IFANS
주요국제문제분석 2022-19

러시아-우크라이나 전쟁의 사이버전: 평가와 함의

송태은

국립외교원 외교안보연구소

이 글은 국립외교원 외교안보연구소에서 매주 개최되는
주요국제문제분석 세미나에서의 논의를 참고로 하여 저자가 작성한 것입니다.

세미나 일자 **2022. 7. 15.**
발 표 **송태은** 안보통일연구부 조교수
토 론 **전봉근** 국립외교원 안보통일연구부 교수
최기천 외교부 유럽국 유라시아2과 과장
박동휘 육군3사관학교 군사사학과 학과장

발 행 일 **2022년 7월 21일**
발 행 처 **국립외교원 외교안보연구소**
편 집 **김자희 연구원**
디 자 인 **역사공간**
발간등록번호 11-1261021-000001-03

국립외교원 외교안보연구소
(우)06750 서울특별시 서초구 남부순환로 2572
http://www.ifans.go.kr
E-mail: ifans@mofa.go.kr

이 문건은 집필자의 견해를 바탕으로 '열린 외교'의 구현과 외교정책수립을 위한
참고자료로 작성된 것으로서 외교부의 공식입장과는 무관한 것입니다.

IFANS 주요국제문제분석
2022-19

러시아-우크라이나 전쟁의 사이버전: 평가와 함의

CONTENTS

문제제기 01
사이버전의 개념 04
전개 양상과 특징 07
평가 16
정책적 함의 23

1. 문제제기

» 2022년 러시아-우크라이나 전쟁은 사이버전이 현대 전면전(a full-fledged war)에서 실제로 어떻게 전개되고 어떤 비중의 역할을 차지하는지 관찰할 수 있는 보기 드문 역사상 첫 번째 사례임.

2022년 러시아-우크라이나 전쟁은 사이버전이 현대 전면전(a full-fledged war)에서 실제로 어떻게 전개되고 어떤 비중의 역할을 차지하는지 관찰할 수 있는 보기 드문 역사상 첫 번째 사례이며...

- 그동안 국제사회에서는 사이버 공격 행위에 대한 다양한 규범적 논의가 진행되어 왔으나 그러한 논의의 사례가 되었던 대상은 모두 '전면전'에서의 사이버전이 아닌 저강도의 국지전에서의 사이버전이나 물리적 폭력이 동반되지 않은 사이버전에 대한 것이었음.
- 이번 전쟁의 사이버전은 전면전에서 사이버전이 얼마만큼의 파괴력을 발휘하며 전세에 영향을 끼치는지 혹은 그러한 영향력이 어떤 한계를 갖는지 보여주는 사례로서 의미가 있음.

» 이번 러시아-우크라이나 전쟁은 사이버전이 사이버 공간뿐 아니라 육·해·공 및 우주 공간의 물리적 군사활동과 밀접하게 연계되며 사이버 심리전의 경우, 인지공간과도 연결되는 만큼 현대 전쟁에서 핵심적인 역할을 수행하고 있음을 여실히 보여줌.

» 이번 전쟁의 사이버전과 관련하여 가장 빈번하게 제기된 의문은 하이브리드 위협(hybrid threats) 수단으로 활용되며 과거 상당한 파괴력을 보여준 러시아의 사이버 전력이 기존에 알려져 있는 것과 달리 상당히 제한적으로 발휘된 것처럼 보인 것이었음.

» 또한 이번 전쟁의 사이버전이 예상보다는 덜 파괴적인 것처럼 보이면서 제기되고 있는 질문은 국지전과 달리 전면전에서 사이버전의 영향력이 물리적인 군사공격에 비해 제한적인지의 여부임.

» 하지만 이번 전쟁의 양국 간 사이버전은 언론을 통해 알려진 것보다 훨씬 강력하고 복잡한 공격과 방어의 상황이 전개되고 있으므로 면밀한 분석을 통한 설명이 필요함.

러시아의 사이버 전력과 전술이 기존의 역량에 비해 제한적으로 보인 것은 우크라이나에 대한 서방의 전폭적인 사이버전 지원과 그동안 촘촘하게 구축되어온 서방과 우크라이나의 사이버전 대비태세가 영향을 끼친 것으로 설명할 수 있으며...

- 이번 러시아-우크라이나 전쟁에서 러시아의 사이버 전력과 전술이 기존의 역량에 비해 제한적으로 보인 것은 우크라이나에 대한 서방의 전폭적인 사이버전 지원과 그동안 촘촘하게 구축되어온 서방과 우크라이나의 사이버전 대비태세가 영향을 끼친 것으로 설명할 수 있음.
- 또한 이번 전쟁의 양국 간 사이버전은 두 국가 간 공격과 방어 차원에서 설명하기에는 다양한 수준의 행위자에 의한 복잡한 공격 행위가 있었고, 물리적 전장에서는 자제된 확전이 사이버 공간에서는 전혀 제어되지 않고 전개됨.

이번 전쟁을 계기로 사이버 공간은 모든 수준에서의 행위자를 본격적으로 군사적 차원에서 활성화시켰고, 그만큼 사이버 공간은 더 불안정하고 예측하기 어려운 전장으로 변모하며...

» 이번 전쟁을 계기로 사이버 공간은 모든 수준에서의 행위자를 본격적으로 군사적 차원에서 활성화시켰고, 그만큼 사이버 공간은 더 불안정하고 예측하기 어려운 전장으로 변모함.

» 한국은 IT 강국임과 동시에 사이버 위협에 빈번하게 놓이고 있으므로 이번 전쟁의 사이버전을 우크라이나와 서방이 어떻게 치렀는지 분석하는 것은 우리의 위기대응 및 대비태세 마련에 중요한 교훈을 줄 것임.

- 사이버 보안 회사 Specops가 조사한 바에 따르면, 한국은 2006년 5월부터 2020년 6월까지의 기간 동안 미국, 영국, 인도, 독일 다음으로 세계적으로 사이버 공격을 많이 당하는 다섯 번째 국가로서 세계적으로 사이버 위협에 가장 많이 노출되어 있는 국가 중 하나임.

» 이러한 맥락에서 이 보고서는 먼저 사이버전의 개념을 간략하게 소개하고, 2022년 러시아-우크라이나 전쟁의 사이버전 전개양상을 살펴보며, 전면전에서의 사이버전이 수행한 역할과 영향력 및 양국 사이버전 능력을 고찰함. 이러한 논의를 바탕으로 이 보고서는 우리가 추구할 사이버 전략과 사이버 안보협력의 의제 등 정책적 함의를 도출하고자 함.

2. 사이버전의 개념

가. 사이버전의 정의와 목적

'사이버전(Cyber Warfare)'은 특정 국가의 컴퓨터 네트워크나 정보 네트워크에 대해 위해를 가하여 대상 국가를 약화시키는 목적으로 수행되는 대규모의 사이버 공격을 의미하며...

» 일반적으로 '사이버전(cyber warfare)'은 국가 혹은 비국가 행위자들이 컴퓨터 바이러스나 디도스(Distributed Denial of Service, DDoS)공격 등의 수단을 통해 특정 국가의 컴퓨터 네트워크나 정보 네트워크에 대해 위해를 가하여 대상 국가를 약화시키는 목적으로 수행되는 대규모의 사이버 공격을 의미함.

» 美 사이버보안 및 인프라 보안국(Cybersecurity and Infrastructure Security Agency, CISA)은 사이버전의 목적이 공격목표로 삼는 국가를 "약화시키고, 분열시키거나 혹은 파괴시키는 것(weaken, disrupt or destroy)"이라고 언급함.

- 사이버전도 전통적 전쟁과 같이 금융기관, 산업기관, 에너지 인프라, 교통 인프라 등 국가의 주요기관을 파괴시켜 해당국가가 전쟁 자원을 동원하지 못하게 방해하고 혼란을 초래할 수 있음.

» 모든 사이버 공격이 사이버전으로 간주되는 것은 아니며, 대부분의 사이버 공격은 사이버 범죄인 경우가 대다수임. 즉 사이버 공격이 사이버전으로 간주되는 경우는 공격주체의 '의도(intentions)'와 공격의 '규모(magnitude)'가 국가 시스템을 붕괴시키고 위태롭게 만드는 효과를 노리는 것이어야 함.

사이버 공격이 사이버전으로 간주되는 경우는 공격주체의 '의도(intentions)'와 공격의 '규모(magnitude)'가 국가 시스템을 붕괴시키고 위태롭게 만드는 효과를 노리는 것...

» 사이버전에 대한 완전히 통일되고 합의된 정의(definition)가 부재한 것은 산발적으로 혹은 간헐적으로 이루어질 수 있는 사이버 공격이 어느 정도의 규모와 수준에서 이루어질 때 이것을 '사이버전'이라 일컬을 수 있느냐에 대한 합의가 아직 존재하지 않고, 사이버전을 수행하는 익명적 주체의 궁극적인 사이버 공격 목적이 국가 파괴인지의 여부를 확인할 수 없기 때문임.

나. 사이버전의 공격 형태

» 사이버전은 주로 금융망, 에너지 시설, 대중교통수단과 같은 사회기반 시설 등 국가의 핵심 인프라를 다양한 공격 수단을 통해 파괴시키는 형태를 취함.

- 디도스 공격, 랜섬웨어 및 와이퍼 공격, 피싱이나 멀웨어 같은 스파이웨어 등이 사이버전의 주요 수단이고, 사이버 심리전 및 사이버 첩보활동도 사이버전의 수단으로 간주됨.

» 디도스 공격은 일종의 '사이버 사보타주(sabotage)'로서 정부기관이나 군 기관 등 국가의 주요 웹사이트에 대한 압도적인 대량의 트래픽을 유입시켜 대상 시스템을 마비시켜 해당 웹사이트에 대한 접근이 불가능하게 만드는 수단임.

» 랜섬웨어(Ransomware)와 와이퍼(Wipers) 공격은 특정 중요 정보가 담긴 파일을 암호화시키거나 삭제하여 해당 파일에 대한 접근을 불가능하게 만드는 방식의 공격 수단임. 피싱(phishing)이나 스파이웨어(spyware)와 같은 멀웨어(malware)는 디지털 기기를 감염시켜 특정 정보를 탈취하는 방식의 공격임.

» 허위조작정보 유포(disinformation campaign)나 디지털 프로파간다(digital propaganda) 활동과 같은 사이버 심리전(cyber psychological warfare)은 인터넷과 소셜미디어(social media) 공간에 거짓정보를 확산시켜 여론을 왜곡하여 공격대상이 되는 국가의 정치적 정당성을 훼손하거나 사회를 분열시키고, 적국의 전투의지나 사기를 저하시켜 적국의 방어력을 약화시키는 공격 방식임.

» 적국의 정부기관이나 군 기관의 네트워크에 침투하여 주요 기밀과 정보를 은밀하게 수집하는 사이버 첩보활동(Espionage)도 사이버전의 주요한 공격 형태임.

3. 전개 양상과 특징

가. 전초전이자 군사적 공격과 결합된 사이버전

» 이번 전쟁의 사이버전은 실제 물리적 공격에 앞서 전세를 공격자에게 유리하게 만들어 놓는 '전초전'으로서도 수행됨.

- 러시아는 2월 24일 우크라이나를 침공하기 전부터 몇 달에 걸쳐 우크라이나에 대한 다양한 대규모의 사이버 공격을 수행했고, 러시아가 이번 전쟁 기간 동안 수행한 사이버 공격은 사이버전 역사상 가장 규모가 크고 가장 오랫동안 지속되었음.

이번 전쟁의 사이버전은 실제 물리적 공격에 앞서 전세를 공격자에게 유리하게 만들어놓는 '전초전'으로서도 수행되며...

» 러시아는 2022년 1월 14일 우크라이나의 외교부, 에너지부, 재무부 및 위기대응 관련 부처 등 70여개에 달하는 홈페이지를 해킹, 마비시키고 "너희들의 개인 정보는 모두 인터넷에 유출됐다. 컴퓨터의 모든 데이터는 파괴되었고 복구될 수 없다. 두려워하라, 그리고 최악을 기대하라"라고 러시아어, 우크라이나어, 폴란드어로 적힌 문구를 해킹된 웹페이지에 띄움.

» 러시아는 1월 15일 우크라이나 정부 웹사이트에 '위스퍼게이트(Whispergate)'로 불리는 멀웨어(malware) 공격을, 2월 15일과 16일에는 우크라이나 국방부, 국무부, 문화정보부 웹사이트 및 프리밧은행(Privatbank)과 오샤드은행(Oschadbank)의 전산 시스템에 디도스 공격 수행함.

» 러시아는 우크라이나를 실제로 침공한 2월 24일 직전 대규모의 와이퍼 공격(wiper attack)을 전개했음.

- 러시아는 침공 직전 우크라이나 정부 시스템과 데이터를 삭제할 의도로 개발한 와이퍼(wiper) 소프트웨어인 '폭스블레이드(FoxBlade)'라는 사이버 무기를 우크라이나 컴퓨터에 이미 설치했음.
- 침공 10시간 전 러시아는 우크라이나 정부 기관과 민간 기업의 300여개 시스템에 대해 헐메틱와이퍼(HermeticWiper)'로 불리는 대규모의 와이퍼 공격을 전개함.
- 마이크로소프트(Microsoft) 톰 버트(Tom Burt) 부사장은 공격의 규모 관점에서 볼 때 사실상 러시아의 침공일은 24일이 아니라 23일이라고 언급함.

» 이번 전쟁에서 최대 규모로 수행된 것으로 알려진 사이버 공격은 우크라이나 침공 1시간 전 러시아가 美 위성회사 비아샛(Viasat)을 겨냥한 멀웨어 공격으로서 전시에 수행된 사이버 공격으로서는 최대 규모로 알려짐.

- 러시아가 비아샛을 공격한 것은 우크라이나군이 미국의 비아샛 통신 서비스를 통해 자국 군을 지휘통제하고 있었기 때문임.
- 러시아의 이 공격으로 우크라이나를 포함하여 동유럽 국가 일대가 정전을 겪었고 비아샛의 핵심 인프라와 위성 자체에는 타격이 없었지만 비아샛의 수만 개 터미널(terminals)이 훼손되었음.
- 러시아의 비아샛 공격 이후 18일이 지난 시점에서도 비아샛의 KA-SAT 네트워크는 지속적으로 공격을 받아 시스템 복구에 어려움을 겪었음.

» 마이크로소프트사(Microsoft)가 파악한 바에 의하면 러시아는 2월 23일부터 4월 8일까지 우크라이나에 대해 40차례에 달하는 대규모 사이버 공격을 수행했고, 이러한 사이버 공격은 지속적으로 수행되어오고 있음.

» 이번 전쟁에서 러시아가 펼친 사이버 공격의 특징 중 하나는 군사공격과 사이버 공격이 합동작전을 펼치는 것과 같이 함께 수행되었다는 것임.

- 러시아의 군사공격과 사이버 공격 간 협동(coordination)의 패턴이 반복적으로 이루어졌으며, 이제 사이버전은 더 이상 새로운 전쟁의 양상이라기보다 전통적인 군사수단과 완전히 결합되어 조직적으로 전개되는 전쟁 수단으로 자리 잡은 것으로 보임.
- 우크라이나 침공 직전 러시아의 대규모 사이버 공격 외에도 러시아는 3월 1일 키이우 TV 타워를 폭격함과 동시에 우크라이나 키이우시의 미디어 회사를 해킹하여 데이터를 탈취, 삭제했고, 3월 2일에는 우크라이나 원전을 군사적으로 점령하면서 동시에 원전회사의 네트워크를 마비시킴.
- 러시아는 3월 4일에는 비니치아(Vinnytsia) 시의 정부기관을 사이버 공격하고 3월 6일 비니치아 공항을 폭격했으며, 11일에는 드니프로(Dnipro) 시 정부기관을 사이버 공격하면서 동시에 정부건물을 폭격함.

이번 전쟁에서 러시아가 펼친 사이버 공격의 특징 중 하나는 군사공격과 사이버 공격이 합동작전을 펼치는 것과 같이 함께 수행되었다는 것이며...

이제 사이버전은 더 이상 새로운 전쟁의 양상이라기보다 전통적인 군사수단과 완전히 결합되어 조직적으로 전개되는 전쟁 수단으로 자리 잡은 것으로 보이며...

나. 우크라이나와 서방의 대응

≫ 전쟁 개시 전 러시아가 우크라이나에 대해 수행한 2월 15일 사이버 공격에 대해 2월 18일 앤 뉴버거(Anne Neuberger) 美 사이버·신기술 담당 국가안보 부보좌관(Deputy National Security Advisor, Cyber & Emerging Technology at National Security Council)은 러시아 총정찰국(GRU)의 인프라가 우크라이나 아이피(IP) 주소와 도메인에 대량의 트래픽을 전송한 기술적 정보를 확보하고 있다고 발언함.

- 사이버 공격이 이루어진 이후 상대적으로 빠른 시점에 美 정부가 공격국가를 공개적으로 신속하게 지목한 것은 이례적인 일이었음.
- 그만큼 러시아가 전개한 사이버 공격의 규모가 위협적이었고, 우크라이나를 비롯한 서방의 대비태세가 시급함을 경고한 것이었음을 말해줌.

≫ 그동안 우크라이나는 주요 기관들이 마이크로소프트의 클라우드를 사용하는 것을 법적으로 금지해왔으나 러시아의 와이퍼 공격에 대응하여 3월 16일 우크라이나의 디지털변환부(Ministry of Digital Transformation)가 이전의 데이터 정책을 변경하여 우크라이나의 기관들이 클라우드를 사용하여 데이터를 저장할 수 있도록 조치함.

- 마이크로소프트사는 우크라이나의 미디어와 커뮤니케이션 기관의 웹사이트를 바로 복구시키고 반격 조치를 취하는 지원을 제공함.

≫ 러시아의 우크라이나 인터넷 인프라 공습으로 인해 2월 26일 미하일로 페도로프(Mykhailo Fedorov) 우크라이나 부총리(Vice Prime Minister) 겸 디지털혁신부(Minister of Digital Transformation) 장관은 일론 머스크(Elon Musk) 회장에게 트윗 메시지를 통해 스타링크(Starlink) 위성 인터넷 서비스제공을 요청하고 이에 일론 머스크가 화답하여 우크라이나의 인터넷 사용이 가능해짐.

- 스타링크는 지구 고도 550km 저궤도에 소형의 군집위성을 띄워 전 지구적으로 인터넷 망을 연결시키는 초고속 인터넷 서비스임.

- 6월 9일 기준 우크라이나에 제공된 스타링크 단말기 수는 15,000대이고 미국국제개발처(United States Agency for International Development, USAID)도 스타링크 단말기 5,000대를 우크라이나에 지원하였으며, 스타링크를 통해 인터넷을 사용하는 우크라이나 사용자 수는 하루 평균 150,000명으로 집계되고 있음.
- 주로 병원과 같은 민간시설에서 이용되고 있는 스타링크는 군사적 용도로도 사용되고 있으며 스타링크를 제공받은 우크라이나군은 스타링크의 단말기와 연결된 정찰 드론으로 러시아군에 대한 정밀 타격을 수행함.
- 마리우폴 아조우스틸 제철소에서 항전하던 고립된 우크라이나군도 스타링크를 이용하여 인터넷을 사용함.

» 5월 10일 미국, 유럽연합과 영국의 국가사이버안보센터(National Cyber Security Centre, NCSC)는 모두 비아샛에 대한 러시아 해커조직의 사이버 공격이 러시아 정부의 소행이라고 국제사회에 공식적으로 알림.

» 최근 6월 1일 에스토니아에서 열린 제14차 사이콘(International Conference on Cyber Conflict)에서 미국 사이버사령부 지휘관인 폴 나카소네(Paul Nakasone)는 미군이 우크라이나를 도와 사이버 공격과 사이버 방어 및 사이버 정보작전을 수행하고 있다고 발언하여 미국의 사이버 군사활동을 공개적으로 인정함.

- 미국이 자국의 사이버 군사활동을 공개적으로 언급한 것은 이례적인 일로서, 이러한 발언은 그만큼 러시아의 사이버 공격이 위협적이고 러시아의 사이버 공격에 대하여 서방이 공격적으로 대응할 것임을 러시아에 경고하는 것으로 볼 수 있음.

미국이 자국의 사이버 군사활동을 공개적으로 언급한 것은 이례적인 일로서, 그만큼 러시아의 사이버 공격이 위협적이고 러시아의 사이버 공격에 대하여 서방이 공격적으로 대응할 것임을 러시아에 경고하는 것으로 볼 수 있으며...

» 미국을 위시한 서방의 대러 사이버 공격으로 인해 러시아가 상당한 고전을 겪고 있는 것은 최근 6월 9일 러시아 외교부의 서방의 사이버 공격에 대한 경고 발언을 통해서 짐작해볼 수 있음.

- 러시아 외교부는 미국이 사이버 무기 사용의 문턱을 고의적으로 낮추어 러시아의 주요 인프라와 기관을 공격하고 있고, 이러한 서방의 사이버 공격이 러시아의 군사적 보복을 불러일으킬 것이라고 경고함.
- 러시아 외교부의 이 발언은 해킹당한 러시아의 건설주택공공시설부(Ministry of Construction, Housing and Utilities) 웹사이트가 "우크라이나에 영광을(Glory to Ukraine)"이라고 적힌 프로파간다 웹사이트로 연결되고 있는 시점 직후에 발표됨.

» 서방의 우크라이나 지원에 대해 러시아가 사이버 보복을 취할 가능성에 대해 6월 2일 백악관 대변인 카린 장-피에르(Karine Jean-Pierre)는 미국이 러시아-우크라이나 전쟁에서 직접적인 군사활동을 펼치지 않겠다고 했으므로 미국의 우크라이나 사이버전에 대한 지원이 러시아로부터의 사이버 보복을 초래할 것으로 보지 않는다고 언급함.

다. 사이버 확전과 비국가 행위자의 가세

이번 전쟁의 사이버전은 비국가 행위자가 대거 사이버전에 가세하여 사이버전의 확전 양상을 보이며...

» 이번 전쟁의 사이버전은 전쟁 당사국인 러시아와 우크라이나 양국 간 쌍방 공격과 우방국들의 양국 지원으로 제한되지 않고 해커(hackers), IT 기업, 일반 시민 등 국가 행위자와 비국가 행위자가 대거 사이버전에 가세하여 사이버전의 확전 양상을 보임.

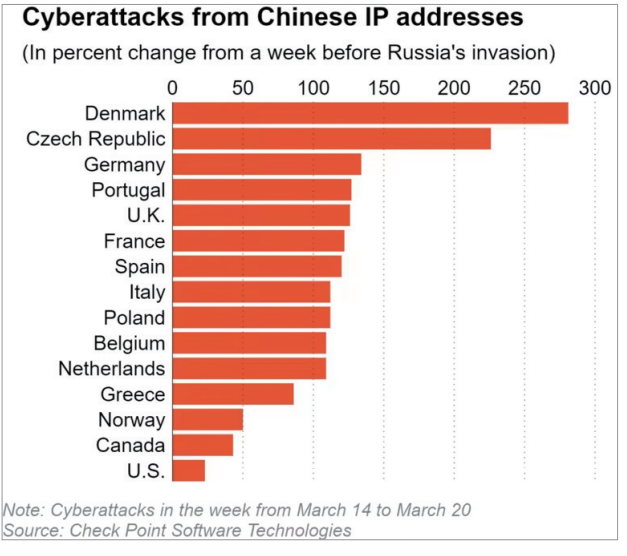
» 중국과 벨라루스의 해커조직이 러시아를 지원하며 우크라이나에 대한 사이버 공격에 가세한 것으로 보이는 정황이 포착되고 있음.

○ 러시아의 우크라이나 침공 직전 우크라이나 원전과 우크라이나 국방부를 포함하여 600개가 넘는 우크라이나 웹사이트에 대한 중국 정부와 연계된 해커조직의 소행으로 의심되는 수천 번의 사이버 공격이 발생.

○ 이스라엘 보안회사 'Check Point Software Technologies'는 3월 14일에서 3월 20일까지 전 세계에 대한 중국 IP 주소의 사이버 공격이 러시아의 우크라이나 침공 전 일주일보다 72%가 증가했고, 특히 나토 회원국에 대한 중국으로부터의 사이버 공격은 무려 116% 증가했다고 밝힘.

○ 호주 국방장관 피터 듀턴(Peter Dutton)은 중국의 화웨이(Huawei)가 러시아 인터넷을 방어하고 있다고 언급함.

〈표 1〉 **중국 IP 주소로 된 사이버 공격**



» 우크라이나 정부가 설립한 'IT Army'는 우크라이나 해커와 해외 해커로 구성되었고 이들은 러시아와 벨라루스 주요 기관 웹사이트에 대한 디도스 공격을 수행하여 우크라이나가 러시아의 사이버 공격을 효과적으로 제어하는 데에 도움을 주고 있음.

- 우크라이나를 지원하는 다양한 해커조직은 러시아와 벨라루스의 고위 관료와 주요 기관의 민감한 정보를 유출시키고 러시아 네트워크와 시스템에 와이퍼 공격을 취하고 있음.
- 이러한 해커조직의 러시아에 대한 공격으로 러시아는 현재 자국의 사이버 방어와 우크라이나에 대한 사이버 공격에 집중할 수밖에 없는 상황임.

» 구글(Google)은 우크라이나 정부의 요청에 따라 구글맵에서 우크라이나 현지 도로 상황을 실시간으로 보여주는 기능을 차단하여 러시아의 사이버 공간을 이용한 정보 활동을 방해함.

- 우크라이나는 구글맵과 위성사진을 분석하여 러시아군의 움직임을 미리 알아내었는데, 러시아도 해당 기능을 사용할 경우 우크라이나군 움직임을 포착하는 데 쓰일 수도 있기 때문에 구글은 이러한 조치를 취한 것임.
- 구글은 우크라이나에서 러시아 국영매체 Russia Today(RT) 애플리케이션 다운로드를 금지했고, 기존 사용자는 앱에 대한 접근은 가능하지만 업데이트된 소식을 받지 못하도록 하여 러시아의 정보심리전 활동을 방해함.

» 초국가적으로 활동하며 핵티비즘(hacktivism)을 표방하는 어나니머스(anonymous)는 러시아의 우크라이나 침공과 동시에 2월 25일 러시아에 공식적으로 사이버전을 선포하고 러시아에 대한 사이버 공격과 함께 사이버 심리전(psychological warfare) 활동도 수행함.

- 핵티비즘(hacktivism)은 '해킹(hacking)'과 '행동주의(activism)'의 합성어로서 정치적 어젠더나 사회변화를 추구하기 위해 해킹과 같은 컴퓨터 기술을 사용하는 인터넷 활동임.
- 어나니머스는 4월 3일 트위터(Twitter)에 우크라이나 영토에 진입한 12만 명의 러시아 군인들의 생일, 주소, 여권번호, 부대 소속 등 개인정보를 유출하고 이들이 전범 재판소에 넘겨져야 한다고 주장함.

- 어나니머스는 러시아 국방부 웹사이트에 디도스 공격을 하고 러시아의 보안이 허술한 프린터들에서 우크라이나의 프로파간다 메시지가 적힌 문서들이 출력되도록 만들었음.
- 어나니머스는 러시아의 관영매체 Russia Today(RT)의 웹사이트를 마비시키거나 러시아 TV 채널이 우크라이나를 지지하는 내용의 메시지나 우크라이나 노래가 나오도록 만들기도 함.
- 어나니머스는 러시아의 400개 이상의 CCTV를 해킹하여 러시아 대중에게 반전 메시지를 송출하였고, 어나니머스와 관련된 프로그래머 조직인 Squad303는 러시아인들의 핸드폰에 7백만 건의 반전 문자 메시지를 보내기도 함.
- 어나니머스는 트위터에 #OpRussia, #OpKremlin, #FckPutin, #StandWithUkraine와 같은 해시태그 문구를 통해 자신들의 사이버 활동을 홍보하고 다른 해커들도 동참하도록 함.

» 이번 사이버전은 대리전이 해커조직 간에도 진행되고 있음. Killnet을 비롯하여 CoomingProject, Sality.botnet, Salty Spider, Emotet, Mummy Spider 등 親 러시아 해커조직들은 나토 회원국과 동유럽국의 정부기관을 공격해오고 있음.

- 미국의 첩보동맹인 파이브아이즈(Five Eyes)는 이들 親 러시아 해커조직이 미국, 영국, 캐나다, 뉴질랜드, 호주를 공격할 것이라고 발표했고, 어나니머스는 그러한 발표 즉시 Killnet으로 불리는 친 러시아 해커조직 가담자 146명의 이메일과 비밀번호를 유출함.

4. 평가

가. 러시아의 사이버 전력

≫ 러시아의 사이버 전력에 대한 종합적이고 객관적인 평가는 현재도 전쟁이 지속되고 있으므로 시간의 경과에 따른 면밀한 분석을 필요로 하나, 개전 이후 현재까지 약 5개월 동안의 전쟁에서 드러난 바는 러시아의 사이버 전력이 예상했던 것만큼의 파괴력을 보여주지 못하고 있다는 것이 전반적인 평가임.

러시아의 사이버 전력이 제한적으로 발휘되고 있는 것은 러시아가 개전과 동시에 신속한 승리를 기대했던 원래의 계획이 의도대로 진행되지 않은 것과도 관련이 있어 보이며...

≫ 러시아의 사이버 전력이 제한적으로 발휘되고 있는 것은 러시아가 개전과 동시에 신속한 승리를 기대했던 원래의 계획이 의도대로 진행되지 않은 것과도 관련이 있어 보임.

○ 지난 4월 존 크리스 잉글리스(John Chris Inglis) 美 대통령실 국가사이버국장(National Cyber Director)은 러시아가 왜 미국과 나토에 대해 대대적인 사이버 공격을 수행하지 않는지가 “the question of the moment”이라며, 러시아가 개전 초반의 신속한 승리를 자신했으나 전쟁이 그렇게 진행되지 않자 주의를 빼앗긴 것(distracted) 같다고 언급함.

» 그럼에도 불구하고, 이번 전쟁의 사이버전을 통해 그동안 알려진 것과 달리 러시아의 사이버 전력은 과대포장되어 있었던 것으로 평가하는 시각도 다수 있음. 즉 현재까지 러시아는 우크라이나 이외 지역에 파괴력 있는 사이버전을 수행할 여력이 없는 것으로 보임.

- 현재 러시아의 사이버 공격은 우크라이나에 대한 공격에 집중되있고 러시아는 자국 네크워크에 대한 우크라이나와 서방의 사이버 공격을 막는 데에 급급한 상황임.
- 미국의 사이버 보안 회사 Cloudflare는 2월 러시아가 수행한 우크라이나에 대한 디도스 공격의 파괴력이 상대적으로 보통(modest) 수준이고 우크라이나를 넘어서는 공격도 라트비아(Latvia)와 리투아니아(Lithuania) 정도에 그치고 있다고 밝힘.

이번 전쟁의 사이버전을 통해 그동안 알려진 것과 달리 러시아의 사이버 전력은 과대포장되어 있었던 것으로 평가하는 시각도 다수 있음. 즉 현재까지 러시아는 우크라이나 이외 지역에 파괴력 있는 사이버전을 수행할 여력이 없는 것으로 보이며...

» 미국과 서방의 우크라이나 지원에 대한 러시아의 사이버 공격 보복을 우려하는 데 대해서 서방의 사이버 전문가들은 러시아가 미국에 사이버 공격을 하게 되면 우크라이나에 대한 공격에 집중할 수 없는 상황이 발생할 가능성이 높아지므로 그러한 가능성을 낮게 바라봄.

- 러시아는 현재 공격을 집중시키고 있는 돈바스 지역 이외의 곳에 한정된 자원을 투입할 수 없는 상황으로 판단함.

미국과 서방의 우크라이나 지원에 대한 러시아의 사이버 공격 보복을 우려하는 데 대해서 서방의 사이버 전문가들은 러시아가 미국에 사이버 공격을 하게 되면 우크라이나에 대한 공격에 집중할 수 없는 상황이 발생할 가능성이 높아지므로 그러한 가능성을 낮게 바라보며...

나. 사이버 플랫폼과 우주공간의 전장화

이번 전쟁은 사이버 공간의 플랫폼을 확보하는 것이 곧 국가의 전시 전투능력임을 증명하고 있으며...

스타링크가 우크라이나에 신속하게 제공되어 우크라이나의 사이버 공간에 대한 접근이 정상화됨에 따라 민간과 군 모두가 지속적으로 항전할 수 있게 하는 데에 절대적인 기여를 했으며...

≫ 이번 전쟁은 사이버 공간의 플랫폼을 확보하는 것이 곧 국가의 전시 전투능력임을 증명하고 있음.

- 러시아의 우크라이나에 대한 가장 첫 번째 공격 대상이 우크라이나의 정보커뮤니케이션 인프라와 사이버 플랫폼이었음.
- 스타링크가 우크라이나에 신속하게 제공되어 우크라이나의 사이버 공간에 대한 접근이 정상화됨에 따라 민간과 군 모두가 지속적으로 항전할 수 있게 하는 데에 절대적인 기여를 했음.

≫ 서방 IT 기업이 세계의 플랫폼을 거의 독점하고 있는 상황에서 러시아 관영매체 發 메시지가 우크라이나와 국제사회의 온라인 공간에서 확산되는 것이 차단되었기 때문에 사이버 플랫폼은 러시아와 우크라이나 양국의 심리전 활동에도 지대한 영향을 끼쳤음.

- 자국에게 유리하고 적국에게 불리한 전쟁 정보와 내러티브를 확산시키는 사이버 심리전 활동에 있어서 러시아는 전시 심리전 활동을 과거만큼 효과적으로 전개할 수 없었음.

≫ 이번 전쟁에서 우크라이나에 대한 우주위성 인터넷 제공으로 인해 중국은 스페이스X의 스타링크 위성 수천 개가 중국 현지에 대한 감시용으로 투입되거나 대만 지원을 위해 배치될 가능성을 경계하게 되었음.

- 러시아와 중국은 스타링크 위성을 물리적으로 파괴할 '하드킬(hard kill)' 무기가 필요함을 인지함.
- 이번 전쟁으로 중국은 일론 머스크의 테슬라(Tesla)에 대한 우려도 커짐. 테슬라는 차량용 카메라에 부착된 주행 영상 데이터를 수집한 뒤 이를 인공지능 빅데이터로 분석하고 있으므로 중국은 테슬라 차량이 수집한 정보가 첩보전에 이용되는 것을 막기 위해 주요 지역에의 접근을 차단하고 있음.

다. 민간의 사이버전 개입 본격화

» 이번 전쟁의 사이버전은 비국가 행위자들이 사이버 공간에서의 군사적 활동을 전면적으로 활성화시킨 계기를 만들었음.

- 어나니머스와 같은 해커조직들의 활동은 우크라이나와 러시아 및 서방 정부와 긴밀하게 공조하고 있는 것으로 보이고 있음.
- 비국가 행위자의 본격적인 사이버전 개입으로 인해 앞으로 사이버 교전과 관련된 국제사회의 규범형성 노력은 더 복잡하고 어려운 과제를 풀어야 하는 상황에 놓이게 되었음.

비국가 행위자의 본격적인 사이버전 개입으로 인해 앞으로 사이버 교전과 관련된 국제사회의 규범형성 노력은 더 복잡하고 어려운 과제를 풀어야 하는 상황에 놓이게 되었으며...

» 국제적 해커조직이 해킹을 통해 민감한 정보를 유출하거나 일국의 프로파간다 메시지를 확산시키는 활동은 심리전 효과를 가져오기도 하는 등 이번 전쟁을 통해 민간도 전시 사이버 심리전 활동에 깊숙이 개입하게 됨.

- 어나니머스는 3월 러시아와 밀접한 경제 관계를 갖고 있는 기업인 마라톤그룹(Marathon Group), 타오지스그룹(Thozis Group), 매쉬오일(MashOil) 등을 해킹하여 이들 기업의 이메일을 비롯한 수십만 개 이상의 정보를 공개했음.

○ 이러한 정보유출은 푸틴 대통령의 측근인 올리가르히 즉 러시아 산업과 금융의 재벌들에게 정치적 압박을 가하기 위한 것으로서 어나니머스의 이러한 해킹은 심리전에 가세한 것과 다름없음.

이번 전쟁은 사이버 심리전에 있어서도 디지털 플랫폼을 본격적으로 무기화시키는 계기로 작동했고, 세계의 디지털 플랫폼을 독점하고 있는 서방의 IT 기업들은 러시아의 사이버 심리전 활동이 기술적으로 가능하지 않도록 원천적으로 차단하여...

» 이번 전쟁은 사이버 심리전에 있어서도 디지털 플랫폼을 본격적으로 무기화시키는 계기로 작동했고, 세계의 디지털 플랫폼을 독점하고 있는 서방의 IT 기업들은 러시아의 사이버 심리전 활동이 기술적으로 가능하지 않도록 원천적으로 차단하는 역할을 함.

○ 구글(Google)이나 Meta 등 서방의 세계적 IT 기업도 Russia Today(RT)나 Sputnik와 같은 러시아 관영매체가 전쟁에 대한 세계 여론에 영향을 끼치는 기사와 메시지를 인터넷과 Facebook, Instagram, YouTube, TikTok과 같은 소셜미디어 공간에 확산시키지 못하도록 차단함.

○ 이들 기업들은 우크라이나인을 대상으로 하는 러시아와 연계된 소셜미디어 계정, 그룹, 페이지, 채널들의 네트워크가 모두 폐쇄되고 수상한 채널들도 삭제되었음.

라. 평시 사이버전 대비태세와 우방 지원의 위기복원력 효과

» 이번 전쟁의 사이버전은 2016년 이후 서방이 나토를 중심으로 마련해 온 나토 회원국과 동유럽 우방에 대한 사이버전을 포함한 하이브리드 위협에 대한 대응태세의 효과를 검증해 볼 수 있는 시험대였음.

이번 전쟁의 사이버전은 2016년 이후 서방이 나토를 중심으로 마련해 온 사이버전을 포함한 하이브리드 위협에 대한 대응태세의 효과를 검증해 볼 수 있는 시험대였으며...

- 나토는 2015년 3월 'East StratCom Task Force'를 조직하여 러시아의 정보 심리전에 취약한 동유럽국에 대한 지원을 제공해왔음.
- 2016년 바르샤바 정상회담(Warsaw Summit)에서 나토가 사이버 공간을 나토의 공동 군사작전이 수행될 공간으로 공식 선언한 이후 나토는 다양하고 촘촘한 사이버전 대비태세를 갖춰오고 다양한 대규모의 사이버전 모의훈련을 회원국 및 파트너국과 수행함.

» 나토가 사이버전과 허위조작정보 유포(disinformation campaign)를 포함한 다양한 하이브리드 위협에 대응하는 위기대응 체계를 갖추게 된 것은 2014년 우크라이나 침공에서 보여준 러시아의 하이브리드 전술과 2016년 미 대선 이후 거의 모든 서구권 선거에 러시아가 허위조작정보 유포를 통해 개입한 것이 계기가 됨.

- 서방은 국가의 핵심 인프라와 네트워크에 대한 사이버 공격뿐 아니라 민주주의의 핵심 제도인 선거에 영향을 줄 만큼 파괴력 있는 러시아의 심리전이 서방의 민주주의 제도의 근간을 훼손하고 주권을 침해하는 것으로 결론내리고 군사적 차원에서 대응해야 할 문제로 판단함.

우크라이나는 러시아 發 사이버 공격과 사이버 심리전에 대응하기 위해 전쟁 전 이미 서방과 다양한 협력과 모의훈련을 수행해왔으며...

» 우크라이나는 러시아 發 사이버 공격과 사이버 심리전에 대응하기 위해 전쟁 전 이미 서방과 다양한 협력과 모의훈련을 수행해 왔음.

○ 2020년 1월 말 우크라이나의 심리전(Psychological Operation, PSYOP)팀은 독일의 합동다국적대응태세센터(Joint Multinational Readiness Center)에서 진행되는 군사훈련인 'Combined Resolve XIII'에 참여했음. 이 훈련에는 우크라이나를 포함한 17개국이 훈련했고, 이 훈련에서 우크라이나는 미국과 2014년 러시아의 정보심리전 경험을 공유하며 협력함.

5. 정책적 함의

가. 외교부 내 사이버 안보 부서 신설 및 사이버 안보 위기 대응역량 강화

» 최근 미국은 이번 러시아-우크라이나 전쟁을 계기로 2022년 4월 5일 국무부에 '사이버 공간·디지털 정책국(Bureau of Cyberspace and Digital Policy, CDP)'을 출범시켜 특별조직을 통해 국무부 차원에서 사이버 안보 및 신기술 이슈를 핵심 외교정책 우선순위에 둘 것을 공고히 했음.

최근 미국은 이번 러시아-우크라이나 전쟁을 계기로 '사이버 공간·디지털 정책국(Bureau of Cyberspace and Digital Policy, CDP)'을 출범시켜 국무부 차원에서 사이버 안보 및 신기술 이슈를 핵심 외교정책 우선순위에 둘 것을 공고히 했으며...

- 미국의 이러한 제도적 조치는 이번 러시아-우크라이나 전쟁이 보여준 사이버전의 역할과 영향력을 확인한 데 대한 대응으로서, 국무부가 사이버 안보 문제를 주요 외교정책 이슈로서 직접 관리하고 외교적 지원을 아끼지 않겠다는 의지를 보여줌.

» 최근 우리 외교부도 경제안보와 군사안보 양 측면의 사이버 이슈를 다룰 과학기술 사이버국(가칭) 신설 가능성을 언급한 바, 새로운 부서 신설이 현실화될 경우 사이버 위협에 대한 우리의 대응력 및 사이버 안보 현안에 대한 우리의 외교역량도 강화될 것으로 기대함.

우리 외교부도 사이버 이슈를 다룰, 새로운 부서 신설이 현실화될 경우 사이버 위협에 대한 우리의 대응력 및 사이버 안보 현안에 대한 우리의 외교역량도 강화될 것...

- 현재 외교부에는 국제안보과가 전통안보와 사이버 안보, 신기술, 기후, 에너지, 보건안보를 포함하는 광범위한 신안보(emerging security) 현안을 모두 다루고 있어 사이버 안보 이슈를 전적으로 다룰 인력과 조직 및 자원이 부재함.
- 전시가 아닌 평시에도 사이버 안보 이슈는 국민의 일상적인 삶과 경제활동 및 국가 산업과 금융, 투명한 여론형성 등 국가와 사회의 정상적인 기능 유지와 직결되므로 군과 정보기관뿐 아니라 외교부도 이 분야에 대한 전문적 이해를 획기적으로 증진시킬 수 있어야 함.

» 외교부에 사이버 안보 및 신기술 이슈를 독립적으로 다루는 부서가 신설될 경우 미 국무부의 사이버 공간·디지털 정책국(CDP)이 자연스럽게 카운터파트너가 되므로 외교부와 美 국무부 간 사이버 안보 현안 관련 협력을 빠르게 진전시킬 수 있음.

- 외교부와 국무부 간 다양한 정책협의회를 비롯하여 전문 인력 간 워크숍과 세미나를 활성화시키고, 그러한 활동을 촉진시킬 직무교육을 외교부 내 개설하는 등 양국 간 사이버 안보 위협에 대한 공동의 위협인식을 토대로 촘촘한 위기대응 태세를 구축해야함.

» 오늘날의 사이버 안보 위협은 현대의 안보환경이 전투공간과 비전투공간, 평시와 전시의 구분, 공공영역과 민간영역의 경계가 모호한 데에서 하이브리드 위협의 형태로 빈발할 수 있으므로 외교부가 신설할 과학기술사이버국(가칭)은 사이버 안보 위협이 다양한 종류의 위협과 결합되는 하이브리드 위협을 염두에 둔 위기대응에도 관심을 두어야 함.

- 현재 미국과 유럽의 사이버 안보 위협에 대한 대비태세는 사이버 공격과 디지털 프로파간다 활동을 포함한 하이브리드 위협에 대한 대응을 중심으로 이루어지고 있고, 그러한 복합적인 위기대응 태세는 국지전과 전면전 모두에서 국가의 위기복원력을 효과적으로 증진시키는 데에 기여할 것임.

» 외교부는 차후 사이버 위협과 아울러 사이버 공격에 빈번하게 동반되는 다양한 하이브리드 위협에 대응하는 데에 가장 중요한 '전략커뮤니케이션(strategic communication) 체제'를 신속하게 구축해야하고, 이러한 체제구축에 있어서 다른 부처와의 긴밀한 협의가 필요함.

외교부는 차후 사이버 위협과 하이브리드 위협에 대응하는 데에 가장 중요한 '전략커뮤니케이션(strategic communication) 체제'를 신속하게 구축해야...

- 사이버전뿐 아니라 사이버 위협과 함께 초국가적, 복합적, 동시다발적으로 일어날 수 있는 다양한 비전통적 위기에 범부처가 효과적으로 대응하기 위해서는 정보공유와 위기대응 메시지 발신 및 신속한 의사결정을 효과적으로 동원하는 데에 전략커뮤니케이션 체제의 구축은 필수적임.
- 나토 또한 2014년 1월 러시아의 우크라이나에 대한 사이버 위협 등 침공 전 두드러졌던 다양한 하이브리드 위협에 대한 대응에서 가장 먼저 회원국 및 관련 조직 간 효과적인 커뮤니케이션을 촉진하고 의사결정 및 명령체계를 강화시킬 수 있는 나토 전략커뮤니케이션센터(NATO Strategic Communication Centre of Excellence)를 라트비아에 설립한 바 있음.

나. 동맹 및 우방과의 사이버 위협 공동대응을 위한 전략대화 강화

» 2022년 5월 정상회담에서 한국과 미국은 사이버, 우주, 인공지능 등 신기술 협력을 위해 한·미 사이버 정책협의회와 사이버워킹그룹의 논의를 가동할 것과 디지털 권위주의에 대항하여 개방적이고 자유롭고 안전한 인터넷 공간을 만들기 위해 공조할 것을 합의했음.

» 최근 군 차원에서 한미 간 사이버 정보공유 활성화와 정기적 위협평가 및 합동군사훈련 등 실제적인 사이버 안보협력이 빠르게 진전되고 있음.

- 우리(국방조사본부)와 미국(공군 특수수사국)은 12월 사이버범죄대응 공동훈련을 계획하고 있고 사이버 범죄 관련 양국의 군 수사기관 간 협력을 강화하기로 함.
- 우리 공군은 미 공군·우주군과의 다자연합훈련, 한·영, 한·호주 우주협력합의서 체결 및 세계항공우주 지휘관 회의 참석을 계획하는 등 동맹 및 우방과의 우주 안보 협력 강화에 적극적인 행보를 보이고 있음.
- 우리 군은 2022년 10월 美 사이버사가 주관하는, 영국, 캐나다, 호주, 뉴질랜드, 일본, 프랑스 등이 참가하는 '사이버 플래그(Cyber Flag)' 연례훈련에 처음 참가할 예정임.

» 다자안보 차원에서도 한국은 사이버 모의군사훈련에 참가하는 등 사이버 위협 대응에 대한 우리의 실제적 대응력이 빠르게 향상될 것으로 기대됨.

- 최근 국정원이 주축이 되어 한국은 아시아 최초로 유럽의 사이버 안보 기구인 나토 사이버방위센터 (Cooperative Cyber Defence Centre of Excellence, CCDCOE) 회원국으로서 가입한 만큼 앞으로 나토와의 사이버 안보협력은 한층 더 강화될 것임.
- 국정원은 나토사이버방위센터가 주최하는 사이버 모의군사 훈련인 '라키드쉴드 훈련(Exercise Locked Shields)'에 2년 연속 참가한 바 있음.
- 우리 군도 그간 참관만 했던 나토 회원국과 파트너국이 참가하는 사이버동맹 (Cyber Coalition) 연례연합훈련에 2023년부터 참가할 예정임.

외교부도 사이버 안보협력을 다차원적으로 도모하여 우리 정부가 외교와 국방 간 균열 없이 일치된 사이버 안보 정책을 펼칠 수 있도록 지원해야...

» 위와 같이 국정원과 군 차원에서 진전되고 있는 다양한 한미 사이버 안보협력 및 다자안보협력에서의 진전과 조응하여 외교부도 사이버 안보협력을 다차원적으로 도모하여 우리 정부가 외교와 국방 간 균열 없이 일치된 사이버 안보 정책을 펼칠 수 있도록 지원해야 함.

- 현재 국정원과 국방부가 사이버 보안 및 방위와 관련된 실제 역할과 책임을 담당하고 있으나 부처 간 사이버 안보 위협에 대한 동일한 인식과 전문적 역량을 형성하고 일관된 사이버 안보 정책을 추진하기 위해 외교부도 적극적으로 관련된 외교정책을 추구해야 함.

» 한국은 미국, 일본, 호주, 캐나다, 뉴질랜드, 유럽 등 유사입장국(like-minded countries) 및 아세안 등과 사이버 안보 위협 관련 어떤 이슈와 수준, 범위와 성격의 차원에서 실제적 협의와 협력을 증진시킬 것인지 사이버 안보 외교를 위한 다층적인 세부 계획을 수립해야 함.

- 우리의 외부로부터의 사이버 심리전 공격에 대응할 역량 구비 의지와 구축 노력이 명확하지 않고 적극적이지 않다면 우리에게 접근해오는 유사입장국과의 협력의 기회를 놓칠 수 있으므로 외교부 및 다양한 관련 부처의 인식제고가 선행되어야 함.
- 한국은 미국과 7월과 11월 개최되는 제8차, 제9차 아세안 확대국방장관 회의(ADMM-Plus) 사이버안보 분과회의 및 9월의 서울안보대화 사이버워킹 그룹에서 사이버 안보협력 관련 다양한 논의를 진전시킬 계획이고, 이번 해부터 아세안과 사이버 모의훈련을 시작할 예정임.
- 호주와 뉴질랜드도 사이버 공격뿐 아니라 외부로부터의 허위조작정보의 공격과 같은 사이버 심리전에 대해 심각하게 인식하고 있고 한국과 다양한 협력을 희망하고 있음.

» 우리의 유사입장국들과의 사이버 안보 협력이 구체적으로 어떤 사이버 위협을 상정하고 어떤 수준의 공동대응 역량을 증진시키려고 하는 것인지 국가 별 혹은 국가군별 협력 계획이 수립되어야 함.

우리의 유사입장국들과의 사이버 안보 협력이 구체적으로 어떤 사이버 위협을 상정하고 어떤 수준의 공동대응 역량을 증진시키려고 하는 것인지 국가 별 혹은 국가군별 협력 계획이 수립되어야...

- 격화되고 있는 미중경쟁과 진영화 추세로 인해 유사입장국 중에서도 서방의 미동맹국들과 비동맹국들과의 사이버 위협에 대한 인식과 실제 사이버 안보 정책은 서로 다를 수 있으므로 국가별, 국가군별로 세밀하게 차별된 정책을 펼칠 수 있어야 함.
- 한국의 사이버 다자안보 협력은 우리와 협력할 국가의 사이버 위협에 대한 동일한 혹은 서로 다른 수준의 위협 인식에 따라 영역과 강도가 달라질 것임.
- 각각의 국가가 우리와 어떤 사이버 위협을 공유하고 있는지, 위협이 되는 어떤 국가 혹은 비국가 행위자를 공유하는지 국가 별 국가군별 분석을 통해 각각의 국가와 협력을 위한 의제 조율 및 발굴에 활용해야 함.

다. 사이버 안보 위협에 대한 대응에 있어서 민간과의 공조 강화 및 민간의 보안역량 증진

» 이번 전쟁의 사이버전에서는 사이버 공격과 방어 및 사이버 심리전 수행 모두에서 마이크로소프트, 구글, 스페이스X 등 IT 기업과 민간 전문가와 프로그래머 등이 국가와 긴밀하고 신속하게 공조, 협력했고, 우방의 IT 기업 등 초국가적 협력에 있어서 민간의 기여가 지대했음.

국지전이나 전면전에 동반될 사이버전 대응에 있어서 민간과의 협력은 전시에 갑자기 가능해지는 것이 아니라 평시 정보공유와 공동된 위협인식 및 사이버 공격 대응에서의 실제 긴밀한 공조가 지속적으로 이루어지고 있는 바탕에서 가능한 것...

» 국지전이나 전면전에 앞으로 반드시 동반될 사이버전 대응에 있어서 민간과의 협력은 전시에 갑자기 가능해지는 것이 아니라 평시 사이버 안보환경에 대한 정보공유와 공동된 위협인식 및 사이버 공격 대응에서의 실제 긴밀한 공조가 지속적으로 이루어지고 있는 바탕에서 가능한 것임.

» 따라서 평시 IT 기업과 정부 간의 사이버 위협 대응 협력을 위한 빈번한 정보교류, 상호지원 및 인력 파견, 공동연구와 국제협력 공동 진출 등이 획기적으로 활성화될 필요가 있음.

» 정부는 민간의 사이버 보안 역량 및 공세적인 사이버 전력 구비를 자발적으로 갖출 수 있도록 다양한 법·제도적 및 예산·인력 등의 자원을 통한 지원을 제공할 수 있어야 함.

» 또한 정부는 민간과의 공조와 협력을 도모하기 위해 민간과 평시 신뢰할 수 있는 파트너십과 연대를 강화하고 공통된 안보관을 구축하기 위한 다양한 교류, 전략토론과 공동훈련의 장을 마련해야 함.

CONTRARIA SUNT COMPLEMENTA

상반되는 것은 보완적인 것이다

Institute of Foreign Affairs & National Security
Korea National Diplomatic Academy

IFANS