<요약보고서>

* 국방 사이버 분야 국제협력 방안 연구

□ 서 론

○ 국제사회 사이버 환경

- 급속한 과학기술의 발전과 정보화에 따라 국제사회의 안보구조는 커다란 도전에 직면
 - * 군사기밀은 물론 첨단무기 및 적대세력에 관한 기밀자료, 금융기관의 시스템 정보, 국가 공공기관의 중요 정보시스템 등 국가의 안보에 큰 영향을 미치는 요소들은 항상 사이버 공격의 위협에 항상 노출
- 사이버공간에서 사이버범죄나 사이버공격 등의 각종 위협은 증가
 - * 사이버위협은 해킹, 디도스, 기밀절취, 정보시스템 무력화 등 다양한 형태로 발생
- 사이버안보의 국제정치는 미중 간에 벌어지고 있는 영향력 확대 경쟁과 상호간 견제, 국제기구 간에 벌어지고 있는 사이버 패권경쟁 심화
- 사이버위협이 강대국 정상 간의 회담 시 최우선으로 다루어지는 의제로 채택
- 세계 각국은 이미 사이버 공격을 국가적 안보 위협으로 인지하고, 사이버 안보태세를 강화함과 동시에 사이버 전장에서 우위를 차지하기 위한 전략을 구체화

○ 사이버에 대한 우리 군의 인식

- 사이버는 재래식 무기를 통한 군사적 위협과 함께 국가안보를 위협하는 요인
- 정보통신 기술과 인프라의 발전에 따라 군의 제반 업무와 군사작전 수행도 사이버 공간에 의존하는 비율이 증가
- 첨단과학기술이 활용되는 군의 작전환경은 사이버 전장의 보이지 않는 적에게 대응할 수 있는 능력을 요구
- 사이버 공격의 형태가 다양화되고 북한·중국 등 해커에 의한 피해 규모가 커지면서 사이버위협에 대한 우려와 걱정은 날로 심화
- 우리나라도 사이버 공격 위협을 심각한 안보 문제로 인식하고 대응방안을 수립 중

○ 국제사회의 사이버 협력 현주소

- 각국이 참여하는 실질적 협의체 구성이나 국제규범 등의 필요성에도 불구하고 미국과 중국 진영 간의 이견으로 사이버 공간에 대한 국제적 합의 도출이 쉽지 않은 상황
 - * (미국 등 서방국가) 자유로운 정보의 유통을 보장하되 사이버 위협행위에 대해서만 기존 국제법을 적용해 통제하자고 주장
 - ** (중국 등 비서방국가) 각국의 국가 주권에 기초하여 국제법과 다른 별도의 사이버 관련 법을 제정하여 사이버 공간을 통제하고 관리하자고 주장
- 사이버위협 및 공격은 초국가적 형태로 진행되어 일국 차원의 대응으로는 한계가 있어 국제협력 및 협력체제가 불가결
- 심각해지는 사이버위협을 제거하여 사이버 전쟁이 발생되지 않도록 미연에 방지하고 사이버 평화안보체제를 구축할 수 있는 국방 차원의 사이버 국제협력의 노력이 필요

□ 주요 사이버위협 사례 및 최근 동향

○ 해외 주요 사이버위협 사례

- 러시아-에스토니아 사이버분쟁(2007년) : 러시아 해커 집단의 디도스(DDoS) 사이버 공격으로 에스토니아 국가기능이 마비된 사건
- 러시아-조지아 사이버전(2008년) : 러시아가 조지아의 정부와 금융기관은 물론 軍 정보시스템을 해킹하여 오작동을 유도한 사건
- 이란 나탄즈 핵시설 공격(2010년) : 이란의 핵무기 프로그램을 방해할 목적으로 이스라엘과 미국이 감행한 사이버 공격 사건
- 소니픽처스 해킹사건(2014년) : 북한 관련 해커집단이 소니픽처스의 기밀정보를 유출하고 내부 시스템을 파괴한 사건
- 러시아 미백악관 전산망 침투(2015년) : 러시아 해커들이 백악관 전산망을 침입하여 버락 오바마 미국 대통령의 일정과 관련된 비공개 정보에 접근한 사건
- 워너크라이 사이버공격(2017년) : 북한 소행으로 추정되는 워너크라이 랜섬웨어 (Ransomware) 사이버 공격 사건
- 솔라위즈(SolarWinds) 공급망 공격(2020년) : 러시아 정부 산하에 있는 첩보조직과 관련된 해커 집단의 소행으로 추정되는 공급망 해킹 공격 사건
- 러시아-우크라이나 사이버 공격(2022년) : 우크라이나 국방부, 외무부 등 정부 기관 사이트들과 대형 은행을 대상으로 한 러시아 소행의 사이버 공격 사건

○ 한국 사이버위협 사례

- 1.25 대란(2003년) : KT 해화전화국이 운영하는 시스템 서버에 트래픽 급증과 인터넷 접속 장애가 발생하고 중단된 사고
- 7.7 DDoS(2009년) : 북한의 110호 연구소의 소행으로 추정되는 3차에 걸쳐 실행된 사이버 공격 사건
- 3.4 DDoS(2011년) : 포털 사이트 및 공공기관의 웹사이트를 대상으로 한 분산 서비스 거부 공격(DDoS) 사건
- 농협 전산장애(2011년) : 농협 전산망 마비되어 현금인출기 사용은 물론 인터넷뱅킹까지 차단된 사건
- 3.20 사이버공격(2013년) : 안랩 서버 및 다수의 컴퓨터가 악성코드에 감염되어 막대한 피해를 입힌 대형 사이버테러 사건
- 6.25 사이버공격(2013년) : 웹사이트 변조 및 디도스(DDoS), 정당·군과 주한미군 병력의 개인정보 유출 등의 공격이 감행된 사건
- 한국수력원자력해킹사건(2014년) : 한수원 내 악성코드가 퇴직자 명의의 이메일을 통해 전파되면서 개인정보 및 설계도 중요 파일이 유출된 사건
- 국방부 통합데이터망 해킹(2016년) : 계룡대 데이터 서버가 북한으로 추정되는 해킹 세력에게 사이버 공격을 당한 사건
- 한반도 사드패치 공격(2017년) : 중국의 고고도미사일방어체계(THAAD)가 한반도 내에 전격 배치를 결정한 것에 대한 보복의 일환으로 중국이 해킹 공격을 가한 사건

- 한국원자력연구원 및 한국항공우주산업(2021년) : 한국원자력연구원 소속 직원의 개인정보가 북한 해커에 의해 유출되고 우리 군 최초 전투기인 KF-21 설계도면 등 다수의 기술 정보들이 해킹당한 사건

○ 사이버위협 동향

- 최근에 국제사회에서 사이버 공격 양상이 다양화되면서 국가에 미치는 피해 규모와 파급 영향이 더욱 심화
- 단순 호기심으로 시작된 개인 해커에 의한 사이버 공격이 조직화되면서 국가기능 자체의 혼란을 목적으로 하는 악의적이고 고도화된 해킹으로 발전
 - * 정치적 갈등 관계에 있는 국가를 대상으로 하는 사이버 불법 해킹, 불법 자금 조달 목적의 가상자산을 활용한 지능범죄, 군사기밀 및 방위산업 등의 국방 관련 기밀정보 탈취, 그리고 금융기관 해킹을 통한 불법 인출 등
- 군사적 측면에서 보면, 사이버 공격은 물리적 전쟁과 병행한 사이버 전쟁 등과 같이 전장 환경의 변화에 맞는 새로운 형태의 사이버위협 양상으로 발전
- 사이버 공격이 지속적으로 증가할 것으로 예상, 사이버 공격의 특성에 부합한 보다 효율적 대응을 위한 국가안보 차원의 대비와 관리 및 대응체계 필요
- 국제사회가 사이버안보에 관한 국제규범이나 군사적 신뢰 구축에 대한 합의 노력 필요

□ 국제사회의 사이버 협력 관련 기구

- 국제사회 내 사이버안보 다자협력 차원에서는 국제연합(Untied Nations, UN) 중심으로 진행, 유엔총회뿐만 아니라 여러 산하 조직에서 의제 논의를 추진
 - UN GGE(정부전문가그룹)과 OWEG(개방형실무그룹)를 구성하여 사이버안보 관련 국가 간의 사이버위협, 국제규범, 그리고 사이버 공간의 신뢰 구축 조치 마련 및 이행, 역량 강화 활동 등을 논의
 - UN 산하기구인 국제전기통신 연합(International Telecommunication Union)과 국제사이버안보다자간협력기구(IMPACT) 등에서 사이버안보 분야에 대한 대응과 협력, 사이버보안 관련 기술 연구와 정책 자문 등의 역할을 수행
- 이외에도 국제인터넷주소관리기구(IMPACT), 세계사이버스페이스총회(GCGS) 등 다양한 국제기구들이 사이버안보와 관련된 노력을 기울이고 있는 상황
- UN 등 국제기구 차원의 협력 외에도 각 지역 차원의 협력기구들을 통해 사이버안보를 위한 협력 역시 이루어지고 있음,
 - 유럽연합(European Union, EU)과 동남아국가연합(Association of Southeast Asian Nations, ASEAN) 등 지역 기구와 북대서양조약기구(North Atlantic Treaty Organization, NATO), 유럽안보협력기구(Organization for Security and Cooperation in Europe, OSCE), 상하이협력기구(Shanghai Cooperation Organization, SCO) 등 지역 안보 협력기구 등이 있음
- 국제 및 지역기구 차원의 노력 외에도 양국 차원의 노력, 민간 차원의 협력과 노력 역시 이루어지고 있으며, 컨퍼런스 및 국제회의 등을 통해 기술적 측면 외에도 사이버안보 전반에 대한 논의 등 다양한 노력이 추진중

- 미국은 현재 한국을 비롯하여 일본, 중국 등 11개국과 양자 사이버 협의를 실시하는 한편 EU와 ASEAN 등 지역기구와의 협력대화 추진과 더불어 NATO, OSCE, ARF 등과 긴밀하게 협력
- 일본은 미국, 영국, 호주, 인도, 한국 등 유럽·아시아 11개 국가와 양자 사이버 대화를 실시하고, EU와 ASEAN 등 지역 안보기구와도 사이버 협의를 실시
- 중국과 러시아는 사이버 협력을 강화하여 중러 사이버보안 협약을 체결하고 사이버 공간에서 서로에 대한 감시를 지양하고 각국의 법집행기관을 통해 기술 전수 및 정보 공유

□ 서방 주요국 사이버대응전략 및 추진체계

○ 미국

- 미국은 자국의 정보 인프라와 지적재산의 보호를 위해서 일찌감치 사이버안보를 강조하며 국가전략의 일부로 사이버안보 문제를 보는 포괄적인 전략을 추진
- 미국은 자유롭고 개방된 규칙에 기반한 국제질서(rule-based international order) 등 기본원칙에 기반한 국제규범과 거버넌스 구축을 추구하고 있으며 우방국들과의 연대를 강화하여 중국·러시아에 대항함으로써 사이버안보에서 전략적 우위를 장악하고자 노력
- 국제협력은 양자, 지역 동맹 강화를 통해 아태지역과 유럽지역에서 미국이 주도하는 사이버안보 방위전략을 구축하고 G7·NATO·EU 등과 함께 중국을 ‘구조적 도전(Systemic Challenge)’으로 규정하고 중국 견제체제를 구축
- UN GGE나 국제전기통신연합(ITU) 등과 같은 기존의 국제기구의 틀을 활용하기보다는 유럽안보협력기구(OSCE), NATO, 아세아지역포럼(ARF) 등 지역 차원에서 존재하는 지역 안보기구를 통한 협력체계 구축과 정부·학계·NGO 등 민간 이해당사자들이 모여 대화하는 글로벌 거버넌스의 논의에 주력
- 사이버사령부 군사조직 외에도 국토안보부(DHS), 국가안보국(NSA), 연방수사국(FBI) 등 민간분야에 초점이 맞춰진 정부기관 간의 긴밀한 협력관계 구축

○ 영국

- 사이버위협을 테러 행위와 함께 국가 안보를 위한 가장 큰 우선순위로 꼽은 바 있으며 유럽국가 중에서 가장 활발하고 적극적으로 대응
- 영국의 사이버안보 전략은 국익의 보호와 체제 수호를 위한 핵심 기반시설의 안전을 확보하고 국내 사이버위협에 대응하는 역량을 강화하는 동시에 사이버안보 공간의 안보 증진을 위한 서방 국가와의 국제연대의 필요성을 강조
- 브렉시트(Brexit) 이후 영국은 제2의 대영제국을 꿈꾸며 유럽연합(EU)과 일정한 거리를 두고 ‘글로벌 브리튼(Global Britain)’이라는 새로운 국가전략을 기치 아래 아시아·태평양 지역과의 협력 강화에 집중
- 악의적이고 범죄적인 사이버 공격에 대해서는 자기방어적 차원의 군사적 보복공격과 더불어 비용 및 책임부담, 경제제재 등 모든 수단을 동원하겠다는 의지
- 미국이 주도하는 국제질서에 적극 동참하고 자신들의 위상을 제고하고자 노력하며, 러시아·중국으로부터 지속적으로 발생하는 공동의 위협을 탐지하고 저지하기 위해 동맹국들과 계속 협력하며 집단안보를 강화

- 우방 국가들과의 양자협력과 UN, EU, NATO 등을 통한 다자 파트너십의 구축을 확대
- 내각부(Cabinet Office)가 주도하여 사이버안보 전략을 수립하고 시행하며 내무부, 외무부, 상업기술규제개혁부, 국방부 등이 영국의 사이버안보를 담당
- 사이버 공격 발생 시 영국군을 지원하고 사이버 방어를 담당하는 군사조직인 '사이버예비군'을 국방부 산하의 합동사령부 내에 창설하여 사이버 공간에서의 네트워크 시스템 보호 및 적국에 대한 사이버 공격을 담당

○ 독일

- 독일의 사이버안보 전략은 정보통신산업이나 프라이버시 보호보다는 국가의 주요 기반시설에 대한 사이버 방위에 상대적으로 더 많은 관심
- 독일은 NATO 국가 중에서 사이버 부대를 운영하는 첫 번째 나라로 국방 차원에서 사이버 공격으로부터 국가 기반시설을 방어하기 위한 임무를 수행
- 독일은 미국·영국과는 달리 민간 이해당사자들이 주도하는 글로벌 거버넌스 구축에 기여하기 보다는 정부가 주도적인 역할을 수행하는 전통적인 다자안보 협력기구의 틀을 활용한 지역협력에 중점
- 독일 연방군이 사이버 공격을 당했을 경우 자위권 차원에서 맞대응할 수 있는 사단급 이상의 사이버 정보사령부를 창설하여 운영
- 유럽 및 국제 사이버안보 정책에서의 독일의 적극적인 참여 등을 강조하면서 높은 수준의 사이버안보를 보장하기 위한 UN, EU, NATO, G8 등 국제기구 및 다자안보협력기구와의 협력체계 구축을 추진
- 연방제 국가인 독일은 연방내무부와 그 산하의 연방정보기술보안청(Federal Office for Information Security, BSI)을 중심으로 사이버안보 업무 수행

○ 캐나다

- 캐나다가 사이버안보에 대해 정부의 책임의식을 인식한 시점은 2000년 후반부터 시작했던 미국 및 서방 선진국들과 유사
- 사이버 공격이 국가 안보 위협 사안이며 개방적이고 자유로운 정보 흐름을 강조하고 다양한 이해당사자들의 참여해야 한다는 인식은 동맹국과 유사한 특징
- 캐나다의 사이버안보 전략은 전통적인 군사안보의 차원보다는 주요 인프라가 미국과 연결되어 있다는 관점에서 볼 때 정보보호 차원에서 전략을 수립
- 미국, 영국, 호주 등 이른바 파이브 아이즈(Five Eyes) 국가들과의 정보공유와 공조하고 UN, NATO, G8 등과 같은 서방 진영과의 다자외교의 장에서도 활발한 활동
- 또한, EU와 일본과도 양자 협력을 추진하고 있으며 일본과는 군사안보 차원의 협력이 아닌 기술자들 간의 정보공유 차원에서 협력 추진
- 캐나다에서는 공공안전부(Public Safety Canada, PSG)가 사이버안보 전략의 시행을 조정하는 역할을 맡고 있으며, 통신보안기구, 왕립기마경찰대, 안보정보청, 국방부가 사이버안보를 담당
- 국방부와 캐나다군은 네트워크를 수호하는 역량 강화에 집중하며 타 정부부처와 공동으로 사이버위협에 대응하고 NATO를 포함한 동맹국 군조직과 정보를 공유

○ 이스라엘

- 이스라엘은 오랜 시간 계속되어 온 아랍권 국가들과의 분쟁으로 국방 및 안보에 많은 자원을 투자
- 이스라엘의 사이버안보 전략이 모두 국방전략으로 관심사에만 머무는 것은 아니고, 정부와 민간기업과의 연계를 통해서 국가안보와 경제번영을 동시 추구하는 국가전략을 채택
- 이스라엘은 국가 존립을 인정하지 않는 아랍국가들로 인해 국제적으로 지지를 받지 못함에 따라 사이버 분야의 국제규범 논의보다는 자국의 사이버역량 강화에만 집중하는데 중점
- 미국과 친미 성향 국가와의 사이버안보 협력 및 공조하고 있으며 특히 일본, 인도, 싱가포르, 태국 등 아시아 국가와 사이버안보 파트너로 협력
- 사이버안보 정부 기관으로는 첩보활동을 하는 샤마크(Israel Security Agency), 총리실 산하 사이버안보부(Israel National Cyber Directorate)가 경제산업부·국방부 등 타 부처를 컨트롤타워하는 역할 수행

□ 한반도 주변국 사이버대응전략 및 추진체계

○ 일본

- 2010년대 접어들면서 일본의 사이버안보 전략은 날로 늘어나고 있는 사이버위협을 중대하게 인식하고 국가안보의 차원에서 적극적으로 대응하여 기존의 수동적 정책에서 주도적 정책으로 변화를 꾀하고 있는 중
- 사이버위협을 단순히 사이버 공간만의 문제가 아닌 국가 안보 전체의 위협으로 인식하고 사이버안보에 대한 대응을 집단적 자위권의 수단으로 활용
- 전통적인 우방인 미국과의 국제협력을 강화하고 양자 협력이나 다자외교를 추진하고 있으며 아세안 지역 국가들과의 협력에도 주력
- UN, OECD, APEC 등 국제기구와 다자 안보협력 기구 등 국제적 논의에 적극 참여함으로써 국제적 규범 형성에 노력
- 내각사이버시큐리티센터(NISC)가 정부 차원의 사이버안보 정책에 대한 조정과 통제하는 컨트롤타워의 역할뿐만 아니라 정부 정보시스템을 모니터하여 사이버위협을 감시·분석·대응하는 역할 및 국제협력 업무도 수행
- 사이버 국방전략의 차원에서도 자위대 산하에 사이버 방어를 감독하는 사령부를 창설하여 사이버 방위 부대(CDU)를 지휘하고 사이버 방위 인력도 1000명 수준까지 증원

○ 중국

- 중국은 미국과 국제질서의 수립과 운영에 있어 주도권을 경쟁하는 강대국
- 1990년 후반부터 금순공정(Golden project)이라는 이름으로 사이버안보 관련 정책을 추구, 자국 핵심 기반시설에 대한 사이버 공격의 위협뿐만 아니라 정치체제의 안전과 미국에 의한 국가주권의 침해(또는 미국의 기술패권)에 대한 방어적 태도를 바탕으로 추진
- 국방전략의 구체화나 사이버 공격을 군작전 개념의 일부로 포함시키고 사이버전을 담당하는 전략지원부대의 창설 및 사이버사령부(인터넷기초총부) 설치 등을 통해 가시화

- 미국이 주도하는 글로벌 거버넌스의 질서 구축에 대항하여 중국 주도의 새로운 사이버 질서를 모색, 중국의 입장에 동조하는 국가들과 지역협력과 국제기구 활동 추진
- 중국은 상하이협력기구, 아세안지역안보포럼 등 지역 내 협력기구에서의 적극적 논의를 통해 영향력을 확대하고 국제연합 GGE나 국제전기통신연합(ITU) 등과 같은 국제기구에서 진행되는 국제규범 수립과정에도 적극적으로 참여
- 국가주석이 총괄하는 중앙인터넷안전정보화위원회가 중앙 컨트롤타워로 사이버안보와 인터넷 단속을 총괄하고 있으며, 국가안전부,公安부, 공업정보화부, 국가보밀국에서 사이버안보를 담당

○ 러시아

- 러시아 사이버안보 전략의 기본방향은 정보 인프라나 지적재산의 보호보다는 러시아 정치사회체제의 안전을 확보하는데 주안
- 러시아는 사이버안보와 관련된 미국-서방의 규범과 인식, 그리고 개념에 동의하지 않으며 자신들이 독자적인 규범과 인식, 그리고 개념을 주장하고 국제적인 규범 표준으로 제시
- 다른 국가에 비해 사이버 부대의 운영이나 사이버사령부의 창설 논의 등이 일찍부터 시작되었고 보다 적극적이고 공세적인 대책들을 마련
 - * 2002년 세계에서 처음으로 해커부대를 창설, 2022년 이미 3,000여 명 이상의 사단급 병력을 보유
- 유엔 정부전문가그룹(GGE) 및 개방형워킹그룹(OEWG)과 같은 기존의 국제기구 활동이나 집단안보조약기구(CSTO), 상하이협력기구(SCO), 독립국가연합(CIS) 등 지역협력체의 틀을 활용하여 주권국가들이 협의하는 사이버안보 국제질서를 모색
- 러시아의 연방보안부(FSB)가 사이버안보 관련 기관을 총괄하면서 국가 비밀을 포함한 주요 정보 통제와 범죄예방을 하고, 연방통신정보국, 연방기술수출통제국에서 사이버 관련 업무를 수행

□ 한국의 사이버안보 전략 및 국제협력 현황

○ 북한의 사이버안보 위협

- 북한은 비대칭 전력 확보를 위해 사이버 부대를 증강하고 사이버 공격기술을 연마
- 김정은 집권 이후 사이버 능력은 핵·미사일과 함께 인민군의 3대 수단 중 하나로 간주, 북한의 사이버 공격 역량은 미국과 중국, 러시아에 이어 거의 세계 최고 수준으로 평가
- 북한 정부가 운용 중인 사이버 전사는 약 6800명에 달하는 것으로 추산되며 금융정보 탈취나 국가기밀 유출을 위해 세계 각국의 정부, 금융권, 군사시설 및 방위산업업체 등을 대상으로 사이버 공격을 광범위하게 시도
- 북한 이외에도 사이버 공격의 주요 근원으로 식별되고 있는 세계 최대의 해커조직을 보유한 중국발 사이버 공격에 노출되어 있는 상황, 국제적인 민간 해커집단 등 국제 사이버테러조직의 공격을 받을 가능성도 크게 증가

○ 한국의 사이버안보 대응 전략

- 한국은 국가정보화를 통해 정보화 인프라를 구축하고 경제·사회시스템을 비약적으로 발전시켰으며 행정기관을 중심으로 전자정부의 행정 효율성과 국민의 편의성을 크게 확장

- 한국에 대한 해킹·사이버 사기 등은 지속적으로 증가하고 있으며 특히 북한 및 중국에 의한 악성코드 유포와 DDoS 공격 등 사이버 공격이 끊임없이 발생
- 한국은 2005년부터 국가안보 차원에서 사이버위협에 대한 대응을 추진하기 시작하였는데 청와대 국가안보실을 컨트롤타워로 국가정보원, 과학기술정보통신부, 국방부가 각자 공공/민간/국방분야를 담당하는 민·관·군 종합 대응체계로 구축
 - * (국가안보실) 사이버안보 컨트롤타워로서 체계적인 사이버안보 수행체계 정립·발전, 사이버공간의 안전한 보호 및 사이버전 수행 능력 확보 등의 업무 수행 (국가정보원) 국가·공공기관에 대한 사이버공격을 예방·대응하는 업무를 수행 (과학기술정보통신부) 민간분야 침해사고 예방·대응체계의 구축 등 민간분야 정보보호에 관한 업무를 수행 (국방부) 사이버공간에서 사이버 작전을 수행하기 위해 '사이버작전사령부'를 두고 사이버작전의 계획 및 시행, 사이버작전과 관련된 사이버보안 활동, 사이버작전에 필요한 체계 개발 및 구축 등 사이버작전과 관련된 임무 수행
- 정부는 「국가사이버안보전략」의 구체적인 추진을 위해 2019년 9월 「국가 사이버안보 기본계획」 수립·발표하였고, 국가사이버안보 강화를 위한 이행방안을 중점·세부과제로 세분화하여 추진중

○ 한국의 사이버 국제협력 현황

- 한국의 사이버안보 국제협력은 국제사회의 사이버안보 논의와 유사하게 UN 정보안보정부전문가그룹 참여, 양자 및 삼자협력, 아세안지역 협력, 세계 사이버스페이스총회 등을 중심으로 추진
- 유엔에서 사이버안보 규범을 논의하는 UN 정부전문가그룹(GGE)에 2004년 출범 이후 현재까지 4차례 참여하고 있으며, 한미동맹 차원에서 미국과 사이버안보의 비전을 공유하고 사이버안보협력 채널의 제도화를 추진
- 미국·영국·호주 등과 양자 사이버정책협의회를 개최하고 아세안지역과는 아세안지역 포럼(ASEAN Regional Forum, ARF)을 통해 아세안 지역 국가와 사이버안보 협력을 추진
- 2017년부터 격년으로 유럽안보협력기구 (OSCE)와 공동으로 한-OSCE 사이버안보 컨퍼런스를 개최하여 아시아와 유럽(OSCE) 지역의 사이버 신뢰구축조치 경험을 상호 공유
- 2012년부터 각국 국방차관이 참석하는 서울안보대화(SSD)를 통해 세계 각국의 국방 관료와 민간전문가들이 한자리에 모여 긴밀한 소통을 하며 국제 안보협력방안을 논의
- 사이버테러, 사이버 범죄, 국제안보 등을 비롯한 사이버 관련 이슈를 종합적으로 논의하는 국제포럼인 세계사이버스페이스총회(Conference on Cyberspace)에도 적극적으로 참여

□ 국방 분야 사이버 국제협력 발전방안

○ 국방 분야 국제협력 현황

- 국방부는 미국을 포함하여 우방국과 양자 및 다자간 사이버 국제협력관계를 추진중
- 한·미간의 대응 능력을 향상시키기 위해 정보공유 및 사이버정책·전략·교리·인력·훈련 관련 협력 강화를 목표로 2014년부터 한·미 간의 사이버정책실무 협의체 운영

- 합참과 주한미군사가 공동 주관으로 토의식 연습(TTX)을 통해 원진·연합·합동 지휘통제체계(C4I)에 대한 사이버공격 시 한미 공동대응절차를 토의
- 방위산업 협력을 계기로 UAE와 정보·사이버 분야에서 협력을 확대 강화
- 호주와는 2022년 수교 60주년을 맞아 외교·국방(2+2) 장관회의를 통해 양자관계를 포괄적·전략적 동반자 관계로 격상하고 사이버안보와 핵심기술 협력 양해각서(MOU)를 체결
- 국방부가 주도하는 서울안보대화(Seoul Defense Dialogue, SDD)를 통해 사이버안보에 특화된 전문가 대화체인 사이버워킹그룹(CyberWG)을 개최
 - * 사이버워킹그룹(CyberWG)은 사이버 현안에 대한 의견과 경험을 공유하며 신뢰를 구축하는 다자 대화의 장

○ 국방 분야 사이버 국제협력 기본방향

- 타국과의 군사적인 유대를 강화하고 교류 협력을 확대함과 동시에 군사적 역량을 증진시키며 외국의 군사적 지원을 획득할 수 있는 방안 등을 모색 필요

○ 국방 분야 사이버 국제협력 발전에 대한 정책적 제언

① 국가 간 상호이해 및 신뢰 제고를 위한 인적교류 확대를 활성화

- 인적교류를 위한 양해각서(MOU) 체결을 통해 상대방 국가의 사이버 부대를 상호 정기적으로 방문할 수 있는 여건 마련 및 사이버 정책과 최신 기술을 경험할 수 기회 부여
- 세계적인 사이버 전문가가 모여 논의할 수 있는 다자간협의체나 심포지엄 등 다양한 국제적인 행사에 적극 참여

② 국가 간 공동의 안보목표를 달성하기 위해 정보공유 및 공조체계 구축을 강화

- 상대국과의 사이버안보 정책협의체 구성을 정례화하여 전략 및 정책을 공유하고 사이버위협에 공동 대응하기 위한 실질적인 협력을 확대·강화
- 주변국들과 사이버 공격 관련 위협정보를 공유
- 지역 평화와 안정과 北 사이버 공격에 대한 긴밀한 공조체계 유지를 위한 미국·일본·중국·러시아 등과 국방 사이버 핫라인 설치 (장기적으로 유럽안보협력기구나 동남아국가연합 국가까지 확대 설치)
- 방산기술 보호를 위한 국제적 공조체계도 구축

③ 국가 간 군사적 사이버 신뢰 구축조치를 위한 다양한 안보협력 추진

- 사이버 공격에 대한 국가적이고 종합적인 사이버 대응역량을 평가하고 확보하기 위한 국방 차원에서의 사이버 연습 및 훈련에 적극적인 참여 및 주관 시행
- 단순한 군사동맹을 넘어 사이버 군사지원을 통한 상호 신뢰에 기반한 글로벌 포괄적 전략동맹을 위한 유사시 사이버 군사지원 수행
- 새로운 안보 위협에 대한 대응전략을 논할 수 있는 서울안보대화(SDD)와 같은 협의체 지속 발전

(기타) 국방 사이버 분야의 국제협력을 위한 전문 수행조직인 「국방 사이버협력단」(가칭)을 국방부 사이버작전사령부 예하에 신설

□ 결 론

- 본고에서는 현존하는 사이버위협을 평가하고 국제 사이버안보 환경과 동향(주요국 정책/전략)을 검토하여 국방 차원의 사이버 국제협력에 대한 정책적 지향점을 제시
- 사이버 대응 능력 강화 및 사이버 역지력을 확보하기 위한 미국 등 우방국들의 사이버 전력을 활용하는 사이버 군사협력 활동과 비우호적인 국가들과의 갈등 최소화 및 확산을 예방하기 위한 장치로서의 군사적 사이버 신뢰 구축 활동 병행 필요
- 이런 점에서 사이버 분야에서 군사적인 유대 강화와 교류 협력 확대, 군사적 역량 강화 및 외국의 군사적 지원을 확보할 수 있는 방안을 강구하여 제안
- 제안한 방안은 국방 여건을 고려하여 즉시 추진 또는 장기과제로 구분하여 충분한 검토와 준비를 거쳐 단계적으로 추진 필요