IT 환경 변화에 따른 국가 사이버 복원력 제고를 위한 고려사항

최용희[1], 최상훈[2], 박기웅[3†]
[1]세종대학교 SysCore Lab. 박사과정
[2]세종대학교 SysCore Lab. 연구교수
[3]세종대학교 정보보호학과 교수
yonghee409@gmail.com, csh0052@gmail.com, woongbak@sejong.ac.kr

Considerations for Improving National Cyber Resilience According to Changes in IT Environment

Yong-Hee Choi[1], Sang-Hoon Choi[2], Ki-Woong Park[3†]
[1-2]SysCore Lab., Sejong University
[3]Dept. of Computer and Information Security, Sejong University

요 약

디지털화의 가속화는 사이버 공간에 대한 의존도를 크게 증가시키고 있다. 군사, 금융, 의료, 통신 등 주요 인프라는 네트워크를 통해 상호 연결되면서 효율성을 극대화하고 있지만, 동시에 사이버 공간의 중단이 가져오는 영향성에 취약해지는 구조가 형성되어 지고 있다. 대표적으로, 2022년 발발한 러시아-우크라이나 전쟁에서 러시아는 사이버 공간과 물리적 공간을 활용한 공격 수단을 통해 우크라이나의 주요 인프라를 마비시키려는 시도를 하였다. 그러나 우크라이나는 높은 사이버 복원력(Cyber Resilience)을 바탕으로 이러한 공격에 능동적으로 대응할 수 있었고, 인프라 마비를 효과적으로 방어하였다. 이에 따라, 러시아의 일방적인 승리로 끝날 것이라는 초기 예측과 달리, 우크라이나는 물리적 전투뿐만 아니라 사이버 공격 속에서도 지속적으로 저항하며 전쟁을 이어가고 있다. 본 연구에서는 IT 환경 변화에 따른 안보 위협과 이를 극복하기 위한 국가 사이버 복원력 제고를 위한 고려사항을 분석하기 위해 우크라이나-러시아 전쟁에서의 사이버 복원력이 발휘된 사례를 분석하고, 그로부터 도출되는 시사점과 향후 연구 방향을 제시한다.

1. 서론

최근 사이버 위협의 양상은 매우 복잡하고 다변화되고 있다. 랜섬웨어, 피싱, 악성코드 등의 공격은 점차 정교해지고 있으며, 공격 주체 역시 국가 단위의 해커 그룹에서부터 사이버 범죄 조직에 이르기까지 다양하다. 특히 주요 사회 기반 시설에 대한 사이버 공격은 국가 안보뿐만 아니라 사회 전반에 큰 영향을 미칠 수 있다.

2023년 3월, 과학기술정보통신부는 2022년 10월에 발생한 SK C&C 데이터센터 화재 사고 이후, 「디지털 서비스 안정성 강화 방안」을 발표하였다. 디지털 서비스 안정성 강화 방안에서는 네트워크, 데이터센터 장애·재난이 발생할 경우 일상 및 사회·경제로 피해가 빠르게 확산 전파되어 대규모 손실을 야기할 수 있다고 평가하였다 [1]. 이와 같은 평가는 사이버 복원력(Cyber Resilience)에 대한 중요성과 필요성을 뒷받침한다. 더불어 사이버 복원력이 국가 안보와도 무관한 관계가 아님을 시사하는 바이기도 하다.

대표적으로 2022년 발발한 러시아-우크라이나 전쟁에서 러시아는 사이버 공격을 통해 우크라이나의 주요 인프라를 마비시키려는 시도를 하였다. 하지만, 우크라이나는 정교한 사이버 복원력(Cyber Resilience)을 바탕으로 이러한 공격에 능동적으로 대응할 수 있었고, 인프라 마비를 효과적으로 방어하였다. 러시아-우크라이나 전쟁은 사이버 복원력의 중요성을 강조하는 대표적인 사례이다.

따라서, 본 연구는 사이버 복원력과 국가 안보라는 상관관계에 주목하고, 이러한 맥락에서 국가 사이버 복원력을 제고할 수 있는 방안을 살펴보기 위해 현재 마주하고 있는 IT 환경의 변화와 이를 통해 발생할 수 있는 국가 안보 위협을 살펴보고, 향후 국가 사이버 복원력 제고를 위한 고려사항을 도출한다.

논문의 구성은 다음과 같다. 2장에서 IT 환경의 변화에 따른 안보 위협을 살펴보기 위해 관련된 사례를 살펴본다. 3장에서는 우리나라의 디지털 의존성과 안보를 분석하고, 4장에서는 결론 및 향후 연구 방향을 제시한다.

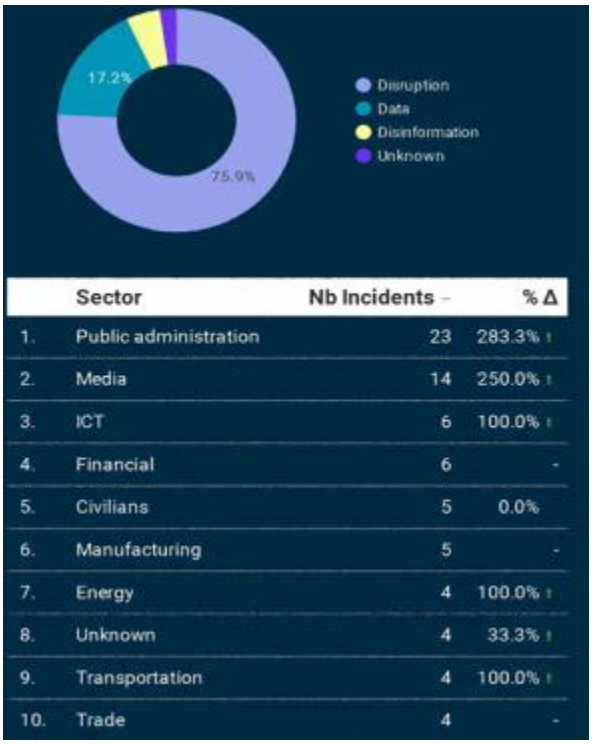
†교신저자: 박기웅 (세종대학교 정보보호학과 교수)
본 논문은 과학기술정보통신부의 재원으로 정보통신기획평가원(IITP)의 정보통신방송기술 국제공동연구(Project No. RS-2022-00165794, 50%), 국방ICT융합연구(Project No. 2022-11220701, 30%), 정보통신방송혁신인재양성사업(Project No. 2021-0-01816, 20%)의 지원을 받아 수행된 연구임.

2. IT 환경의 변화와 안보 위협

불과 십몇년 전만 하더라도 세계 대부분의 IT 환경은 자사의 서비스 운영을 위한 서버를 자체적으로 설치 및 보유하는 온 프레미스(On-Premise) 방식으로 운영하였다.. 하지만, 최근에는 중앙화된 데이터센터를 중심으로 하여 IT 자원을 데이터센터에 위탁하여 운영하거나 클라우드 서비스 제공자(CSP, Cloud Service Provider)로부터 IT 자원을 부분 또는 전반적으로 임대받아서 사용하는 오프 프레미스(Off-Premise) 환경으로 전환되고 있다.

이러한 IT 환경의 변화는 조직의 입장에서 비용 효율성과 관리의 편의성 측면에서 많은 주목을 받고 있다. 그러나 국가 안보적 관점에서 보면, IT 환경의 변화는 중요한 시사점을 제공한다. 이에 따른 국가 안보 위협을 가장 잘 보여주는 대표적인 사례로는 2022년 발발한 러시아-우크라이나 전쟁을 들 수 있다.

'22년 발생한 러시아-우크라이나전(이하 '러-우전')은 러시아의 일방적 승리로 끝날 것이라는 예측이 대다수였다. 하지만, 우크라이나는 러시아의 각종 물리적·사이버 공격 속에서도 오늘날까지 전쟁을 지속하고 있다. 이러한 배경에는 우크라이나의 높은 사이버 복원력이 크게 기여했다고 볼 수 있다. 러-우전에 있어 러시아는 군사적 목적의 달성을 위하여 전시 초 수많은 사이버 공격을 수행하였다. 그림 1과 같이 러시아는 중앙 행정 기관이나 통신, 정보통신 기반에 대한 서비스 운영 중단을 노리거나, 중요 데이터를 타겟으로 한 공격이 주를 이루었다 [2].



	Sector	Nb Incidents	% Δ
1.	Public administration	23	283.3%
2.	Media	14	250.0%
3.	ICT	6	100.0%
4.	Financial	6	-
5.	Civilians	5	0.0%
6.	Manufacturing	5	-
7.	Energy	4	100.0%
8.	Unknown	4	33.3%
9.	Transportation	4	100.0%
10.	Trade	4	-

(그림 1) 러시아의 사이버 공격 동향('22년 3분기 기준)

즉, 러시아는 전장에서의 유리한 고지를 점하기 위하여 일단 정부가 정상적인 국정 운영을 수행하지 못하도록 관련된 인프라를 마비시키는데 집중하였다고 분석할 수 있다. 러시아는 이러한 사이버 공격 외에도 군사적 목적의 달성을 위해 그림 2와 같이 사이버 공격과 동시에 우크라이나의 국가 인프라에 대한 물리적 공격 수단(미사일 등)도 병행하곤 하였다 [3]. 그리고 이러한 공격 중에는 우크라이나 키이우(Kyiv)에 위치한 정부 소유의 데이터센터에 대한 공격도 포함되어 있었다.

(그림 2) 영국, 주간 러-우전 정보 보고서

우크라이나의 디지털 전환 담당 차관인 조지 두빈스키(George Dubinsky)에 따르면, 우크라이나는 정부 소유 데이터센터에 대한 미사일 공격을 받았고, 그로 인해 대부분의 데이터를 잃을 뻔한 위기를 겪었다고 주장하였다[4]. 그러나, 사전에 데이터 센터에서 운용 중인 민감한 데이터를 대부분 해외로 이전하는 데 성공했기 때문에 국정 운영에 필요한 데이터를 소실하지 않아 안정적인 국정 운영이 가능했다고 밝혔다. 이와 같은 사례는 다양한 데이터를 관리하는 데이터센터가 국가 안보 측면에서 주요 표적이 될 수 있음을 보여주며, 이러한 위협에 대비한 전략 수립이 필요함을 시사하고 있다.

3. 우리나라의 디지털 의존성과 안보 상황

러시아-우크라이나 전쟁 사례를 우리나라 상황에 비추어 살펴보면, UN 전자정부 평가를 인용할 때 우크라이나가 46위인 반면, 우리나라는 3위에 올라 있어 43단계나 높은 순위를 기록하고 있다. 이는 우리나라가 우크라이나보다 훨씬 더 높은 사이버 인프라 의존도를 가지고 있음을 보여준다 [5].

더 나아가, 「제3차 클라우드컴퓨팅 기본계획」에서는 행정·공공기관 정보시스템의 클라우드 전환 및 6대 공공분야 주요 시스템 대상 클라우드 기반 혁신을 제시하였다 [6]. 「디지털플랫폼정부 실현계획」 항목에서 분산되어 있는 전 국정 운영 및 관리 업무를 디지털을 기반으로 통합하여 추진하며 이러한 기반 환경으로 클라우드를 이용하겠다고 제시하였다 [7]. 즉, 이러한 정책으로 향후 데이터센터에 대한 의존도가 더욱 높아질 수 있을 것이란 예상을 할 수가 있다.

한편, 우리나라는 클라우드를 기반으로 국가 데이터를 운용할 수 있는 데이터센터의 수는 제한적인 상황이다. 2024년 현재 기준으로 공공기관이 운영하는 클라우드 데이터센터는 국가정보관리원 대구센터 등 일부에 불과하다. 또한, 공공기관이 기반시설을 포함한 모든 서비스를 위탁

운영할 수 있는 인증을 받은 업체는 클라우드 보안인증제(CSAP, Cloud Service Assurance Program)를 기준으로 총 13곳에 불과하다 [8].

즉, 전시상황에 적(敵)의 관점에서는 기존의 분산된 타겟보다 공격해야 할 타겟을 단순화할 수 있어 기존보다 적은 전력으로도 효과적으로 공격을 수행할 수 있다는 것을 시사한다. 결과적으로 우리나라 국정 운영을 위한 정보체계 등이 모두 클라우드 기반으로 이동한 이후, 적(敵)은 데이터가 집중되어 있는 일부 데이터센터만 집중적으로 공격함으로써 우리나라의 국정 운영을 마비시킬 수 있는 것이다. 특히, 우리나라와 휴전 중인 북한 기준, 북한은 러시아와 유사한 작전을 펼칠 수 있을 것이라는 예상이 가능하다. '22년 국방백서에 따르면, 북한군은 기습공격 및 속전속결을 중심으로 하는 군사전략에 기초하여 미사일, 장사정포, 사이버·전자전 등 비대칭 전력을 증강하고 있다고 서술하고 있다 [9].

또한, 이는 국가의 데이터를 저장 관리할 수 있는 데이터센터를 확장하더라도 완전한 해결은 요원할 수 있다. '23년 기준 우리나라에는 총 177개의 데이터센터가 구축되어 있으며, 이 중 약 60% 정도가 서울, 경기 등의 수도권에 위치하여 있다. 그리고, 적의 전력 중 하나인 장사정포의 최대 사거리(200KM)를 고려할 경우에는 그림 3과 같이 강원·충청·경북을 포함한 93%의 데이터센터가 물리적 공격 위험에 노출되어 있다 [10, 11].

(그림 3) 북한 주요 장사정포 사거리

더불어, '23년도 공개된 「국가 정보보안기본지침」에 따르면, 각급 기관의 장은 민간 클라우드컴퓨팅서비스를 이용하고자 할 경우 국내에 위치한 정보시스템(인증서버, 로그 및 백업서버 등)·관리주체에 의해 데이터가 저장·관리되는 서비스의 이용만 허용하고 있다 [12]. 이는 민간 클라우드 우선 정책을 펼치더라도 국내에 위치하고 활성화된 리전(Legion)만 사용할 수 있다는 것을 의미하므로, 우크라이나와 같이 데이터를 해외에 이전하는 것과 같은 물리적인 공격에 의한 데이터센터 파괴에 대응할 수 있는 사이버 복원력을 마련하기 어렵다는 사실을 시사한다.

4. 결론

현대의 디지털화의 가속화는 사이버 공간에 대한 의존도를 크게 증가시키고 있다. 2022년 발발한 러시아-우크라이나 전쟁에서 러시아는 사이버 공격을 통해 우크라이나의 주요 인프라를 마비시키려는 시도를 하였다. 하지만, 우크라이나는 높은 사이버 복원력을 바탕으로 이러한 공격에 능동적으로 대응하였다.

현재 우리나라는 우크라이나보다 정보통신 의존도가 높은 상황이며, 앞으로 그 의존도는 더욱 증가할 것으로 예상된다. 따라서, 우리나라가 여전히 전시 상태에 있다는 점을 고려할 때, 우크라이나에서 발생한 사례를 바탕으로 우리 역시 이에 상응하는 대응책을 사전에 준비할 필요가 있다. 우리나라는 민간 클라우드 우선 정책을 추진하고 있지만, 사실상 국내에 위치한 데이터센터에서만 서비스를 구축하고 운영할 수밖에 없다는 한계점이 있다. 이는 우크라이나와 같은 수준의 사이버 복원력 준비에 한계가 있음을 시사한다. 향후 연구에서는 우리나라의 클라우드 기반 인프라에 대한 한계점을 바탕으로 사이버 복원력을 강화하기 위한 방안 등을 연구 수행할 예정이다.

참고문헌

[1] 과학기술정보통신부, "디지털서비스 안정성 강화 방안 발표", 보도자료, 2023. 3. 30.

[2] CyberPeace Institute, "Cyber Dimensions of the Armed Conflict in Ukrine",Quarterly Analysis Report Q3 July to September 2022, 2022. 12. 16.

[3] UK Defense Intelligence, "Intelligence Report",2022.3.7.

[4] Catherine Stupp, "Uknaine Has Begun Moving Sensitive Data Outside Its Borders, Wall Street Journal, 2022.6.14.

[5] UN, "UN E-Goverment Survey 2022", 2022.

[6] 정보통신전략위원회, "제3차 클라우드컴퓨팅 기본계획", 2021.9

[7] 디지털플랫폼정부위원회, "디지털플랫폼정부 실

현계획”, 2023.4.14.
[8] 한국인터넷진흥원, https://isms.kisa.or.kr
[9] 국방부, 2022년 국방백서, 2023.2.
[10] Colliers, “한국 데이터센터 시장 보고서”, 2023.1.3.
[11] 연합뉴스,
https://www.yna.co.kr/view/GYH20190626000700044
[12] 국가정보원, “국가 정보보안 기본지침”, 2023. 1. 31.