국방 사이버안보 발전 방안

유도진, 이용준
극동대학교 해킹보안학과 교수
e-mail:2022080@kdu.ac.kr, 2020032@kdu.ac.kr

Study on the Development Strategies of Multilateral Cybersecurity in National Defense

Prof. Dr. Do-Jin Yoo, Prof. Dr. Young-Jun Lee
Dept. of Hacking Security, Far East University

요 약

러시아-우크라이나 전쟁의 지속과 함께 국제기구들은 안보 분야에서 더욱 적극적인 역할의 필요성이 대두되고 있으며, 특히 최근 전쟁의 양상이 대규모의 재래식 군사력 충돌뿐만 아니라, 사이버-전자전 분야에서의 군사작전 개념이 포함되면서 사이버안보의 중요성이 대두되고 있다. 이에 본 연구는 2022년 서울안보대화(Seoul Defense Dialogue, SDD)와 아세안국방장관확대회의(Asean Defense Ministers Meeting Plus, ADMM-PLUS)를 분석하여 국방 사이버안보의 보장에 기여하는 방안을 제시하였으며, 주요 내용을 축약하면 첫째, 국제기구와 협력 강화; 둘째, 국가 간 정보공유 체제 구축; 셋째, 국제규범화와 신뢰구축 추구이다. 이를 통해 다자안보회의 발전과 국가 간 사이버안보 협력 강화, 적 사이버 공격 대응 방안의 마련이 기대된다..

1. 서론

작년부터 지금까지 지속되고 있는 러-우 전쟁으로 인해 NATO 등 국제기구는 안보분야에서 더욱 적극적인 역할이 요구되고 있다. 한편 최근의 전쟁양상이 대규모의 재래식 군사력 충돌뿐만 아니라 사이버전 분야에서 우군의 네트워크와 정보시스템 등을 보호하거나 적의 군사정보를 탈취 및 사이버 자산의 가용성을 제한시키는 공격의 성공여부가 전쟁의 'Key'가 되는 중요한 역할을 하고 있으며, 이를 위해 S/W와 악성코드가 사용되거나, AI 기술을 활용되고 있다. 또한 사이버안보는 민간기업을 포함하여 전 세계적으로 영향을 미치고 있으며, 따라서 이를 방지하고 선제적으로 대응하기 위한 다양한 방안이 그 어느 때보다 요구되고 있다고 할 수 있다. 즉, 사이버안보 분야에서 우군의 핵심정보를 보호하고 자산의 가용성을 제한시키는 네트워크 및 시스템 공격에 대응할 수 있는 인프라를 구축해야 하며, 이를 위해 '국방 사이버안보 발전 방안'의 연구성이 제기된다. 이를 통해 국가 간 사이버안보 협력을 강화하고 적의 사이버 공격에 대응하는 방안을 마련할 수 있으며, 국제기구와의 협력을 통해 제반 국가안보를 강화할 수 있는 방안을 모색하는데 기여할 수 있다.

2. SDD 운영결과 및 발전방안

2.1 '22년 SDD 운영결과

2022년 SDD 사이버워킹그룹(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. 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 적절

하다고 평가하였다. 또한, 2023년도 SDD에도 다양한 주제를 다루는 프로그램을 바란다는 응답이 많았다. 향후 초청할 국가, 국제기구, 연구기관과 관련해서는 ASEAN 국가, 일본, 터키 등이 제시되었다. 이를 토대로 더욱 향상된 프로그램을 제공하여 국제사회에서 사이버안보 분야에서의 강력한 협력체계를 구축하는데 도움을 줄 수 있다.

2.2 설문조사

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

2.3 발전방안

발전 방안으로 조직체계와 행사 운영을 개선이 제시되었다. 이를 위해 사무국 운영이 필요하며, 체계적인 업무 프로세스와 효율적인 DB 관리가 필요하다. 또한 참석자 수준을 높이기 위해 차관급 인사 참석 확대와 국내외 NGO 참여 활성화, 국내 연구소 및 단체의 참여자 확대 필요성이 제기되었다. 또한 행사 운영에서는 코로나-19 이후 2년간 행사가 진행되지 않아 어려움이 있었으며, 매년 고정된 행사시기와 장소를 확정하여 고위관료의 참가일정을 사전에 반영할 수 있도록 하고, 전문가 불참 등의 우발상황 대비도 강구되어야 함이 지적되었다. 한편 의제선정에서는 의제 조기 선정 및 충분한 사전 협의기간을 확보하고, 전문가 자문회의 구성, 의제 선정 및 내용 구체화를 필요와 더불어 의제에 대한 깊이 있는 연구로 토론 활성화 유도가 필요하다는 의견 등이 제시되었다.

3. ADMM-PLUS 운영결과 및 발전방안

3.1 '22년 ADMM-PLUS 운영결과

우리나라는 전문가 패널을 통해 국내의 다양한 정책과 프로그램을 통해 사이버보안 전문가 양성방안을 설명하였다. 특히 융합보안 대학원 등을 운영하여 보안 전문가를 배출하는 것과 BoB와 K-Shield 등의 프로그램으로 훈련생을 전문가급 사이버보안 인재로 육성하며, 실전형 사이버 훈련장(Security-Gym)을 운영하여 실전형 공격 및 방어훈련을 실시하고 보안 전문가 인력을 양성 방안을 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 주장하였다.

3.1.2 ASEAN 및 PLUS국 발표

ASEAN 및 PLUS국이 사이버안보 관련 현안들에 대해 의견을 나누고, 각 국가들이 추진 중인 사이버 교육훈련, 인력 관리, 보안 기술 및 역량 개발 등에 대한 내용을 발표했다. 특히 미국은 국가차원에서 사이버 교육훈련을 추진하며, 호주는 디지털 포렌식 등에 대한 관심을 나타냈다. 이 외에도 다양한 국가들이 각자의 사이버안보 분야에서 주목할 만한 발전 내용을 발표했다. 또한, 역내 다자간 사이버 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.

3.2 원격 사이버 모의훈련

원격 사이버 모의훈련은 각 군의 사이버 공격에 대한 탐지·대응 능력 향상을 목표로 계획되었으며, 사이버보안의 국방분야에 초점을 맞춘 시나리오 기반으로 회원국간 공동대응 연습을 통해 사이버 안보 억지력 강화하고자 하였다.

3.2.1 훈련 방법

본 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 모의훈련단을 편성하였으며, 美·中 포함 14개국, 총 33명 참여하였다. 팀 구성을 살펴보면 2~3개국이 1개팀 구성으로 플러스국 1개국, ASEAN 1~2개국 정도로 편성하여 ASEAN국과 플러스국간의 협력 대응을 도모할 수 있도록 하였다.

[표 1] 사이버 모의훈련 팀 구성

그룹 A	그룹 B	그룹 C	그룹 D	그룹 E	그룹 F
호주	인도	한국	중국	*	미국
브루나이	인니	캄보디아	라오스		말련
필리핀	싱가포르	태국	미얀마		

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

[표 2] 사이버 모의훈련 시나리오 구성

구분	세부사항	중점 사항
시나리오1	XX국의 방산업체인 XX항공이 랜섬웨어에 감염, 랜섬웨어를 분석하여 항공 설계도를 복원	랜섬 웨어
시나리오2	XX군 국방망에서 공격 흔적이 발견, 침해 흔적을 분석하여 피해 규모를 확인	봇넷
시나리오3	XX항공에서 Agent가 설치된 PC가 랜섬웨어감염 사태가 발생, 암호화된 파일을 복호화	공급망 공격

3.2.2 훈련 진행

3가지 공격 시나리오 발생 상황 하, 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. 이는 회원국내 주요국이 모두 참가 또는 참관(일·러)하며 진행된 최초의 사이버훈련으로, 회원국들도 적극적으로 참여 및 호응하였다.

3.2.3 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.

[표 3] 사이버 모의훈련 결과

구분	그룹 A	그룹 B	그룹 C	그룹 D	그룹 F
개수	호주(1)	인도(1)	한국(5)	중국(3)	미국(0)
	브루나이(0)	인니(1)	캄보디아(0)	라오스(0)	말련(2)
	필리핀(3)	싱가포르(2)	태국(0)	미얀마(2)	
해결	4	4	5	5	2

위처럼 한국이 최다 문제를 해결하는 등 우리 군의 높은 사이버안보 역량 우위 증명하였으며, 시간에 비해 많은 문제가 주어진 것으로 판단, 추후 훈련 시 문제수·시간 등 종합적인 고려의 필요성이 제기되었다.

2.3 발전방안

사이버안보 정책 및 전략 공유를 위해 다자간 협력과 자국 안보 위협 최소화가 필요하며, CWG 운영체계를 개선하기 위해서는 사무국 구성, 기획 협업, 다양한 참여 등의 필요성이 제기되었다.

한편, 사이버 모의훈련 관련해서는 ASEAN 회원국의 기술 역량 증진을 위한 훈련을 추진할 수 있으며, 이를 위해 참여 분위기를 마련해야 함이 강조되었으며, 이러한 발전 방향을 위해서는 사전 협의, 연구 및 토론 활성화, 온라인 운영체계 강화, 사이버안보 전문가 및 선진 기술 도입 등의 필요성이 제기되었다.

4. 결론

사이버 안보는 현재 국제안보에서 가장 심각한 위협중 하나로 간주되고 있다. 이러한 사이버 공간에서의 안보는 공격과 방어의 경계가 분명하지 않고, 국가급 배후의 공격자는 새로운 공격 기법을 계속 개발하고 있어 방어가 점점 어려워지고 있다. SDD와 ADMM-PLUS는 사이버 안보를 대하는 주요국과 ASEAN 국가의 상이한 인식, ICT 인프라, 다양한 시스템적 차이로 인해 어려움이 있다. 이에 우리 군은 적극적 행위

자로서 역할을 강화하고, 집단 방어권 행사를 위한 국제규범화, 신뢰구축조치를 추구하는 의제관리 등의 역할을 수행해야 한다. 따라서, 사이버안보 정책 및 전략의 개발 및 공유, CWG 운영체계의 개선, 다자적 사이버 모의훈련의 지속적 개발이 필요하다. 이를 위해 전문가 패널 섭외 등 다양한 우발상황에 대처할 수 있도록 대비해야 하며, 국내 사이버 훈련 진행 동향을 추적하고 향후 실전형 사이버 훈련장 운영에 대한 준비가 사전 준비되도록 유관 기관과의 지속적인 협력이 필요하다.

참고문헌

[1] Deloitte (2022). Cyber Smart: Enabling APAC Businesses, 2022.
[2] KISA (2022). 상반기 사이버위협 동향 보고서, 2022.
[3] ITUPublications (2020). Global Cybersecurity Index 2020.
[4] ITUPublications (2020). ICT Development Index 2017.
[5] Song Tae-Eun (2022). “Cyber Warfare in the Russo-Ukrainian War: Assessment and Implications”, 2022.
[6] 외교부 (2022), 아세안 개황, 2022. 10.
[7] 이형동, 윤준희, 이덕규, 신용태 (2022), 러시아-우크라이나 전쟁에서의 사이버공격 사례 분석을 통한 한국의 대응방안에 관한 연구, 한국정보처리학회, 2022