dialogue (SDD) Cyber Working Group (CWG) 2017, we discussed several agendas related to the civil-military cooperative effort those can improve cybersecurity capabilities with high-risk/high-payoff research in the digital transformation era. The essence is granting the cyber workforces access to appropriate data from various sources needed to assure mission completeness based on the current technological achievement.

In various situations, military operations must be synchronized with kinetic forces by appropriate cyber information. For this purpose, the cyber situational awareness (SA) provides the risk mitigation and the resilience capability for the mission completeness. To improve SA capabilities, it is important to share data with big data and machine learning technology among civil-military and international cooperation especially for defensive cyber operations.

In this paper we described the lessons learned from SDD CWG to improve the state of the cybersecurity and the cognitive technology for the improved cyber situational awareness.

Keywords: Cybersecurity · Seoul Defense Dialogue · Cognitive technology
Digital transformation · Cyber situational awareness

1 Introduction

By the rapid advancement in computer and communication technologies, today's information and communication environment has become more prevalent and attacks have moved from static to dynamic. It is generally accepted that cybersecurity could be started from removing potential vulnerabilities that are susceptible to exploitation and then established security systems. However, the complete protection of information

O. Gervasi et al. (Eds.): ICCSA 2018, LNCS 10964, pp. 193–204, 2018.
https://doi.org/10.1007/978-3-319-95174-4_16

systems at the boundary of internal network is hardly achievable. Attackers utilize multiple vectors to accomplish their objectives, hence it requires a change in the way of understanding and the strategy about cybersecurity.

In the military, as tightening the correlation between the cyber and kinetic operations, military forces are very dependent on cyber capabilities for their mission completeness. The cyberspace is one of the operational space and the cybersecurity is considered as an essential factor of military activities even in the peace time. The connectivity expansion of weapon systems and business systems incurs hardships of preventing adversary attacks and internal threats. Furthermore activists, nation states and cyber terrorists are increasing with a little modification of easily available exploitation toolkits as a persuading method of their requirements with the same or similar hacking tools.

Hence, most countries have been trying to expand the civil-military cooperation for the mitigation of cyber threat not only in the war-time and in the peace time. Whenever new malware is shown up, government agencies and companies share the signature information to make detection rules or develop defense methods with new technologies. The cyber situational awareness (CSA) can help detecting initial breach in parallel with understanding comprehensive operational environments to share information with kinetic activities.

In spite of previous efforts, the cyber threat detection in real time is still remained as a big challenge. In practice, military forces build security operation centers (SOC) for conducting cyber operations in a complex global security environment. For this purpose, we have studied technologies related to an enhanced CSA and discussed in a partial effort of the Seoul Defense Dialogue (SDD).

In this article, we presented three main objectives of our research as a partial effort of SDD.

- Share knowledge and experiences on the cybersecurity research and development based on civil-military cooperation.
- Ensure survivability and resilience capability based on cognitive technology with open source platforms.
- Enhance CSA capability for prevention, mitigation and recovery of military information systems from adversarial attacks.

The rest of this article is organized as follows. Section 2 places our research into the field of related work. Section 3 discusses the background of security issues for military operations and the international cooperative work for cybersecurity. Section 4 provides our research on technological achievement for cybersecurity. Our conclusion is shown in Sect. 5 with future work.

2 Research Background

2.1 Cybersecurity in Military Operations

In the military, most warfighting and business information systems are becoming more complex to being monitored and protected by commercially available anti-virus and

anti-APT (Advanced Persistent Threat) solutions those acclaim more than 99% malware detection. Security professionals have challenges of constantly evolving current information and network environments that of the emergence of the Internet of Things (IoT), the transition to software defined networks (SDN) and the proliferation of embedded mobile devices with the spread of cloud services [1, 2].

The operational environment is the composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander [3]. It encompasses cyberspace of networks, systems and information to provide current and predictive knowledge of operational environments including all factors affecting friendly and adversary forces. In the defensive cyber operations, for both military operations and the public safety, the situational awareness (SA) must be maximized so operational risks may be mitigated, managed, or resolved prior to a mission or during operations but it is very time consuming and costly [4].

The Endsley's definition of SA is that it denotes a person's "perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future [5]." To detect, analyze and correlate intrusion events through the network and application monitoring, the capability of performing strategic and tactical analysis should be improved based on the collected threat information in real time.

There are several perspectives on cyber capabilities depending on the specific situation of countries and requirements for the military forces. In spite of each circumstances, the more commercial information technology is adopted into military systems rapidly.

2.2 Cooperative Effort to Mitigate Cyber Threat

In the year of 2012, the deputy minister-level and civil experts on security affairs participated an international dialogue that was held in Seoul for the purpose of interchanging opinions in the region of Asia-Pacific named Seoul Defense Dialogue (SDD). In the SDD, participants had consensus about the importance of cybersecurity and settled a working group on the cybersecurity continuously named the Cyber Working Group (CWG).

Since 2014, Korean Ministry of National Defense has hosted the SDD CWG to play a consultative body to foster multi-lateral cooperative effort of responding to growing cybersecurity effectively. In the year of 2017, the SDD CWG was an opportunity for the participants came from twenty-one countries and two international organizations to build trust, and to get one step closer to cooperation in matters of cyber defense and cybersecurity.

Information technology has generated much faster tempo in modern military operations and has changed the reactive posture into the proactive defensive operations, persuasion and more generally achievement of the competitive information advantage in the battle space. In the public society, exaggerated fears of cybersecurity even with a little harm may cause huge economical damage [4]. A futuristic direction would include methods for establishing cooperative relationship between elements of the defense force and the public. The diplomatic effort with neighbor countries to share cyber threat information and a comprehensive global norm is important as like an

enhancement of domestic technical capability. However, effective collaboration is difficult in the domain of cybersecurity.

In the SDD CWG, participants discussed two objectives 'Deployment of cyber security technology developed through civil-military cooperation' and 'Confidence building for global cybersecurity' in the era of digital transformation age. The delegations showed a special interest in a role for civil-military collaboration of the state-of-the-art cybersecurity technology [6].

2.3 Cognitive Technology in the Cybersecurity

Traditionally the cybersecurity service has been provided by on-premise infrastructures with well-known concepts. In cyber operations, strategic cybersecurity capability process must show connectivity in the information environment and help navigate that environment. Digital transformation urges technological innovation to fill the gap between offensive and defensive posture.

Cyber situational awareness models provide a new paradigm to view the platform-based ICT environment such as weapon systems, internet services and business systems. A platform constitutes a set of the network traffics to be connected friendly forces and adversaries.

Security intelligence comes from the experiences of cyberattacks. However, it is more challenging to detect malicious codes in today's complex network environments while cyberattacks taking instantaneous effect in a privileged position against adversaries. In the defensive perspective, the detection of cyber threats and information leakage must be achieved in real time and defenders need to rethink the effectiveness of indicators of compromises (IoC) (Fig. 1).

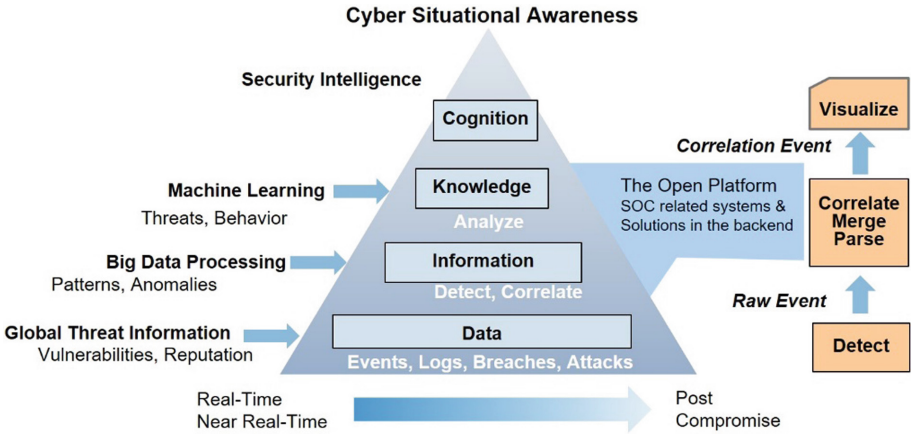

Fig. 1. A conceptual view for cyber situational awareness with related cognitive technology and required information.

3 International Cooperative Cybersecurity

3.1 Lessons Learned from the Seoul Defense Dialogue Cyber Working Group

The Seoul Defense Dialogue (SDD) 2017 contributed to establishing "a culture of multilateral defense dialogue" thorough an active and diversified defense exchange and cooperation under the main theme of "Visions for Security Cooperation in an Age of Uncertainty [6]." There are number of international agreements or treaties are existed for cyber cooperation among countries in a shape of bilateral or multi-lateral. In this perspective, the SDD CWG is an opportunity for the delegates to build trust and cooperation in matters of cybersecurity.

In today, policymakers in Korea as well as western countries often portray North Korea as posing an organizational hacking group. North Korean officials described cyberspace as a highly asymmetric and decisive domain of warfare as like the western countries define it a domain of battlespaces [3]. But usually there is little evidence of skill or subtlety by North Korean military forces regardless of overt damage like destroying data or causing information leakage.

The secrecy regarding the cyber capabilities and activities between South and North Korea creates difficulty in estimating the relative balance of cyber power in Asia-Pacific region. That is the reason why the SDD announced that the main theme of "Visions for Security Cooperation in an Age of Uncertainty [6]." Working group members representing their countries and organizations presented their views on confidence-building measures together with their cyber policies.

Previously, the US and the NATO countries have thrived the Tallinn Manual for more than decade as an international norm. In spite of previous effort, there is no solid international treaty concerning on cyber operations.

In the panel discussion, many participants and invited presenters talked especially on security solutions powered by artificial intelligence (AI) and big data technologies in an era of the digital transformation age. They shared their opinions about various strategies for deploying AI-based cybersecurity technology in the defense sector. In the next session, they discussed on the topic of "Confidence-building for global cybersecurity."

Even though AI has a potential, security professionals must aware of gaps between the technology and appropriate information. Those are very expensive and another challenging issue that will be discussed continuously in the SDD CWG. However, the scientific intricacies of cyber technology and bureaucratic issues sometimes prohibit civil-military cooperative research and investigation. Policymakers may depend on ideas and opinions from experts especially for technology dependent areas.

3.2 A Strategy to Counter Cyber Threat

The information systems generate huge amounts of log data difficult to be analyzed in real time. The existing techniques for predictive protection take input as some pre-processed or mined data that becomes time consuming. Hence most organizations

continue to invest in prevention-only strategies since enterprise systems are under continuous attack and are compromised with limited visibility in advanced attacks.

The cyber operational environment is rapidly evolving and CSA models do not support uncertainty appropriately that leaves us exposed to dangerous influences without proper defenses. It is critical to regard the cyber domain not as a separate warfighting space, but rather an integral component of each of the traditional battle spaces. The operational environment can be characterized by technical features against various attacks that typically take advantage of security vulnerabilities. It thrives the weaponization of information.

A desirable starting point for research direction would be changing mindset shift from existing blocking and prevention capabilities to a new approach of enterprise security immune systems. Many global security companies use their next-generation solutions with AI technology and one of participants in SDD CWG showed the current status of security intelligence [6, 7].

In order to enhance the performance of predictive analysis, the cybersecurity system encompasses event correlation technique within the data processing phase. In addition to correlation of security alerts, we require valid and proper predictive log analysis to track the adversarial tactics, techniques and procedures (TTP). Such a resource ideally isn't achievable by one country or organization based on their isolated experience, though. Instead, it should focus on cooperation between different organizations to be capable of quickly adapting to new cyber-attacks.

COGSEC uses intelligent technologies to be resilience over time, learning with each interaction and getting better at preventing threats proactively. It is basically based on rule-based approach for processing real-time events and produces attack classes as output for multistage attack detection [8]. The security intelligence gives military forces an information superiority because it helps security professionals know what enemies might do in the future, offering indicators of potential compromises. This approach is a big challenge, allowing information superiority in the cyberspace. A COGSEC architecture uses a security operation center (SOC) that supports continuous detection and protection with security intelligence. Security professionals need to understand how to improve threat detection, monitoring and incident response capabilities especially for freedom of maneuver in cyberspace.

COGSEC services leverage advanced threat defense, along with security analytics, which can be expensive, difficult to obtain and hard to sustain for many organizations, but is vital in defending and fighting through cyberspace in order to assure the security interests and systems. Because enterprise systems produce a lot of data, and it would be impractical to take on the burden of collecting and analyzing it in real time.

That's why IT security industries are dedicated to collecting up-to-date threat intelligence together and offering it as actionable business intelligence for security service providers. Event processing typically acts upon log files or network messages like SNMP. In the perspective of networks, detecting the exploit is essential since every phase after that can be encrypted by the attacker [10, 11]. Hence the security event monitoring in many organizations is focused on internet and network perimeter, ingress-egress traffics, rather than lateral (east-west) movement, once an attacker is inside the organization [9].

4 Cognitive Technology for Cyber Situational Awareness

Cognitive security (COGSEC) is a next generation cybersecurity concept to mitigate cyber threats, and managing escalation and hardening cybersecurity capability against cyberattacks. The COGSEC can empower the CSA to harness the intelligent analytics within tremendous volume of datasets [12, 13].

What is needed for COGSEC is a security operation center (SOC) to develop and apply relevant tools those are integrated into legacy cybersecurity systems. Open platforms for a cyber security operation center (SOC) have already begun to emerge [14]. Those are fundamental infrastructures of our ever-changing information environment and to defend us in that environment both in the military and private sectors (Fig. 2).

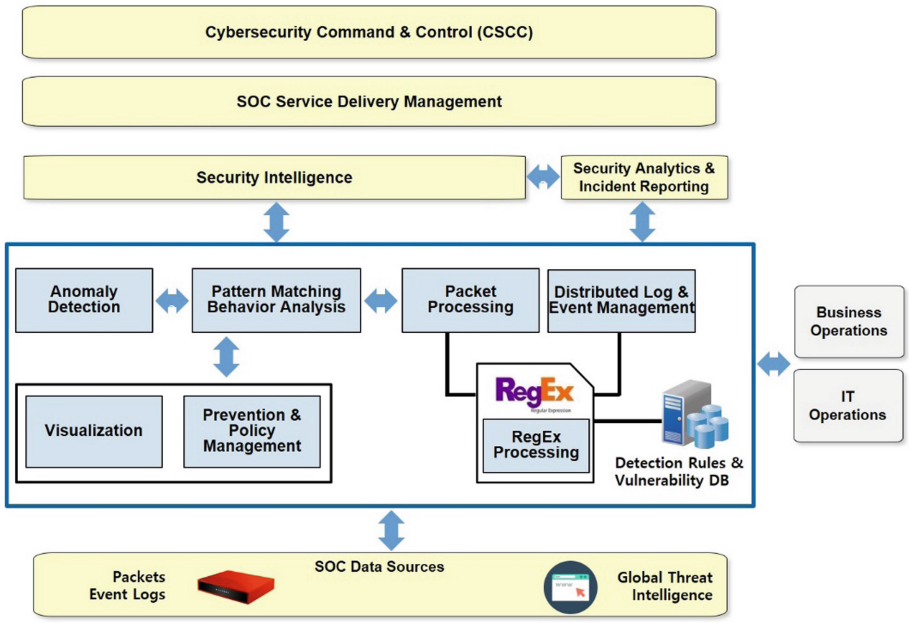

Fig. 2. A conceptual view of SOC and COGSEC architecture proposed by Petabi Corp.

Unstructured data such as video, audio and application specific data have to be translated to an universal language for effective analysis and information sharing. Regular expressions offer a more expressive method for representing patterns over fixed binary strings. Several commercial and open source tools adopted it and several high-performance regular expression matching libraries can increase the throughput performance of intrusion detection systems such as Hyperscan, Snort, Bro and Suricata in an effective way but it does not support full PCRE features.

Since PCRE has become a de facto standard in regular expression matching, it is important to provide full PCRE features for detecting malicious codes and their variants. Petabi's regular expression matching software library REmatch utilizes parallelism that is already available in various CPUs for high-speed matching in capable of providing full PCRE features as shown in [1].

4.1 Event Correlation Based on Regular Expressions

The two pillars of cognitive technology are data sets and algorithms. The primary data source is network packets and log data, but heterogeneous security devices produce threat information, vulnerabilities and configurations in various formats. In the previous research, we developed PERL compatible regular expression processing toolkit, names REmatch, in real time [1]. In addition, we have developed an event enumeration and correlation tool, called REconverge, that can read these events and automatically condense the events into smaller, but more meaningful events, that can be propagated further into the system [15].

The event processing system must assure worst-case processing capabilities in order to handle large amounts of events. Regular expression based pattern matching performance for log analysis, threat management, network security event monitoring and user behavior analysis (UBA) has been developed to provide line-speed processing without incorporating special purpose hardware [15].

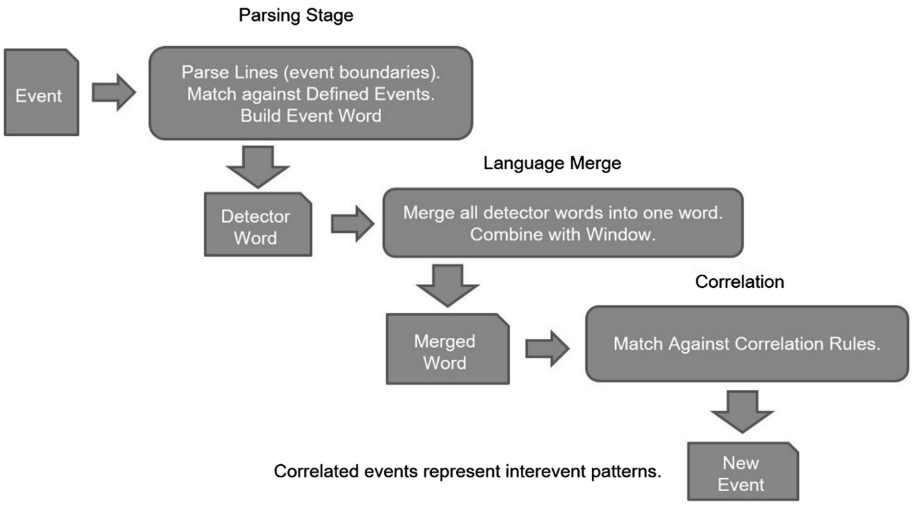

Fig. 3. Event correlator workflow

Transforming events into regular expressions can provide identification of threats through analysis of frequent signatures from massive datasets for effective anticipation of the environment at the edge of network segments. We have studied these shared patterns for automatic analysis and propose a framework for clustering and classifying

malware based on regular expressions. A schematic overview of our analysis framework is depicted in Fig. 3. It provides semi-supervised classification of 'Base Events' with a regular expression processing method rather than text based event log processing.

For this particular evaluation, 4 million randomly generated events were processed by a single Universal Translator with only a single Detector and with the number of events. All tests were performed in a single-threaded process on a MacBook Pro with 2.9 Ghz i5 CPU and 16 GB RAM.

An event system must have good worst-case processing capabilities in order to handle large bursts of events. We have implemented our event processing using high-speed regular expression matching to ensure no bottlenecks from that crucial aspect of this work. Non-optimized regular expression matching ran at speeds 100 times slower than the worst-case processing times. Regardless, we further optimized the critical path to minimize any extraneous processing.

Table 1 illustrates the statistics concerning the training sets employed and the resultant number of clusters. It correlations across a diverse set of data formats with universal language and in small latency. Our approach can reduce processing overhead and leads to low utilization of memory. It makes use of such highly processed data for future attack prediction which makes the system more efficient.

Table 1. Number of events and derived clusters with training data.

Data	Total events	Total clusters
Nginx access log	1,240,874	216
Nginx error log	562,244	80
Auth.log	8,555	39

4.2 Cognitive Security with Open Platforms

We have studied regular expressions and COGSEC technologies, open platform and CSA framework while emphasizing formality and quantitative measurement, as distinct from the more conceptual discussions. For the speed and scalability, compatibility and quality in the cybersecurity of military operations, the overall achievement of this study can be used for security professionals and enterprise security systems for enhancing CSA. It usually supports decision makers in relation to knowing about the state of an operating environment and relevant entities within the complications relating to cyber defense and problems of strategic instability.

Figure 4 shows the conceptual architecture of our methodology and software toolkits. Many organizations install firewalls or IPS's as initial response systems to cyber threats. In this paper, we recognize that any detector, be it a logging system, a sensor, a Network Intrusion Detection System (NIDS), or an event message from a router, will speak a language. We further recognize that these languages can be translated into an Universal Language that can be shared among detectors. Further, we note that each detector language will demonstrate common cases that can be used to

classify and define that language. This simple, powerful, transformation provides the groundwork for comparison of events across time and space.

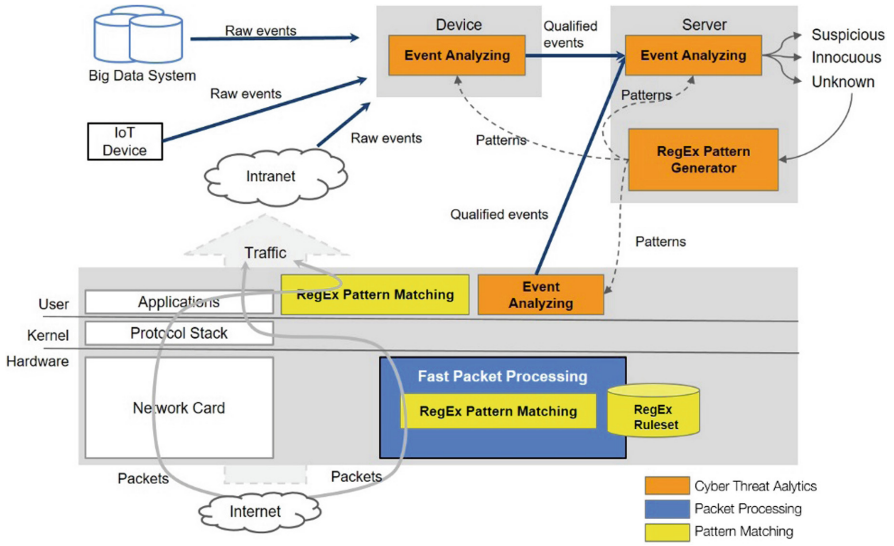

Fig. 4. An architectural view of network packet and event correlation processing based on regular expressions in real time.

Advanced analytics and other software tools help security analysts detect anomalies and determine high-risk threats, but the volume of information combined with the rate and sophistication of attacks has made it nearly impossible for any single analyst to keep up. Our toolkits need to be able to recognize patterns involving events. First, integrating cognitive technologies into military operations is necessary both for developing effective policies and for enhancing the cyber situational awareness.

The main contribution of the research effort can be transferring the previous cooperative work to a mission-oriented integrated security management. In the past, network packets and event logs from various devices treated and processed by security professionals in a batch mode as an incident response.

By taking COGSEC with our regular expression based analytics technology, cybersecurity professionals can be more mission-oriented with relevant data to understand cyber operational environment. Consequently, it can enhance the CSA capability with an information superiority.

5 Conclusive Remarks

The current military operational environment is putting new requirements on cyber operations. Although the cybersecurity has not fundamentally altered the nature of war, it nevertheless has consequences for important issues of new normal including

non-military threats and the ability of hacktivists, criminals to influence both international and private sectors. One of intrinsic characteristics of cybersecurity is the dependency between military and civil technology. Hence there are various strategies for possibility of adopting civil technologies into military information systems.

The civil-military cooperative work is unlikely to the traditional criterion of research because cyberweapons are not overtly, and malware is characterized by covert and diverse behavior in various forms of simple modifications of previous malicious codes or a new method. It is reasonable that the artificial intelligence technology can be regarded as a future direction of cybersecurity research.

In the Seoul Defense Dialogue Cyber Working Group, we acknowledged a consensus on the civil-military cooperation for the end-to-end protection and workforce trainings. Those issues are main topics of the SDD CWG for the future of collaboration and acceleration progress both technology and policy. It is generally accepted that it is almost impossible to prevent all cyber threats at the edge of networks.

This article has described the CSA and its related technological research achievement in the perspective of defensive operations. The changing requirements coupled with technological advancements have triggered a paradigm shift in the design and establishment of a SOC that is a core infrastructure of the CSA.

In the future, the research and development plan will proceed as demonstrating the generality and applicability of this approach in a practical way and implementing feedback from both in the simulation and real environments. Also, the SDD CWG will be held at Seoul from 12 September for 3 days and productive discussion related cybersecurity enhancement is expecting.

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

References

1. Park, H.K., Kim, M.S., Park, M., Lee, K.: Cyber situational awareness enhancement with regular expressions and an evaluation methodology. In: IEEE MILCOM Conference 2017, October 2017
2. Cisco, I.: Cisco visual networking index: forecast and methodology (2014–2019), Cisco white paper, May 2015
3. United States Army War College Strategic Cyberspace Operations Guide, June 2016
4. Matthews, E.D., Arata III, H.J., Hale, B.L.: Cyber situational awareness. Army Cyber Institute, West Point (2016)
5. Endsley, M.: Toward a theory of situation awareness in dynamic systems. Hum. Factors **37** (1), 32–64 (1995)
6. Ministry of National Defense, Republic of Korea, Seoul Defense Dialogue 2017, Book Chapter 10, September 2017
7. Dheap, V., Hale, V.: Applied cognitive security complementing the security analyst. In: RSA Conference 2017, February 2017
8. Vaarandi, R., Kont, M., Pihelgas, M.: Event log analysis with the LogCluster tool. In: IEEE MILCOM Conference, November 2016

9. Crowly, C.: Future SOC: SANS 2017 Security Operations Center Survey. SANS Institute InfoSec Reading Room, May 2017
10. Schales, D., Hu, X., Jang, J., Sailer, R., Stoecklin, M., Wang, T.: FCCE: highly scalable distributed feature collection and correlation engine for low latency big data analytics. In: Proceedings of ICDE, pp. 1316–1327, April 2015
11. Krizak, P.: Log analysis and event correlation using variable temporal event correlator (VTEC). In: 24th LISA Conference, November 2010
12. Rieck, K., Trinius, P., Willems, C., Holz, T.: Automatic analysis of malware behavior using machine learning. J. Comput. Secur. **19**(4), 639–668 (2011)
13. NIST, SP 800-92 Guide to Computer Security Log Management, NIST CSRC, September 2006
14. OSSEC: Open Source Host Intrusion Detection Security. https://ossec.github.io
15. Valgenti, V.C., Lin, Y.W., Suzuki, A., Kim, A.S.: Simulating exploits for the creation and refinement of detection signatures. In: IEEE MASCOTS (2017)