https://doi.org/10.33778/kcsa.2021.21.4.003

국방 디지털 전환에 따른 사이버역량 강화 방안 연구

김 인 중* , 이 수 진**

요 약

인공지능(AI), 클라우드, 사물인터넷(IoT), 빅데이터, 모바일 등 다양한 신기술들이 유기적으로 연동되어 디지털 전환 시대를 만들어가면서, 그에 대한 역기능으로 사이버보안에 대한 문제도 함께 대두되었다. 기술의 발전으로 인하여 물리적 환경이 그대로 사이버공간으로 옮겨가면서 새로운 현안으로 떠오른 것이다. 사이버공간은 물리적 공간과 달리 경계가 명확하지 않기 때문에, 물리적 공간보다 더 많은 부작용과 위협이 발생한다. 이렇듯 국방에도 디지털 전환을 추진하면서 사이버안보 측면에서의 접근은 이러한 시대적 흐름과 기술의 속성을 이해하고 준비해야 함에도 기존의 전통적 관습과 행동 방식으로 인하여 전환에 어려움을 겪고 있다. 이에 본 연구에서는 국방 디지털 전환에 따른 기술 적용 방향을 살펴보고, 사이버안보 관점에서 어떻게 대응해야 할지를 분석해보고자 한다.

A study on Strengthening Cyber Capabilities According to the Digital Transformation in the Defense Sector

InJung Kim*, Soojin Lee**

ABSTRACT

As new technologies such as artificial intelligence (AI), cloud, Internet of Things (IoT), big data, and mobile become organically integrated, a new era of digital transformation is emerging. As a result of this digital transformation, cybersecurity issues have surfaced as a negative side effect. Cyberspace, unlike physical space, has no clear limits, which leads to additional side effects and hazards. While promoting digital transformation in defense, conventional customs and behavioral approaches make it difficult to alter the cybersecurity strategy, even if it is vital to comprehend and prepare the attributes associated with time and technology trends. As a result, in this study, we will look at the direction of technology application in the defense as a result of digital transformation and analyze how to correlate from the standpoint of cybersecurity.

Key words : Digital Transfomation, Cyber Capabilities, Cybersecurity, Cyber Conflict, AI

접수일(2021년 09월 29일), 수정일(2021년 10월 17일), 게재확정일 (2021년 10월 22일)

* 국방대학교 안보과정

** 국방대학교 국방과학학과(교신저자)

1. 서 론

펜데믹 이후 지속하는 불확실성과 빠르게 변화하는 기술 환경에 적응하기 위하여 인공지능(AI), 클라우드, 사물인터넷(IoT), 빅데이터, 모바일 등 여러 새로운 기술들이 유기적으로 연동하면서 디지털 전환이 화두로 떠오르고 있다[1]. 특히, 비대면 시대를 맞이하여 최적화된 디지털 환경을 구축하여 시간과 공간의 제약을 극복하고, 모바일 기술을 이용하여 몇 번의 클릭으로 업무를 간단하게 해결할 수 있는 서비스와 디지털 도구, 그리고 이에 걸맞은 운용 환경이 제공되고 있다. 실제로 불가능하게만 여겨졌던 재택근무와 온라인 화상회의 등 사이버공간에서의 업무가 현실화하고 일상화되면서 이제는 이러한 환경에 익숙해지면서 더는 비대면 업무가 비효율적이지 않으며, 시간과 비용을 줄여 생산성을 높일 수 있다는 판단으로 전 분야에 걸쳐 디지털 전환이 급속하게 이루어지고 있다.

한편, 이러한 디지털 전환이 이루어지면서 그에 대한 역기능으로 사이버보안에 대한 문제도 함께 대두되었다[2]. 기술의 발전으로 인하여 물리적 환경이 그대로 사이버공간으로 옮겨가면서 새로운 현안으로 떠오른 것이다. 사이버공간은 물리적 공간과 달리 경계가 명확하지 않기 때문에, 물리적 공간보다 더 많은 부작용이 발생하고 있다[3]. 국가와 기업이 관리 운영하는 대부분의 기반시설이 디지털화되면서, 기반시설을 마비시키고 경제적 손실을 초래하기 위한 전문 사이버 공격이 등장하기 시작한 것이다. 이러한 사이버테러가 국가기관 또는 국가기관에서 지원하는 조직에서 테러를 일으키는 경우 국제적, 국가적으로 커다란 파장을 낳게 된다[4].

일명 사이버 충돌(Cyber Conflict)이라 일컬어지며, 최근 사이버공간에서 빈번하게 발생하고 있다. 사이버 충돌은 3가지 범주로 구분하는데, 국가 간 영역으로 전쟁법과 같은 국제법에 적용되며 유엔과 같은 전통 국제기구에서 다룬다. 둘째는 정부 간 영역인데 외교적 측면에서 적용되며 사이버 공격이 지역적, 부분적으로 이루어질 때 논의된다. 세 번째는 민간영역으로 민간, 기업 측면에서 적용되며, 사이버 범죄나 사생활 침해, 개인정보보호 측면에서 다루어진다. 하지만 최근에는 이러한 영역의 경계가 모호해짐에 따라, 민간영역에서의 충돌도 국가나 정부 영역에서도 논의되고 있다[5].

이렇듯 디지털 전환 시대를 맞이하여 사이버안보 측면에서의 접근은 이러한 시대적 흐름과 기술의 속성을 이해하고 준비해야 함에도 기존의 전통적 관습과 행동 방식으로 인하여 어려움을 겪게 된다. 특히, 군에서 디지털 전환을 수행하는 경우 사이버안보라는 특수성을 고려해야 한다. 따라서, 본 연구에서는 디지털 전환에 따른 기술 진화 방향을 살펴보고, 사이버역량을 어떻게 향상할 것인지를 제안한다.

2. 개념 정립

2.1 디지털 전환

인공지능, 빅데이터, 클라우드, 사물인터넷, 모바일 등 디지털 전환기술은 인류가 개발한 최고의 발명품이다. 과거에도 관련된 많은 연구가 진행되었지만, 메모리, 속도, 연산 처리 등 자원의 성능이 효율적이지 않아 인간처럼 사물을 인식하고 판단할 수 있을 만큼 고도의 알고리즘을 구현할 수 없었다. 하지만 반도체 기술이 발전하면서 메모리 저장 능력은 갈수록 증가하고, 원격 실시간으로 처리하는데 지연시간을 고려하지 않아도 될 정도로 전송과 처리 속도도 빨라졌다. 특히 새로운 알고리즘을 이용하여 컴퓨터도 학습하고 이를 기반으로 새로운 지식을 만드는 것이 가능해졌다. 또한, 수많은 데이터를 모을 수 있는 클라우드 기술과 이를 분석하고 추출할 수 있는 빅데이터 기술, 학습을 통해 사람이 원하는 정보를 제공하는 인공지능 기술, 사물과 사물 간의 정보를 교환하는 사물인터넷 기술에 더해서 모바일·5G 무선통신기술 등이 결합하면서 디지털 전환은 성공적으로 진행되고 있다.

군사 분야에서도 디지털 기술이 적극적으로 활용되고 있다[6]. 대표적으로 전투기, 드론과 로봇과 같은 이동체에 대한 성능이 향상되고 있다. 지형, 지물 등을 스스로 판단하여 우회로를 확보하거나, 이전 상황과 비교하여 위험 판단을 내릴 수 있다. 또한, 위험지역에 대한 순찰과 장애물을 파악하는 데 투입되기도 한다. 전장을 감시하고 파악할 수 있는 C4ISR과 같은 전략, 전술 지휘체계에서도 뛰어난 성능을 보장한다. 척후병이 주력부대 전방에서 적의 동태를 살피고 적 진영을

교란하거나 수색대가 매복 또는 지형정찰을 하는 임무를 대신하여, 지하 참호 안에서 모니터를 바라보며, 키보드와 조이스틱만으로도 로봇과 드론을 원격으로 작동시키기만 해도 만족할 만한 성과를 창출한다. 특히, 디지털 기기는 사람을 대신해 위험지역에 투입되면서 인명 피해를 줄일 수 있을 뿐만 아니라 자연환경에 구애받지 않으므로 극한 환경 속에서도 자율적으로 임무를 차질 없이 진행할 수 있게 되었다.

2.2 사이버 충돌

인터넷이 발전하기 이전에, 미국, 중국, 일본, 러시아 등 주요국들은 신호 수집, 정찰 등을 통해 각종 정보를 수집하였으나, 암호통신 체계가 고도화되고 난독화되면서 정보 활동에 어려움을 겪게 되었다. 이러한 상황에서 사이버공간은 정보를 수집하거나 상대방을 교란하는데 좋은 수단이 되었다[7]. 이제는 단순 메일이나 영상을 전송하는 수단을 넘어, 무기체계와 연동하여 실시간으로 군사 작전을 수행할 수 있는 환경이 되었다. 실제로 디지털 시스템은 전력, 가스, 철도, 항만 등 각종 기반시설과 연동되기 시작하면서 디지털 기기의 의존도가 높아짐에 따라 기반시설 장애 및 중단이 해당 국가의 사회적 혼란과 공포, 경제적 손실에 크게 작용한다는 점도 인식하게 되었다. 결국, 포괄적 안보 측면에서 사이버안보는 새로운 핵심 이슈로 등장하게 되었다[8]. 그러나 전통적인 국가 간의 전쟁이나 분쟁과 달리 사이버공간에서 발생하는 사이버 충돌을 이해하고 분석하는 것은 매우 생소하다. 현재 사이버공간에서 벌어지는 사이버 충돌의 원인과 대응을 위하여 기술적으로 충분히 파악해야 하며, 그 속성을 들여다볼 수 있어야 한다. 즉, 사이버 충돌에 따른 피해와 확산을 예측하고, 대응할 수 있는 기술적 역량을 동시에 확보해야 한다. 또한, 사이버 충돌을 초래하는 상대국가 또는 집단에 대해서 사이버 공격을 단념시키거나 억제하고 무력화시켜야 한다. 하지만 사이버 충돌은 전통적 전쟁과 달리, 정보 절취와 사회 혼란을 주목적으로 하면서, 은밀하게 진행되기 때문에 그 의도를 파악하여 적시에 차단하는 데 많은 어려움이 있는 것이 사실이다. 또한, 사이버 충돌의 주체가 국가인지, 국가가 지원하는 조직이 수행하는지, 범죄를 저지르는 해커 집단이 수행하는지를 파악하기도 쉽지 않다.

국가 주도로 이루어진 대표적인 사이버 충돌은 2007년에 발생한 에스토니아 사건을 들 수 있다. 국민의 절반 이상이 인터넷 뱅킹을 이용하던 에스토니아는 사이버 공격으로 인해 3주간 큰 사회적 혼란과 함께 수천만 달러에 달하는 금전적 피해를 보았다. 이처럼 사이버 공격은 사이버 혼란과 물리적 피해를 동반한 치명적인 행동이라는 점에서 기존의 작전개념 자체를 뒤바꾸고 있다. 배후에 러시아로 의심되는 사이버 조직이 개입되었다는 의심을 받고 있으나, 사이버 공격의 주체를 규명하고 증거를 확보하기가 상당히 어렵다는 점에서 앞으로 물리적 충돌을 대신해서 사이버 충돌이 일어날 가능성이 상당히 크다. 실제로 우크라이나 갈등, 이라크와 시리아 사건, 이란의 스턱스넷 사건, 미국의 소니 해킹 사건, 북한의 방글라데시 중앙은행 해킹[9], 워너크라이 랜섬웨어 공격 이외에 러시아의 미국 대통령선거 개입, 솔라윈즈 해킹, 콜로니얼 파이프라인 랜섬웨어 감염, 마이크로소프트 공급망 해킹 등 크고 작은 사이버 충돌이 곳곳에서 지속적으로 발생하고 있다. 비슷한 시기 한국도 북한으로부터 대규모 사이버 공격을 당했다. 2009년 7.7 사이버테러, 2011년 3.4 사이버테러와 농협 해킹 사건, 2012년 7.7 사이버테러, 2014년 12월 한국수력원자력 해킹 등의 피해가 발생하였다[10]. 2021년 6월 21일에는 한국원자력연구원 직원의 이메일 주소, 개인 휴대전화 번호, 사내 아이디·비밀번호가 포함된 계정정보가 북한에 의해 해킹당한 것으로 확인되었다.

이러한 사이버 공격에 대한 경험과 인식이 부족하다 보니, 사이버 충돌도 물리적 환경과 동일 선상에서 접근하게 된다. 즉, 사이버공간에서 발생하는 각종 사안도 물리적 환경에 처한 상황에 따른 경험을 바탕으로 이해하고 적용하게 된다. 그러나 앞으로는 사이버 충돌에 대한 폭넓은 이해와 사고 전환, 그리고 환경 변화를 인정하고 전략과 전술, 정책과 제도, 그리고 각종 교리를 새롭게 재정립해야 한다.

2.3 사이버 역량(Cyber Capability)

디지털 환경으로 전환되면서, 하드웨어, 소프트웨어의 지속적인 발전으로 사이버공간은 점차 확대되고 있다. 디지털 기술은 인류에게 많은 부가 가치를 제공하고 있지만, 물리적 환경에 처해 있는 각종 범죄와

테러, 그리고 사이버 무기로 이용되기도 한다. 실제로 사이버 무기는 여러 가지 관점으로 들여다볼 수 있다. 바이러스, 웜과 같은 악성코드이기도 하고, 더 넓은 의미로 전자전에 사용되는 전파 교란이 포함되기도 한다. 일부에서는 드론이나 로봇도 범주에 포함한다. 특히, 군 체계에서 사용되는 전장 환경을 시각화해 주는 감시정찰체계도 해당한다. 이러한 사이버 무기는 비살상 무기의 범주에 포함하기도 한다.

사이버 무기는 총, 칼, 대포와 같은 물리적 무기와 달리 하나의 객체, 품목으로 정의될 수 없다. 사이버 무기는 하드웨어와 소프트웨어로 구성되므로 국가의 디지털 역량, 정책, 조직, 인력, 교육·훈련 등 많은 요소가 유기적으로 결합하여야 능력을 발휘할 수 있다. 그러다 보니 현대는 사이버 무기라는 한정된 용어를 사용하기보다 사이버역량이라고 지칭한다.

2.4 '능동'적인 사이버 방어의 한계

사이버 충돌에도 국제 사회가 합의된 규칙을 마련하는 것이 필수적이다. 지금까지 국제 사회가 핵확산 금지조약을 통해 국제적으로 대규모 살상 무기를 규제해 온 것과 마찬가지로, 사이버역량도 함께 해결해야 한다. 사이버역량에 대한 국제적 합의는 디지털 전환이 급속도로 진화하면서 더욱 필요하다. 특히, 사이버 무기가 비대칭 무기로 주목받으면서 이를 활용하려는 시도가 늘고 있다. 따라서 새로운 국제 규범을 조속히 마련하여 국제적인 동의를 얻어야 한다. 실제로 가장 우려되는 부분은 사이버 무기가 어느 수준까지 개발되었고 그 파괴력이 얼마나 될지 아무도 모른다는 점이다. 사이버 기술도 핵무기와 마찬가지로 "억지력, 피해제한, 군비 통제, 비확산"을 통해 관리되어야 한다. 그렇지 않으면 앞으로 사이버 공격을 당했을 때, 손실비용을 감당하기 불가능한 상황에 이를 수도 있다.

그러나 사이버 충돌이 발생하는 경우 심각한 사태가 벌어지지 않도록 미리 방지할 수 있는 역량을 갖추기는 쉽지 않다. 암호화, 방화벽, 인증 등과 같은 수동적 방어는 상대방에게 위협을 주지 않는다. 일부 국가에서 수행 중인 '능동'적인 사이버 방어는 국제적 공감을 확보하고 규범으로 정립되어야 하지만 아직 규범화가 되어 있지 않다. 이는 국가 주권과 관련한 민감한 사안이며, 국제관계에서 외교적 마찰을 겪을 수 있기 때문이다. 특히, 능동적 사이버 방어를 수행하는 과정에서 다른 국가의 기반시설에 대해 심각한 경제적 피해를 주거나 국가의 정보시스템을 구성하는 컴퓨터와 네트워크에 대한 중단/마비를 일으키는 경우 외교적, 경제적, 형사적 처벌을 받을 수 있다.

예를 들어, 미국이 사이버 공격을 주도하거나 지원하는 국가를 대상으로 군사적인 대응을 할 수 있다고 선언했지만, 이러한 군사적인 대응은 물리적 전쟁을 내포하기보다 국경 봉쇄를 통한 경제 제재, 외교 단절, 제한적 무력사용 등으로 해석된다. 이러한 판단은 능동적 사이버 방어가 법적, 윤리적 문제를 내포하기 때문이다. 능동적 사이버 방어는 국가 또는 군사적 시설을 대상으로 수행하는 것이 아닌 기업과 민간 시설에 대한 공격을 주로 수행하기 때문이다. 실제로 각종 정보시스템과 기반시설들은 국가보다 민간 시설로 운영 관리되고 있다. 그러므로 이러한 시설을 대상으로 공격하는 것은 법적 또는 윤리적인 부담으로 작용한다.

3. 디지털 전환과 사이버보안 기술

3.1 디지털 전환에 따른 고려사항

디지털 전환기술은 인공지능, 사물인터넷, 클라우드, 모바일(5G) 이외에 최근 가상현실을 포함한 메타버스[11], 디지털 트윈[12], CPS[13] 등이 결합한 스마트시티, 스마트 공장 등 다양한 분야에서 광범위하게 적용되고 있다. 군에서도 정찰, 감시, 통제, 명령 등 지휘체계에 적용되고 원격으로 조작이 가능한 드론과 로봇, 그리고 타격체계에도 도입이 추진되고 있다.

디지털 기술을 활용하기 위해서는 여러 가지 제한사항과 역기능을 고려하여야 한다. 먼저 많은 데이터를 확보해야 한다. 그리고 수집한 데이터를 분류하고 식별하고 정형화 처리를 한 후 빅데이터로 구축해야 한다. 많은 데이터를 확보하지 않으면 디지털 시스템이 학습하는 데 어려움이 발생할 수 있을 뿐만 아니라 통계적으로 신뢰도를 높일 수 없다. 이는 군 특성상 극한 환경에서 다루어지는 시스템이기에 자칫 오류가 나거나 비정형 데이터 입력으로 인하여 오판을 할 수 있는 결과를 제공할 수 있기 때문이다.

둘째, 디지털 시스템 스스로 문제를 해결하기 위해서는 신뢰성 있는 센서로부터 정보를 수집할 수 있도록 해야 한다. 일반적으로 센서에서 입력된 정보들로부터 상황을 파악하고 이를 토대로 작전을 수행하게 되는데, 센서와의 유기적인 결합과 통신 상황에서 안전성과 보안성이 확보되지 않는다면 군 체계의 운용에 제약을 받게 된다.

세 번째로, 향후 디지털 시스템이 대량 생산되고 가격이 저렴해짐에 따라 민간 제품이 군에 도입될 것이다. 만일 신뢰성이 검증되지 않은 디지털 시스템을 적용하는 경우 피아식별이 어려워질 수 있다. 즉, 상용제품을 전투에 활용하게 되면, 아군 제품인지 적군 제품인지 파악하는 데 많은 어려움이 발생하게 된다. 디지털 시스템은 소프트웨어로 구성되어 있어 적도 이를 역이용할 수 있다. 예를 들어, 전파방해나 스푸핑(Spoofing)을 통해 디지털 시스템을 탈취하거나 기능을 마비시킬 수 있다. 특히, 디지털 전환 지휘 통제 체계에 대한 사이버 공격이 이루어지는 경우 전장에서 수행 중인 시스템이 제 기능을 발휘하지 못하거나 아군을 오인 공격할 수도 있다.

3.2 사이버보안 기술

디지털 전환에 따라 원천 사이버보안 기술이 바뀌는 것은 아니다. 암호, 인증, 전자서명 등은 필수사항이며, 디지털 포렌식, 보안 관제도 마찬가지이다. 최근 블록체인과 가상화폐로 인하여 랜섬웨어 공격이 지능화·첨단화되면서 이에 대한 대응과 인공지능을 접목한 사이버보안 기술 등이 선보이고 있다[14]. 이외에도 방화벽, IDS, IPS 등과 같은 경계 보안 제품을 비롯하여 안티바이러스, DB 암호화, 내부정보 유출방지 기술이 주종을 이루고 있으며, 이기종 보안 제품의 로그를 관리하는 통합보안 관리 기술도 적용된다.

그러나 이러한 전통적 사이버보안 기술로는 다양한 기술들이 결합한 디지털 전환체계에 유기적으로 연동하는 것이 거의 불가능하다. 특수 목적을 가진 조직이 하나의 표적에 대해 다양한 해킹 기술을 이용하여 지속해서 정보를 수집하고 취약점을 파악하여 이를 바탕으로 손해를 끼치는 공격을 하면 대응은 어려워진다. 따라서 지금부터라도 디지털 전환체계에 적합한 전용 보안 기술이 필요하다. 예를 들어, 중앙집중화된 보안 관리 기술을 바탕으로 잠재적 취약점을 식별하고 제거하는 보안 기술이 필요하다. 또한, 다양한 빅데이터로부터 발생하는 정보를 분석하여, 알려지지 않은 보안 위협을 사전에 예측하고 방어할 수 있는 기술, 공급망을 통해 유입되는 바이러스를 차단할 수 있는 보안 센서와 인텔리전스 관제 기술 등이 국방 디지털 전환체계에 적용되도록 해야 한다. 특히, 무기체계와 연동에 있어 결함을 확인, 제거, 추적할 수 있는 신뢰성 검증 기술에 대한 역량을 확보해야 한다.

4. 국력과 사이버역량 평가

2021년 6월 29일 영국의 국제전략문제연구소(IISS)에서 '국력과 사이버역량 평가' 보고서[15]를 공개하였다. 총 15개국을 대상으로 7가지 평가 기준을 적용하여 해당 국가의 사이버역량이 어느 정도 수준인지를 파악하고 (그림 1)과 같이 순위를 부여하였다.

(그림 1) 국력과 사이버역량 평가

조사 대상 국가들의 전략과 정책들, 그리고 각종 활동을 자세히 조사하고 분석한 후 이를 활용하여 각국을 3개의 범주로 구분하였다. 그 결과 전 분야에 걸쳐 사이버역량을 확보한 나라(Tier 1)로는 미국을 선정하였다. 일부 영역에서 강점이 있는 국가(Tier 2)에는 호주, 캐나다, 중국, 프랑스, 이스라엘, 러시아, 영국이 선정되었다. 그리고 일부 약점을 가지고 있지만, 일부 영역에서는 강점도 있는 국가(Tier 3)로 인도, 인도네시아, 이란, 일본, 말레이시아, 북한, 베트남을 선정하였다. 이 평가에 한국 및 중국의 사이버역량 평가는 제외되었지만, 보고서가 제시하는 방법론과 공개된 정보를 바탕으로 자체적으로 사이버 역량분석을

수행한 결과는 <표 1>에서 보는 바와 같다.

<표 1> 한국과 중국의 사이버 역량분석

항목	한국	중국
사이버안보 전략, 정책	○	○
사이버보안 조직, 통제	○	○
사이버 정보 수집, 분석, 공유	△	○
디지털 환경 수준	○	△
사이버보안 환경, 대응 능력	○	△
국제협력	△	△
공세적 사이버역량	?	○

한국은 2019년 4월 '국가사이버안보전략'을 마련하고, 2020년 12월 국가정보원법을 개정하여 사이버에 대한 임무를 명확하게 하였으며, 2004년 2월부터 국가사이버안전센터를 운영하여 사이버안보에 대한 임무를 수행하고 있다. 각 정부 부처는 사이버안전 전담조직을 운영하면서 보안관제를 통해 위협을 사전에 차단하는 데 주력하고 있다.

한국의 디지털 환경은 세계 최고 수준이며, 사이버보안 여건도 매우 양호하다. 그러나 사이버공간에 대한 위협 정보를 신속하게 수집하고, 분석하며, 유기적으로 협력하여 공동 대응을 수행할 수 있는 환경이 진행 중에 있다. 또한, 국제협력에서 주도권 행사를 할 수 있는 전문가가 필요하며 사이버 충돌에 따른 중재 역할을 수행할 수 있는 역량도 요구된다. 공세적 사이버역량 부분에 대해서는 공개된 부분이 없으므로 제외한다.

중국은 정부 주도의 전략과 조직, 통제가 일사불란하게 이루어지고 있고[16], 사이버 전사를 육성하면서 사이버공간에서 무차별적으로 사이버 정보 수집을 수행하고 있다. 현재 중국의 디지털 환경은 일부 지역과 분야만 발전되어 있지만, 앞으로는 전 분야에 걸쳐 수준이 향상될 것으로 예상한다. 국제협력에서는 상하이협력기구, 아세안지역안보포럼, 유엔 GGE 등을 통해 러시아 등과 협력해 나가고 있기는 하지만 긴밀하고 실질적인 협력관계를 유지한다고 보기는 어렵다.

항목별로 사이버역량을 추정해 보면, 한국과 중국은 미국처럼 사이버역량이 최우수 등급에 자리매김하지는 못한 것으로 판단된다. 이는 여러 분야에서 아직 미진한 부분이 있고 여러 보완책을 마련하고 실행해 나가야 하기 때문이다. 다만, 한국과 중국은 지속해서 미진한 부분을 보완하고 역량을 넓혀갈 것으로 예상함으로, 몇 년 이내에 Tier 1 국가로 자리매김할 것으로 판단된다. 이에 분석 결과를 바탕으로 미진한 부분인 국제협력을 포함하여, 우리의 사이버역량을 강화할 방안을 제시한다.

5. 사이버역량 강화 방안

5.1 디지털 전환에 따른 사이버보안 능력 향상

5.1.1 디지털 전환에 맞춘 사이버안보 전략 추진

세계 각국은 디지털 전환에 따른 위험을 줄이고자 사이버안보를 국가 안보 측면에서 다루고 있다. 바이든 미국 대통령은 취임하자마자 '사이버안보 증진' 행정 명령을 내렸다[17]. 이 행정 명령은 공공 부문, 민간 부문, 그리고 궁극적으로 미국 국민의 안전과 사생활을 위협하는 점점 더 정교하고 지속적인 악성 사이버 공격에 맞서 안보를 위협하는 활동을 추적하고 맞서고 식별하며, 정부가 민간 부문과 파트너 협력을 강화하기 위한 노력을 담고 있다. 클라우드 서비스 및 기타 사이버 인프라의 보안 업그레이드를 추진하며 다중 인증도 의무화했다.

이러한 미국의 새로운 국가 안보에 대한 전략과 정책을 참고하여, 한국도 디지털 전환이 전 분야에 걸쳐 보편화하기에 앞서 국가 안보 측면에서 사이버안보 전략을 마련하고 이에 대비해야 할 것이다. 한국군도 기존의 전통적 작전개념을 탈피하여 디지털 전환에 따른 사이버역량을 강화하기 위한 전략을 마련하고 추진해야 한다. 디지털 기기의 취약점이 적으로부터 노출되거나 공격의 대상이 되지 않도록, 신뢰성 있고 강인하며, 생존 가능성을 보장할 수 있는 대책을 담아야 한다. 이를 위해서 전주기 선순환 구조의 체계를 마련하고 이를 관리하고 지원하며 상시 운영할 수 있도록 해야 한다. 또한, 디지털 전환 전담부서를 신설하여 인력을 배정하고, 각종 체계 운영 계획을 포괄하는 '국방사이버안보전략'을 수립한 후, 이를 바탕으로 구체적인 실행 방안을 마련해야 한다.

5.1.2 전략적 조직 구성

미 바이든 정부는 사이버안보의 중요성을 인식하고, 대통령이 취임하자마자 백악관 내 국가 사이버 실(the Office the National Cyber Director)을 신설하고 신기술과 사이버안보에 대해 대통령을 보좌하는 최고위 정책결정자를 선임하였다[18]. 아울러 연방 정부의 사이버보안을 총괄 관리하는 임무를 국토안보부 산하 사이버보안 및 인프라보안국(CISA)에 주었다. 영국도 국가안보를 위협하는 적대적인 테러리스트와 범죄자를 대상으로 사이버 작전을 수행하는 정보통신본부(GCHQ) 산하 '국가 사이버안보센터(NCSC)'와 더불어, 새로운 '국가 사이버 포스(NCF: National Cyber Force)' 조직을 설립하였다. 신설된 NCF는 영국의 사이버역량을 혁신적으로 변화시킬 것으로 예상한다.

한국군도 미국 바이든 정부가 출범하면서 신설한 조직과 영국 NCF 조직의 임무와 역할을 면밀하게 검토하여 사이버 임무 수행 및 역량을 강화하는 데 반영해야 할 것이다.

5.1.3 기반시설에 대한 대응 역량 강화

디지털 전환에 있어 가장 파급력이 강한 분야는 에너지 분야이다. 특히 전력 분야의 경우에는 경제, 산업 등에 밀접한 영향을 미치게 된다. 전력 대부분은 원자력, 화력 등 발전소에서 생산되며, 발전소에서 생산된 전기를 변전소로 송전하고, 이를 가정이나 공장 등 필요한 장소로 나누어주는 배전 과정을 진행한다. 이 과정에서 전력 수요를 예측하고 그에 맞춘 공급이 이루어지는데 최근에는 이러한 일련의 과정이 디지털로 전환되면서 좀 더 실질적인 예측과 제어가 가능해졌다.

그러나 전력 수요를 잘못 예측하여 전력 불안이 발생하면 대규모 정전을 겪을 수 있다. 이는 비단 전력 분야에만 국한된 문제는 아니다. 항공, 교통, 상하수도, 가스 등도 전력과 마찬가지로 공급과 수요에 대한 예측이 잘못될 때는 심각한 체증과 지연, 심지어는 해당 기반시설의 중단과 마비까지 발생할 수 있다. 따라서 이에 대한 예방과 관제, 그리고 비상시 복구 및 대응을 위한 대책을 마련하고 만만의 준비를 해야 한다.

한국군은 기반시설 관리·운영기관에서 지원을 요청하는 경우 참여하여 복구 및 대응을 위해 함께 노력해야 한다. 또한, 디지털 전환에 따른 군 운영 기반시설의 현대화 계획 내에 사이버보안에 대한 역할과 임무를 명확하게 반영하여 사이버 공격으로부터 생존 가능성과 회복력을 강화해 나갈 수 있도록 해야 한다.

5.1.4 사이버 위기대응 협력체계 구축

일부 사이버보안 전문가들은 디지털 전환체계에 대한 해킹, 바이러스 등 사이버 공격에 대한 우려를 표명하였다. 실제로 디지털 전환체계 내에 사이버 공격이 발생하면 사회적 피해는 재난 수준 이상으로 발생할 수 있다. 이에 따라 디지털 전환체계에 대한 자동화, 원격 제어, 온라인 관제 등을 수행하기 위해서는 각종 보안 대책이 선결되어야 하며, 취약점 분석 및 위험관리가 철저히 수행되어야 한다. 아울러 정부 주도하에 사이버보안에 대한 신뢰성을 향상할 수 있는 노력을 수행해야 하며, 주요 사이버 자산에 대한 보호계획을 수립하고 군·산·학·연 간 상호 표준을 준수해야 한다. 또한, 사이버 공격 때문에 체계의 중단 및 손실이 발생하는 것에 대비해 사전 방지 및 예방할 수 있는 제도와 규범을 마련해야 한다.

디지털 전환체계에 대한 사이버 공격은 기존 IT 보안의 시각에서 바라보면 해결할 수 없다. 군이 먼저 이러한 심각성을 인식하고, 위기 상황을 사전에 차단하고, 바이러스에 감염되더라도 숨기지 말고 당당하게 적극적으로 대처할 수 있도록 정보공유를 통해 상황을 공동 대처할 수 있는 환경과 대책을 조속히 마련해야 한다.

5.1.5 연구개발 역량 강화

앞으로의 미래는 디지털 전환을 누가 더 빨리 효율적으로 수행하며 안전하고 견고하게 구축하느냐에 성패가 달려있다. 그러나 디지털 전환의 가장 큰 걸림돌은 호환성 및 연동성 문제이다. 군 특성상 군에서 사용하는 각종 체계는 윈도, 애플과 같은 상용 운영체제를 사용하지 않고 각종 무기의 특성에 맞는 별도의 운영체제를 사용한다. 따라서 이러한 체계들은 디지털 전환이 매우 더딜 수밖에 없으며, 동시에 디지털 전환 과정에서 다양한 보안 위협에 노출되기도 한다.

군에서 운용하는 각종 체계가 이중 삼중으로 격리

되어 철통같이 관제가 된다고 할지라도 사이버 공격에 대해서 절대적으로 안전하다고 장담할 수 없다. 적이 언제 어떻게 체계의 결함을 파악하여 사이버 공격을 감행할지 알 수 없다. 굳이 사이버 공격이 아닐지라도 잘못된 정보를 입력하여 전혀 다른 결과가 생성되도록 유도할 수도 있다. 따라서 국방 분야의 특수환경에 적합한 디지털 전환체계를 구축해야 한다. 이를 위해 민간영역보다 더욱 강한 신뢰성을 보장할 수 있는 사이버보안 연구개발이 요구되며, 충분히 검증된 장비와 체계를 획득하여 운영되도록 해야 한다.

5.1.6 위험분석과 위험관리 수행

매년 <세계 위험보고서(The Global Risks Report)>[19]는 인류가 마주할 가장 큰 위협을 단기, 중기, 장기로 나누어 선정하고 있으며, 사이버보안 관련 사항이 매년 상위권에 포진되고 있다. 2021년도에도 테러, 환경문제보다 사이버보안 실패와 디지털 불평등을 각각 4위와 5위로 선정하였다. 가능성 측면과 영향력 측면을 종합적으로 분석한 결과에서도 사이버보안은 상위권에 포진되어 있다. 특히, 5년 이내 예측되는 위험으로 사이버보안 실패에 따른 IT 기반시설의 붕괴가 공동 1위로 선정되었다. 다른 하나는 코로나 19로 촉발된 과도한 재정 지출 및 저금리로 인한 자산 거품 붕괴라는 점을 고려하면 사이버보안 실패가 인류에게 얼마나 위협이 되는 사안인지를 실감할 수 있다. 더욱 우려스러운 사실은 앞으로 핵, 미사일 등 대규모 살상 무기와 견주어 기술 발전에 따른 역기능도 10년 이내 우리에게 당면 위협으로 다가올 것으로 경고하고 있다는 점이다.

이렇듯 새롭게 대두되는 사이버 위협을 예방하고, 대처할 수 있는 역량으로는 상시적 위험분석과 위험관리 활동을 꼽을 수 있다. 물리적 공간의 바이러스와 달리 사이버공간의 바이러스는 시간적 여유를 주거나 공간적 제한 없이 우리의 주변에 한순간에 소리소문 없이 다가올 수 있다. 따라서 위험분석과 위험관리를 통해 취약점을 제거하고, 위협을 차단해야 하며, 대응에서는 비용 대비 효과보다는 국가안보 측면에서 보호 대책을 마련해야 한다.

5.1.7 디지털 기기의 체계적 군수 지원책 마련

이제는 물리적 전쟁을 수행하는 경우 사이버 작전 요소를 반영하지 않고서는 승리를 장담할 수 없다. 그런데 소프트웨어는 수명 주기가 짧으며 수시로 운영체제 업그레이드 및 보안 패치를 수행해야 한다. 또한, 하드웨어도 성능을 보장하기 위해 용량을 증설하거나 시스템을 보강해야 한다. 그러다 보니 제품을 유지하고 관리하는 데 많은 어려움이 따른다. 실제로 기존 체계는 정비 및 관리 측면에서 한번 획득한 이후 보급 및 운영에 큰 어려움이 없지만, 디지털 전환 기기의 경우에는 도입에서 폐기까지 항상 모니터링하고 관리해야 하며, 수시로 부속품을 변경하거나 소프트웨어를 개량해야 한다. 이러한 비용은 초기 획득비용과 별반 차이가 없거나 오히려 더 많은 부담으로 작용할 수도 있다.

따라서 디지털 전환체계에 맞는 군수 지원 대책을 마련하여 시행하여야 한다. 필요하다면 상용제품을 적기에 확보하여 사용하는 것도 고려해야 한다. 상용 디지털 전환 제품은 대량으로 확보할 수 있고 가격이 저렴하므로 단기간에 운용한 후 폐기할 수 있다. 따라서 디지털 획득 체계의 운영에 대한 새로운 작전개념을 마련해야 하며 그와 동시에 보안 대책도 함께 반영해야 한다.

5.2 국제협력 강화

5.2.1 국제적 사이버안보 전문가 양성

현재 사이버 공격에 대해서는 국제법과 국제 규범이 명확하게 마련되어 있지 않은 상황에서 물리적 환경에서 적용했던 법과 제도를 그대로 적용하고자 시도하고 있다. 그러다 보니 당분간은 사이버공간에 적용할 규범이 정해지지 않은 상태로 갈등과 충돌이 지속할 것으로 예상한다.

따라서 한국은 사이버 공격에 대해 대처하고 법적으로 대응할 수 있는 역량과 환경을 마련해야 한다. 한국이 더 사이버 놀이터로 인식되지 않도록 하기 위해서는 가장 먼저 시급히 해결해야 할 과제가 사이버안보 전문가 양성이다. 국가적 침해 사고가 발생하였을 때, 해커를 정확하게 찾아내 기소하고 처벌하며, 특정 국가의 소행으로 밝혀지면 경제적으로 강력한

제재를 가하거나 배상을 받아낼 수 있는 전문 지식과 역량을 갖춘 전문가가 양성되어야 한다.

5.2.2 국제 규범 및 모범 사례 연구

사이버 충돌이 발생하면 자위권의 범위와 절차, 전투원을 대신하는 디지털 무기에 대한 대응, 사이버 공격에 관한 비례성과 시의성 결정, 사이버 공격의 특징인 은닉성에 대처하기 위한 전문 기술 등 다양한 국제 규범과 모범 사례를 마련해야 한다.

먼저, 군은 디지털 기기를 사이버 무기로 사용하면서, 적절하게 설계되고 사이버 무기가 국제인도법(IHL, international humanitarian law)에 맞는 방식으로 사용될 수 있는지를 검토해야 한다. 둘째, 군이 안전하고 신뢰할 수 있는 지원을 수행하며 사이버 무기를 배치하면서 국제인도법에 맞는 범위 내에서 운영되는지를 알 수 있어야 한다. 셋째, 상대 국가가 사이버 무기를 책임감 있게 설계하고 합법적으로 사용되도록 하는 엄격한 규정과 절차를 갖추도록 상호 협상을 벌일 수 있어야 한다. 마지막으로 사이버 무기에 관한 연구개발은 지속해서 수행하되 비인도적으로 사용되는 사이버 무기에 대해서는 제재나 금지를 할 수 있어야 한다. 이렇듯 디지털 전환체계로 인해 발생하는 사이버 충돌은 물리적 환경과 달리 새롭고 기존 방식과는 상당히 다르다. 따라서 합리적으로 판단되는 많은 모범 사례를 발굴하여 디지털 전환체계에 적합한 국제법, 규범, 그리고 교리를 만들 수 있도록 환경을 마련하고 지원해야 한다.

5.2.3 기술력 확보를 통한 중재자 역할 강화

아무리 보안 대책을 철저히 수행하는 국가라 하더라도 모든 사이버 위협을 적시에 효과적으로 막아내기란 쉽지 않으며, 국제적인 협력을 통한 공동 대응이 필요하다. 그리고 국제협력을 강화해 나가기 위해서는 누군가가 중심이 되어야 하고 중재자 임무를 수행해야만 한다.

중재자로서의 임무를 수행할 수 있는 국가는 이러한 기술력을 확보하고 있으면서 중립적인 나라가 적합할 것이다. 한국은 디지털 전환과 사이버보안 분야에서 강국이며, 다양한 경험과 능력을 바탕으로 다른 국가의 지지를 얻어가면서 국제협력에 대한 규범과 대응 매뉴얼을 만들어가는 데 있어 최적의 국가이다. 따라서 국제 사법재판소나 국제원자력기구의 핵 안전조치 점검팀과 같은 형태의 임무를 수행하는 사이버 안보 협력 기구를 한국에 유치하여 사이버 충돌이 발생하면 상황 파악 및 증거 확보, 재발 방지를 위한 임무를 수행할 수 있도록 해야 한다.

5.2.4 국제 교류의 장 마련

물리적으로 전투병이 상대국에 침투하여 직접 기반시설을 공격하는 행위에 대해서는 엄격하게 국제법을 적용할 수 있다고 할 수 있다. 그러나 해킹, 바이러스뿐만 아니라 드론이나 로봇 등 디지털 기기를 원격조종하여 사이버 공격을 수행하는 것에 대해서는 국제적 수준의 합의가 이루어지고 있지 않다.

특히, UN의 경우 많은 국가가 참여하고 있기는 하지만, 자국의 이익과 관심에 따라 움직이다 보니 합의까지 가는 것은 매우 어렵다. 따라서, 디지털 전환에 관심을 두는 국가끼리 서로 모여 미래 디지털 전환에 따른 안전 사항을 논의할 수 있는 국제 교류의 장이 필요하다. 이 협력의 장을 통해 모범 사례를 개발하고 정보를 교환하면서 다양한 선택지를 만들어 제공하면 그동안 해결되지 못했던 대부분의 기본적인 사항들은 손쉽게 정리될 수 있을 것이다. 그리고 이러한 노력을 통해 증거 확보, 비례성, 즉각성 등 사이버 충돌에서도 물리적 환경과 마찬가지로 적용 가능한 규범이 정해지고 국제 공조를 수행할 수 있는 기구 또는 협의체까지 마련될 것이다. 이를 기반으로 한미연합 또는 NATO 사이버 동맹에도 참여하여 한국군의 위상을 높이는 데 주력해야 한다. 한국이 먼저 참여를 제안하고 협력적 노력을 주도하여 명실상부한 디지털 전환 시대를 이끌어갈 선도국가로 발돋움할 기회를 마련해야 한다.

6. 결 론

정보시스템과 기반시설이 인공지능, 클라우드, 빅데이터, 사물인터넷 등 디지털 기술과 결합하여 첨단화·지능화되면서 편리함과 효율성이 극대화되고 있다. 이에 현재 거의 모든 국가가 디지털 전환을 추진하고

있으며, 국방 분야에서도 무기체계 개발, 획득, 운용 등 전 분야에 걸쳐 디지털 전환 노력을 기울이고 있다. 하지만 이러한 디지털 전환체계는 매우 복잡하고 유기적으로 동작하다 보니 위협과 취약점이 상존한다. 이에 공급망(Supply Chain)을 이용하여 상시 보안 패치나 운영체제 업그레이드를 수행해야 한다. 그런데 적시에 적절한 패치나 업그레이드가 진행되지 않았을 경우, 노출된 취약점을 교묘하게 파고드는 사이버 공격으로 인해 디지털 시스템뿐만 아니라 사회 전반에까지 영향을 끼치게 되어 심각한 경제적 손실과 더불어 인명 피해를 입을 수 있다. 이에 본 연구에서 디지털 전환 시대에 맞춘 사이버역량 강화 방안과 한국군의 대응방안을 제시하였다.

앞으로 디지털 전환은 계속해서 진화하고, 사이버 위협과 취약성 또한 갈수록 증가할 것으로 전망된다. 따라서 효율적인 대응을 위해서 제시한 사이버 역량 강화 방안 이외에도 정보보호 기업 육성 및 글로벌 진출 지원, 보안 관련 표준 평가 제도 마련, 사이버안전 교육·훈련체계 구축 등에도 관심을 기울여야 한다. 아울러 가장 중요한 부분은 군과 산·학·연 모두가 정보공유를 통해 위협을 조기에 막을 수 있는 협업체계를 공고히 해나가는 것이다. 본 연구에서 제시한 디지털 전환에 대비한 사이버역량을 확보한다면, 디지털 전환을 성공적으로 수행한 모범 국가로 인식되면서 우리는 세계 최고의 안전한 국가, 세계 최강의 군대로 자리매김할 것이다.

참고문헌

[1] 김형택, 이승준, '그들은 어떻게 디지털 트랜스포메이션에 성공했나', 월컴퍼니, 2021.7.15.

[2] The National Security Commission on Artificial Intelligence, "Final Report," 2021.3.1.

[3] 김인중, '사이버공간과 사이버안보', 글과 생각, 2013.

[4] 김인중, "빅 데이터 시대의 사이버안보와 인텔리전스의 대응," 2017년 국가정보학회 춘계학술회의, 2017.

[5] 김소정, 김규동, "UN 사이버안보 정부전문가 그룹 논의의 국가안보 정책상 함의," 한국정치정보학회 정치정보연구, 제20권2호, 2017.6.

[6] 한국방위산업진흥회, "정부, 올해 민군기술협력사업에 총 1,772억 원 투자 : 로봇, 드론, 3D 프린팅 등 4차 산업혁명 핵심기술개발 및 국방분야 적용," 국방과 기술, 2020.4.

[7] GEORGE PERKOVICH, ARIEL (ELI) LEVITE, "Conclusions from Understanding Cyber Conflict: 14 Analogies," October 16, 2017.

[8] 장노순. "글로벌 사이버 환경과 한국의 사이버 안보," 2018 국가정보학회 연례학술회의, 2018.

[9] BBC news, "The Lazarus heist: How North Korea almost pulled off a billion-dollar hack," 2021.6.21.

[10] 백상미, "북한의 대남 사이버공격에 대한 국제법적 검토와 이에 대한 한국의 대응전략," 서울국제법연구 제27권, 2020.12.

[11] 윤경로, "메타버스 표준화 동향," 한국통신학회지, 2021.8.

[12] 신규용 외 3명, "디지털 트윈 및 확장현실 기반 미래형 통합전투훈련플랫폼 구축 방안 연구," 한국디지털콘텐츠학회논문지, 2021.4.

[13] 주현식, "4차 산업 시대의 ICT 보안 변화와 CPS 보안 시스템에 관한 연구," 한국디지털콘텐츠학회지, 2018.2.

[14] 김주원, '인공지능 보안 : 인간의 영역을 넘어서', 인포더북, 2021.4.15.

[15] IISS, "Cyber Capabilities and National Power: A Net Assessment," 28th June 2021.

[16] 박민숙 외 1명, "중국의 사이버보안 정책 연구," 대외경제정책연구원 연구자료 제20권, 2020.7.

[17] The White House, "Executive Order on Improving the Nation's Cybersecurity," 2021.5.12.

[18] 오일석, "2021년 바이든 정부의 사이버안보 정책 전망," 국가안보전략연구원 이슈브리프 244호, 2021.2.16.

[19] World Economic Forum, "The Global Risks Report 2021," 2021.1.19.

〔저자소개〕

김 인 중 (InJung Kim)
1990년 2월 충남대학교 학사
1992년 2월 충남대학교 석사
2006년 2월 성균관대학교 박사
2000년~ 현재 한국전자통신연구원 부설연구소 책임연구원
2021년 국방대학교 안보과정 교육파견
email : steganogr@gmail.com

이 수 진 (Soojin Lee)
1992년 3월 육군사관학교 학사
1996년 2월 연세대학교 석사
2006년 2월 한국과학기술원 박사
2006년~현재 국방대학교
국방과학학과 교수
email : cyberkma@gmail.com