Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 8 pp. 461-467, 2023

https://doi.org/10.5762/KAIS.2023.24.8.461
ISSN 1975-4701 / eISSN 2288-4688

국제 다자회의 발전을 통한 국방 사이버안보 향상 방안 연구

유도진, 이용준*
극동대학교 해킹보안학과 교수

Advancing Defense Cyber Security through the Development of International Multilateral Conferences

Dohjin Yoo, Yongjoon Lee*
Department of Hacking & Security, Far East University

요 약 사이버안보의 중요성이 급증하면서 국제 사회는 공격과 방어의 경계가 모호해지고 국가급 배후의 공격자들이 새로운 공격 기법을 개발함에 따라 대응이 어려워지고 있다. 이를 토대로 2022년 진행된 서울안보대화(SDD)와 아세안 국방장관확대회의(ADMM-PLUS)에서는 사이버안보에 대한 주요국과 ASEAN 국가들의 다양한 인식과 시스템적 차이로 인한 어려움을 고려하여 사이버안보 의제를 모색하였다. 본 연구는 이러한 논의를 통합하여 사이버 모의훈련(CAX)을 통한 전략 발전, 국제기구간 협력 강화, 국가 간 신속한 정보공유 체제 구축, 국제규범화와 신뢰구축 등의 방안을 제시하였다. 또한, 체계적인 사무국 운영과 효율적인 DB 관리, 다양한 참석자 확대, 사이버 범죄 공동 해결 논의, 다자 안보회의 주관, 실무자급의 다양한 참여기회, 전문가 패널 섭외 및 사이버 훈련장 운영에 대한 사전 준비 등의 구체적 방안을 제안하였다. 이를 통해 국제 사회의 사이버안보 환경 개선과 우리나라의 사이버안보 체계 강화가 기대되며, 사이버안보가 기술적 문제를 넘어서 협력과 공유, 실천이 필요한 다차원적 주제임을 강조한다. 이 연구는 사이버안보 이슈를 심도 있게 이해하고 효과적으로 대응하기 위한 중요한 발판을 제공할 것으로 예상된다.

Abstract With the growing importance of cyber security, the international community is struggling to respond as the boundary between offense and defense becomes ambiguous and state-backed attackers develop new techniques. In 2022, the Seoul Defense Dialogue and the ASEAN Defense Ministers' Meeting-Plus (ADMM-PLUS) has sought cyber security agendas that consider the varied perceptions and systematic differences among nations. This study proposes strategies such as development through cyber exercise, enhancement of cooperation between international organizations, construction of rapid information-sharing systems, and trust-building. Additionally, it offers specific measures like systematic secretariat operation, efficient DB management, expansion of various participants, and preparations for cyber training fields. This study emphasizes that cyber security is a multi-dimensional subject requiring collaboration and practice, and it could provide an important foundation for understanding and effectively responding to cyber security issues.

Keywords : Cybersecurity, Multilateral Conference, SSD, ADMM-Plus, Information Sharing

1. 서론

작년부터 지속되고 있는 러시아-우크라이나 전쟁으로 인해 UN과 NATO 등의 국제기구는 안보분야에서 더욱 적극적인 역할이 요구되고 있다. 한편 러-우 전쟁에서도 알 수 있듯이 최근의 전쟁 양상은 대규모의 재래식 군사력 충돌뿐만 아니라 사이버-전자전 분야에서의 군사작전 개념이 포함되고 있다[1]. 특히 사이버전 분야에서 발사

*Corresponding Author : Yongjoon Lee(Far East University)
email: bigman2u@naver.com
Received June 29, 2023 Revised August 3, 2023
Accepted August 10, 2023 Published August 31, 2023

의 왼편작전(Left of Launch) 개념을 포함하여 우군 무기체계의 네트워크와 정보시스템 등을 보호하거나 적의 군사정보를 해킹 및 사이버 자산의 가용성을 제한시키는 공격의 성공여부가 전쟁의 'Key'가 되는 중요한 역할을 하고 있으며, 이를 위해 인공지능 기술을 활용한 보안공격을 비롯하여 최신 기술과 융합된 사이버전이 전개되고 있다[2]. 또한 사이버안보 분야는 국가간의 전쟁 뿐 아니라 민간기업을 포함하여 전 세계적으로 영향을 미치고 있으며, 따라서 이를 방지하고 선제적으로 대응하기 위한 다양한 방안이 그 어느 때보다 요구되고 있다[3]. 즉, 사이버안보 분야에서 우군의 핵심정보를 보호하고 자산의 가용성을 제한시키는 네트워크 및 시스템 공격에 대응할 수 있는 인프라를 발전시켜야 하며, 이를 위해 '국제 사회의 사이버안보 강화를 위한 모의훈련과 정보공유 전략'의 연구 필요성을 제기할 수 있다. 따라서 UN, NATO, ASEAN 등 국제기구와의 협력을 통해 제반 사이버안보의 강화 방안을 모색해야 하며, 특히 우리나라의 서울안보대화(Seoul Defense Dialogue, 이하 SDD) 및 아세안국방장관확대회의(Asean Defense Ministers Meeting Plus, 이하 ADMM-PLUS) 등 다자안보회의에서 사이버안보 분야 발전을 위한 논의를 통해 국가 간 사이버안보 협력을 강화하고 적의 사이버 공격에 대응하는 방안을 마련할 수 있을 것으로 기대된다. 본 논문은 다음과 같이 구성된다: 제1장은 서론으로, 사이버안보의 현재 상황과 중요성을 개괄하며, 연구의 필요성과 목표를 제시한다. 제2장은 SDD 운영결과 및 발전방안으로, SDD의 사이버안보 분야에서의 운영 결과를 분석하고 발전방안을 모색한다. 제3장은 ADMM-PLUS 운영결과 및 발전방안으로, ADMM-PLUS에서의 사이버안보 협력과 모의 훈련의 실시 및 결과 분석을 포함하여 운영 결과를 검토하고 발전 방안을 제안한다. 제4장은 결론으로, 연구의 주요 발견과 통찰을 종합하고, 향후 사이버안보 강화를 위한 전략과 방향을 제언한다. 이 연구는 국제 사회의 사이버안보 강화에 기여할 것으로 예상되며, 다자 모의 훈련과 정보 공유, 협력 체계 구축의 중요성을 강조하였다.

2. SDD 운영결과 및 발전방안

2.1 '22년 SDD 운영결과

2022년 SDD 사이버워킹그룹(Cyber Working Group, 이하 CWG)은 3년 만에 대면으로 개최되어 국제기구의 국방분야 관료 및 국내외 다양한 사이버안보 전문가가 참석하여 사이버안보 협력을 논의하였으며, 이를 통해 사이버안보에 대한 국제사회의 높은 관심이 확인되었고, 사이버안보 분야에서 우리나라의 위상과 리더십도 제고되었다[4]. 특히 워킹그룹의 역할이 확대되어 워킹페이퍼를 제작하여 공동의 성과물을 도출하고 관리하여 참가의지를 독려하는 등 구체적인 성과를 도출하였으며, 이를 통해 국제사회에서 사이버안보 분야 협력체계 강화에 기여하였다. 또한 SDD CWG은 참가자들의 만족도를 설문조사하여 프로그램 완성도를 제고하였다. 설문조사 결과, 대부분의 참가자들은 프로그램 구성이 적절하다고 평가하였다. 또한, 2023년도 SDD에도 다양한 주제를 다루는 프로그램을 바란다는 응답이 많았다. 향후 초청할 국가, 국제기구, 연구기관과 관련해서는 ASEAN 국가, 일본, 터키 등이 제시되었다.

2.2 설문조사 및 평가분석

본 설문은 SDD 프로그램 전반에 대한 참가자들의 만족도 조사와 함께 참가자들의 의견을 피드백하여 SDD의 완성도 제고하고자 실시하였다. 조사대상은 SDD 참가자 중 답변자이며, 총 12문항으로 참가자들의 이메일로 Google Forms 설문조사 참여를 요청하였다. 조사 결과, 총 34명이 유의미한 답변하였으며, 세션 구성의 만족도에 있어서 대부분인 90%가 SDD 프로그램 구성이 적절하다고 평가하였다. 다만 일부 참여자들은 암호기술 분야 관련 내용의 부재와, 프로그램에서 다루는 내용의 어려움으로 인해 만족하지 않은 것으로 아래 Fig. 1과 같이 나타났다.

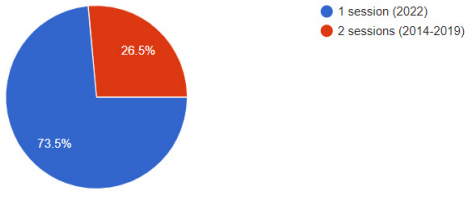

Fig. 1. 2022 SDD CWG Session Satisfaction

프로그램의 흥미도(관심도)는 참여자들의 대부분이 높게 평가하였으며, 이에 대해 YES로 응답한 인원은 2023년도 SDD에도 참석을 희망한다는 의사를 밝혔다. 또한 NO로 응답한 인원은 2023년에 SDD에서 다루기 바라는 주제를 구체적으로 제시하였다. 이를 정리하면 아래 Fig. 2와 같다.

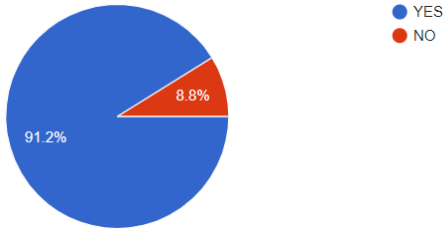

Fig. 2. 2022 SDD CWG Program Interest

한편 SDD의 1박 2일 구성 및 본회의와 별도로 단독 진행 등 프로그램 일정 변경 후 참석 의향에 대해서는 73.5%가 찬성하였으며, 26.5%는 현행이 더 필요하다는 의견이 나타났다. 이를 정리하면 아래 Fig. 3과 같다.

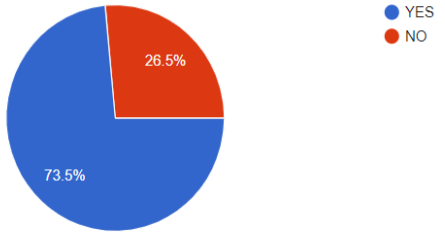

Fig. 3. CWG Willingness to Attend After Schedule Change

2.3 발전방안 및 도출 절차

2.3.1 도출 절차

사이버안보 분야의 전문가 및 참가자들과의 자문회의와 워크숍을 개최하였으며, 이전 연도의 SDD와 다른 유사 행사의 운영 경험을 분석하였다. 이를 통해 현행 방식의 한계와 새로운 아이디어, 전략 등을 도출하였으며, 위 설문의 결과를 바탕으로 다각도 평가 및 검토를 진행하였다.

2.3.2 발전방안

발전방안으로 조직체계와 행사 운영의 개선이 제시되었다. 이를 위해 SDD 사무국의 체계적 운영이 필요하며, 업무 프로세스와 효율적인 DB관리가 강화되어야 한다. 특히 DB관리는 참가자의 관심사, 행사 내용, 참가자의 만족도 등의 정보를 체계적으로 모으고 분석함으로써 향후 행사 운영에 있어 더욱 효율적인 계획 및 실행을 가능하도록 할 것이다. 또한 참석자 수준을 높이는 것도 중요한 발전방안이다. 이를 위해 차관급 인사의 참석을 확대하고, 국내외 NGO의 참여를 적극 활성화시키는 것이 필요하다. 더불어 국내 연구소 및 단체의 참여를 확대하는 것 역시 중요하다. 이를 통해 전문성을 높이고, 더 넓은 시야에서의 토론이 이루어질 수 있게 한다. 코로나-19 팬데믹 이후 2년간 행사가 진행되지 않았으므로, 이와 관련된 다양한 어려움이 있었다. 이를 극복하기 위해 매년 고정된 행사시기와 장소를 확정하는 것이 필요하다. 이를 통해 참가자들, 특히 고위관료들의 참가 일정을 사전에 반영할 수 있게 하여 참가율을 높이고, 행사의 안정적인 운영을 보장할 수 있다. 이러한 방안들은 SDD가 국제적인 사이버안보 토론의 플랫폼으로서의 역할을 강화하고, 더욱 전문적이고 협력적인 환경을 제공하는데 기여할 것으로 예상된다. 추후 이러한 발전방안이 체계적으로 실행되고 평가되면서 SDD는 지속적으로 성장하고 발전할 수 있을 것이다.

3. ADMM-PLUS 운영결과 및 발전방안

3.1 국내 전문가 패널 강연

우리나라는 전문가 패널을 통해 한국인터넷진흥원(이하 KISA)의 팀장급 구성원이 참석하여, 국내의 다양한 정책과 프로그램을 통해 사이버보안 전문가 양성방안을 설명하였다. 특히 융합보안 대학원 등을 운영하여 보안 전문가를 배출하는 것과 KISA BoB(BEST OF THE BEST) 및 K-Shield 등의 인재양성 프로그램으로 훈련생을 전문가급의 사이버보안 인재로 육성하며, 실전형 사이버 훈련장의(Security-Gym) 운영을 통해 실전형 공격 및 방어훈련을 실시하고 보안 전문가 인력을 양성 방안을 설명하였다. 또한 국내에서는 지역 맞춤형 사이버 훈련이 필요하다는 인식이 고조되었다[5]. 이에 따라 정부에서 실전형 사이버 훈련장을 4개 수준으로 확대하고 대학과 산업계의 협업을 통해 지역에 맞는 실전 대응 인력을 양성할 계획을 세우고 있음을 설명하였다. 또한, 군 대상으로도 실전형 훈련장을 운영하고 융합보안 대학원 등에서 사이버 직무에 특화된 군 전문인력을 양성할 예정이며, 이러한 노력을 통해 국내 사이버보안 분야의 전문인력 양성에 기여하고 있음을 논의하였다. 또한 의장발언을 통해 실질적으로 각 국에서 수행하는 사이버 훈련 방안 등에 대한 공유를 통해 자국의 사이버 능력 발전 계획 수립에 기여할 수 있는 논의의 진행 필요성을 제기하였으며, 이에 각 국의 호응을 확인하였다.

3.2 ASEAN 및 PLUS국 발표

ASEAN 및 PLUS국이 사이버안보와 관련된 현안들에 대해 의견을 나누고, 각 국가들이 추진 중인 사이버 교육훈련, 인력 관리, 보안 기술 및 역량 개발 등에 대한 내용을 발표했다. 특히 미국의 경우 국가차원에서 사이버 교육훈련을 추진하며, 호주는 디지털 포렌식 등에 대한 관심을 나타냈다. 이 외에도 다양한 국가들이 각자의 사이버안보 분야에서 주목할 만한 발전 내용을 발표했다. 특히 미국의 경우 GS14 이상 뿐 아니라 GS 9~6급의 실무 레벨에서도 다양한 참여기회 보장해야 실질적이고 실무에서 공유 가능한 회의가 진행될 수 있음을 주장하였다. 또한, 역내 다자간 사이버안보 분야의 국가간 파트너십 형성을 위한 공동지침으로서 검토·작성 중인 사이버안보 프레임워크 수정안 발표와, ASEAN 회원국만을 대상으로 하며, 플러스국은 초안 검토 등 작성을 지원하는 역할에 한정된다는 내용으로 ASEAN 회원국 토의가 이루어졌다.

3.3 원격 사이버 모의훈련

원격 사이버 모의훈련(이하 CAX)은 각 군의 사이버 공격에 대한 탐지·대응 능력 향상을 목표로 계획되었으며, 사이버보안의 국방분야에 초점을 맞춘 시나리오 기반으로 회원국간 공동대응 연습을 통해 사이버안보 억지력 강화하고자 하였다.

3.3.1 훈련 구성

훈련은 가상환경에서 회원국 2~3개국이 1개 팀을 구성하여 각 시나리오별로 주어진 문제를 해결하고, 같은 팀으로 구성된 국가간 의사소통하여 해답을 공유하는 방식으로 진행되었다. 훈련 참가는 회원국당 사이버보안 전문가 2명 이내로 훈련단을 편성하였으며, 美·中 포함 14개국, 총 33명이 참여하였다. 팀 구성을 살펴보면 2~3개국이 1개팀 구성으로 플러스국 1개국, ASEAN 1 ~ 2개국 정도로 편성하여 ASEAN국과 플러스국간의 협력대응을 도모할 수 있도록 하였다. 이를 정리하면 아래 Table 1과 같다.

Table 1. Cyber Wargaming CAX Team Formation

GroupA	GroupB	GroupC	GroupD	GroupE	GroupF
AUS	IND	KOR	CHN	*	USA
BRN	IDN	KHM	LAO		MYS
PHL	SGP	THA	MMR		

또한 시나리오는 랜섬웨어, 봇넷, 공급망 공격의 대응을 중점으로 아래 표와 같이 3가지 시나리오로 구성하여, 각 시나리오별 CAX 팀이 대응 연습할 수 있도록 구성하였다.

Table 2. Cyber Wargaming CAX Scenario Formation

Class	Details	Focus
Scenario 1	XX Aviation, a defense company of Country XX, is infected with ransomware. Analyze the ransomware to restore the aircraft blueprints.	Ransomware
Scenario 2	Signs of an attack are detected on the defense network of the XX military. Analyze the intrusion traces to determine the extent of the damage.	Botnet
Scenario 3	A PC with an Agent installed at XX Aviation experiences a ransomware infection incident. Decrypt the encrypted files.	Supply Chain Attack

3.3.2 훈련 진행

위 공격 시나리오 발생 상황 하에, 사이버보안 실무자 관점에서 공격 식별 및 팀간 정보를 공유하여, 4시간 동안 랜섬웨어, 봇넷, 공급망 위협 등 최근 사이버의 주요 위협에 대한 방어작전 중심의 시나리오를 토대로 상황별 4개의 문제 해결하였다[6-8]. 이는 주요국이 모두 참가 또는 참관(일·러)하며 진행된 최초의 사이버훈련으로, 회원국들도 적극적으로 참여 및 호응하였다.

3.3.3 훈련 결과

그룹별 성적은 한국이 속한 그룹 C와 그룹 D가 총 5문제 해결하였으며, 국가별 성적에서는 총 12문제 중, 한국이 5문제, 다음으로 중국, 필리핀 각 3문제 해결, 말련, 싱가포르, 미얀마가 2문제 해결, 호주·인도·인니가 각 1문제를 해결하였다. 이를 정리하면 아래 Table 3와 같다.

Table 3. Cyber Wargaming CAX Results

Cls.	Group A	Group B	Group C	Group D	Group F
No.	AUS(1)	IND(1)	KOR(5)	CHN(3)	USA(0)
	BRN(0)	IDN(1)	KHM(0)	LAO(0)	
	PHL(3)	SGP(2)	THA(0)	MMR(2)	MYS(2)
Res.	4	4	5	5	2

또한 아래 표와 같이 적색구간 안에서 일정 시간 미해결 시 강제 해결 및 점수 배부하여 최종 결과를 아래 Fig. 4와 같이 산출하였다.

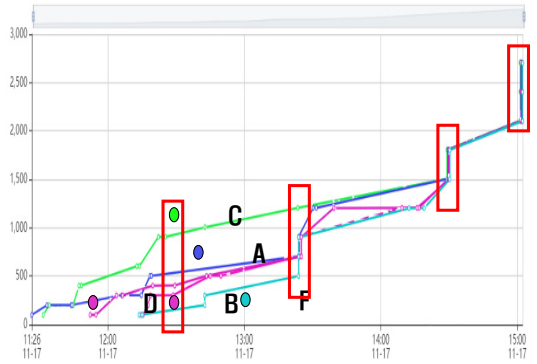

Fig. 4. Cyber Wargaming CAX Score Calculation

한국이 최다 문제를 해결하는 등 의장국으로서 우리 군의 높은 사이버안보 역량 우위 증명하였으며, 시간에 비해 많은 문제가 주어진 것으로 판단, 추후 훈련 시 문제 갯수·시간 등 종합적 고려의 필요성이 논의 되었다. 한편 CAX의 경우 첫 훈련이고 원격으로 의사소통이 쉽지 않아, 주어진 문제에 비해 시간이 다소 부족한 면이 식별되었으며, 특히 미국이 사실상 참관하는 등 일본을 비롯한 주요 플러스국의 참여 부재로 각 국의 구체적 사이버안보 억지력 평가에는 일부 한계가 존재하였다.

3.4 발전방안 및 도출 절차

3.4.1 도출 절차

사이버안보 정책 및 전략 공유 방안의 발전을 위해 현장 토론 및 분석을 진행하였다. 사이버 모의 훈련(CAX) 및 각 국가의 사이버안보 현안 발표를 분석하고, 토론을 통해 실현 가능한 정책과 전략의 공유가 필요하다는 결론에 도달하였다. 또한 현행 모습에서의 다자간 협력의 경향성 및 한계점을 식별하여, 랜섬웨어 대응 등 사이버 범죄 공동 해결에 집중해야 한다는 공통의 의견을 도출하였다. 각 국가에서 수행하는 사이버 훈련 방안 등에 대한 공유를 통해, 자국의 발전 계획 수립의 필요성을 인식하였다. 사이버워킹그룹의 운영체계를 개선하기 위해 SSD 사무국과 연계하여 '사이버안보 다자회의 사무국 구성'의 필요성을 논의하였다. 실무자급의 참여기회 확장, 국내외 NGO 참여 활성화를 통한 논의의 다양성에 대한 검토 및 계획을 수립하였으며, 기획단계에서부터 관련 유관부처와의 협업을 강조하였다. CAX 관련 개선 방안으로 미·일·러 등 선진국을 훈련에 참가시키기 위한 참여 분위기 마련의 필요성을 논의하였다. 주어진 문제와 시간, 참가 국가의 역량 등을 종합적으로 평가하며, 향후 훈련의 문제 개수 및 시간 조정 등에 대한 논의를 진행하였다. 마지막으로 발전방안에 대한 종합적인 논의를 통해 각 국가의 동의를 받았으며, 의장국의 주도 하에 각 부문별 발전방안을 마련하고 실천 방향을 설정하였다. 이러한 절차를 통해 구체적인 발전방안을 도출하였으며, 그 결과를 토대로 앞으로의 사이버안보 협력과 훈련, 그리고 정책 구축 등에 대한 지속적인 노력과 집중이 필요하다는 결론에 도달하였다.

3.4.2 발전방안

사이버안보 정책 및 전략 공유 방안 관련해서 실현 및 공유 가능한 사이버안보 의제가 제시되어야 함이 강조되었다. 또 회의 진행간 현재 모습은 다자간 협력보다 자국에 대한 안보 위협 최소화를 통해 균형을 모색하는 경향이 존재함이 나타났으며, 이를 해소하기 위해 군사적 측면에서 사이버 작전능력 등 국가경쟁력과 직결되는 주제보다는 랜섬웨어 대응 등 사이버 범죄 공동 해결 논의 등의 방안 구축 필요성이 나타났다. 우리나라가 의장국 발언에서 진행하고 각 국이 동의하였듯이 실질적으로 각 국에서 수행하는 사이버 훈련 방안 등에 대한 공유를 통해 자국의 발전 계획 수립에 기여 필요성이 제기되었다. 한편 사이버워킹그룹 운영체계 개선에서는 앞서 논의한 SSD 사무국과 연계하여 국제다자회의를 주관하는 가칭 '사이버안보 다자회의 사무국 구성' 필요성이 제기되었으며, 여기서는 전문가 불참 등의 우발상황 대비하거나, 매년 고정된 행사시기·장소 사전 확보, 기획단계에서부터 관련 유관부처와의 협업 필요성이 제기되었다. 또한 실무자급에서도 다양한 참여기회를 보장하고, 국내외의 NGO 참여 활성화를 통한 논의의 다양성 확장 필요성이 확인되었다. CAX 관련해서는 향후 사이버안보 분야 선진국인 미·일·러 등을 훈련에 참가시켜 ASEAN 회원국의 기술 역량 증진을 위한 훈련 목적에 부합되도록 진행할 수 있도록 참여 분위기 마련 필요하다는 의견이 제기되었으며, 이렇게 도출된 발전방안을 통해, 사이버안보 협력과 훈련의 효과적인 진행을 위한 다양한 접근 방식과 전략을 마련하였으며, 이를 통해 전체 사이버안보 체계의 향상을 기대할 수 있을 것이다. 이러한 노력은 앞으로도 지속되어야 하며, 국제적인 협력과 공동의 노력을 통해 보다 안전한 사이버 공간을 구축하는데 기여할 것으로 예상된다.

4. 결론

사이버안보 이슈는 현재 국제사회에서 가장 중요한 아젠다 중 하나로 논의되고 있으며, 공격과 방어의 경계가 모호하고, 국가급 배후의 공격자들이 새로운 공격 기법을 계속 개발하고 있어 방어가 점점 어려워지고 있다는 점에서 그 중요성이 강조된다[9]. SDD와 ADMM-PLUS에서도 사이버안보를 대하는 주요국과 ASEAN 국가들의 상이한 인식, ICT 인프라, 다양한 시스템적 차이로 인한 어려움이 존재한다. 이에 대응하기 위해, 우리는 적극적 행위자로서의 역할을 강화하고, 집단 방어권 행사를 위한 국제 규범화, 신뢰 구축 조치를 추구하는 의제 관리 등의 역할을 수행해야 한다. 이를 위해 우선, 조직 체계와 행사 운영의 개선이 필요하다. 이를 위해 체계적인 사무국 운영과 효율적인 DB 관리를 추진하며, 다양한 인사의 참석과 국내외 NGO, 및 연구소 등 단체의 참여를 확대하여 참석자 수준을 높이는 노력이 요구되며, 의제의 조기 선정 및 충분한 사전 협의 기간을 확보하는 등의 우발 상황 대비도 필요하다. 다음으로, 실현 가능하고 공유할 수 있는 사이버안보 의제가 제시되어야 한다. 군사적 측면에서의 사이버 작전능력 등 민감 주제보다 랜섬웨어 대응 등 사이버 범죄 공동 해결 논의 등 방안을 모색해야 한다. 이를 통해 각국이 자국의 발전 계획 수립에 기여할 수 있는 방안을 공유하고, 사이버워킹그룹의 운영 체계를 개선하여 다자 안보 회의를 주관하는 '사이버안보 다자회의 사무국'의 구성을 추진해야 한다. 여기서는 다양한 우발 상황에 대비하고, 매년 고정된 행사 시기와 장소를 사전에 확보하며, 기획 단계에서부터 관련 유관 부처와의 협력이 필요하다는 점이 강조되었다. 또한 GS14 이상 고위급이 아닌 GS9~6등 실무자급에서도 다양한 참여기회를 보장하며, 국내외 NGO 참여 활성화를 통해 논의의 다양성확장 방안을 모색해야 한다. 이 뿐 아니라 사이버안보전략과 정책을 개발하고 공유하는 과정에서는 전문가 패널의 섭외와 다양한 우발상황에 대비할 수 있도록 준비하며, 국내 사이버 훈련 진행 동향을 추적하고 실전형 사이버 훈련장 운영에 대한 사전 준비를 하는 것이 필요하며, 사이버 모의훈련을 지속적으로 개발해야 한다. 특히, 미·일·러 등을 훈련에 참가시켜 ASEAN 회원국의 기술 역량 증진을 위한 훈련을 진행을 유도하는 노력이 요구된다. 이러한 훈련은 각 국의 기술력 향상뿐이 아닌 사이버 공간에서의 안전성과 신뢰성을 높이는데 기여할 것이다. 이러한 부분에서 사이버안보는 단지 기술적 문제를 넘어서 다양한 차원에서의 협력과 공유 및 실천이 필요한 주제임을 다시 한 번 강조한다. 우리는 이러한 과제들을 인식하고, 이를 통해 국제 사회의 사이버안보 환경을 개선하고, 우리나라의 사이버안보 체계를 더욱 강화할 수 있을 것으로 기대된다.

References

[1] D. J. Yoo (2023). Research on Countermeasures Against the Cyber Weapon System of the Chinese Hacking Group Xiao Qi-ying: SQL Injection and OSINT-Based Known Vulnerability Attacks. Korean Association for Information Systems, 24(6), 267-273. DOI: https://doi.org/10.5762/KAIS.2023.24.6.267

[2] U. S. Song, & H. S. Jo, (2021). The operation of 'Left of Launch' and Suggestion of Cyber Deterrence Strategy in Korean Peninsula. Strategy Studies, 28(3), 37-78. DOI: https://doi.org/10.46226/jss.2021.11.28.3.37

[3] D. G. Kim, J. H. Cha, J. D. Lee, & S. S. Baek, (2022). A Study on the Establishment of a Military Art System for Cyberwarfare from the Analysis of Ukraine-Russia War. Korean Journal of Military Studies, 78(2), 1-21. DOI: https://doi.org/10.31066/kjmas.2022.78.2.001

[4] Editorial Department. (2022). Ministry of National Defense, 2022 Seoul Security Dialogue: Complex Security Threats, International Community Solidarity Response, Korea-Japan Vice Ministerial Meeting. Defense and Technology, (524), 16-18.

[5] Y. H. Choi, I. S. Jang, I. T. Hwang, T. G. Kim, S. J. Hong, I. S. Park, J. S. Yang, Y. J. Kwon, & J. M. Kang, (2020). Design and Implementation of Cyber Range for Cyber Defense Exercise Based on Cyber Crisis Alert. Journal of Korea Information Security, 30(5), 805-821. DOI: https://doi.org/10.13089/JKIISC.2020.30.5.805

[6] J. Y. Moon, & Y. H. Jang, (2016). Ransomware Analysis and Method for Minimizing the Damage, 2(1), 79-85. DOI: https://doi.org/10.17703/JCCT.2016.2.1.79

[7] J. M. Yang, (2015). The Criminal Regulation of Internet of Things Cyber Crime. Criminal Law Trends, 48, 305-350. DOI: https://doi.org/10.23026/crclps.2015..48.008

[8] E. G. Lee, & J. D. Kim, (2019). A Case Study on ICT Supply Chain Attacks. Information Research, 16(4), 383-396. DOI: https://doi.org/10.22865/jita.2019.16.4.383

[9] J. I. Lim, Y. J. Kwon, G. H. Jang & S. J. Baek, (2014). North Korea's Cyber War Capability and South Korea's National Counterstrategy. Defense Policy Studies, 29(4), 9-45. DOI: https://doi.org/10.22883/jdps.2014.29.4.001

유 도 진(Doh-Jin Yoo) [정회원]

- 2021년 8월 : 명지대학교 대학원 보안경영공학과 (공학박사)
- 2020년 9월 ~ 현재 : 행정안전부 정보통신 안전교육 전문인력
- 2022년 9월 ~ 현재 : 극동대학교 해킹보안학과 교수
- 2023년 2월 ~ 현재 : 한국국가정보학회 이사

〈관심분야〉
사이버보안, 개인정보보호, 중국학

이 용 준(Yong-Joon Lee) [종신회원]

- 1999년 2월 : 강남대학교 전자계산학과 (공학사)
- 2001년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2005년 2월 : 숭실대학교 컴퓨터학과 (공학박사)
- 2010년 2월 ~ 2016년 3월 : KISA 사이버침해대응본부 수석연구위원
- 2010년 2월 ~ 2016년 3월 : 군사안보지원사 국방보안연구소 연구관
- 2016년 4월 ~ 현재 : 극동대학교 해킹보안학과 교수

〈관심분야〉
사이버보안, 산업보안, 융합보안