물리적 사이버 위협 대응을 위한 사이버전자전 기술

김소연, 김성표, 이정훈, 최승호, 최채택, 채명호, 박범준, 정운섭
국방과학연구소
e-mail:comet613net@daum.net

Cyber Electronic Warfare Technology for Responding Physical Cyber threats

Soyeon Kim, Seongpyo Kim, Jung_Hoon Lee, SeongHo Choi,
ChaeTaek Choi, Myoung Ho Chae, ByumJun Park, Un-Seob Jeong
Agency for Defense Development

요 약

모든 객체와 공간이 네트워크로 연결된 초연결 사회는 시·공간에 제약받지 않은 상호 소통으로 새로운 가치와 혁신을 창출할 수 있다. 그러나 이와 더불어 불특정 다수의 고도·지능화된 사이버 위협이 폭발적으로 증가하고 있다. 특히, 초연결 사회의 사이버 위협은 기존 사이버 공간 공격에만 그치지 않고, 물리적인 공격수단으로까지 진화 중이다. 본 논문은 이와 같은 물리적 사이버 위협에 대응하기 위한 사이버전자전 수행 개념, 적용 핵심 기술들에 관해 연구하였으며 향후, 사이버전자전 발전방향을 제안하였다.

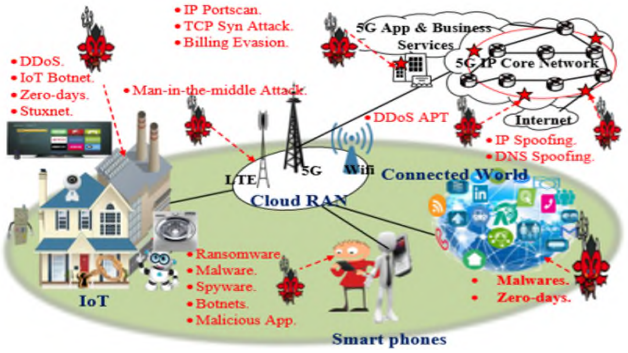
1. 서론

초연결 사회(Hyper-Connected Society)에서 사이버 위협은 사이버 공간 공격에만 그치지 않고, 물리적인 공격수단으로까지 진화 중이다. 따라서 이와 같은 이와 같은 물리적 사이버 위협에 대응하기 위해서는 기존의 사이버 공간 방어기술에서 탈피하여 사이버전과 전자자전의 개념을 융합한 사이버전자전 수행개념과 기술을 발전시킬 필요가 있다. 본 논문은 사이버전자전 수행 개념, 적용 핵심 기술들에 관해 연구하였으며 향후, 물리적 사이버 위협 대응에 핵심전력이 될 수 있는 사이버전자전 발전방향을 제안하였다.

2. 초연결 사회와 사이버 위협

2.1 사이버 위협의 공격양상 발전전망

초연결 사회라는 말은 2008년 미국 IT 컨설팅회사 Gartner Inc.에서 처음으로 사용되었으며, 모든 객체와 공간이 네트워크화 되어 시·공간에 제약받지 않는 상호소통으로 새로운 가치화 혁신을 창출할 수 있는 사회를 의미한다. 그러나 초연결 사회는 불특정 다수의 고도·지능화된 사이버 위협이 폭발적으로 증가된 사회이기도 하다. 이는 사이버 위협 또한 초연결 되기 때문이다. 그림 1은 초연결 사회 핵심기술들과 더불어 여기에 기생하는 각종 사이버 위협 기술들을 보여준다[1].



[그림 1] 초연결 사회와 사이버 위협[1]

특히, 최근에는 사이버 위협에 의한 공격이 사이버 공간에만 국한되지 않고, 물리적 공격으로까지 진화되고 있다. 즉, 사이버 위협의 교란대상과 공격수단은 “사이버 공간에 대한 정보탈취/오염을 위한 악성코드” 에서 “물리적 공간에 대한 주요시설 파괴, 핵심인물 암살을 위한 물리적 공격” 으로 발전되고 있다. 이는 물리적 공격으로 인한 파급효과가 훨씬 더 크기 때문이다. 물리적 사이버 위협의 대표적인 예로는 고정형 RC-IED(Radio Control Improvised Explosive Device, 무선조정 급조폭발물), RC-IED 탑재 소형 드론, 미사일/공격무기 장착 중형 드론 등이 있다.

2.2 물리적 사이버 위협에 의한 비정규전 증가

RC-IED는 Shooter(사수)가 원격(무전기, 휴대폰 등)제어장치로 특정주파수에 반응하는 급조폭발물 기폭장치를 조

정하여 폭발을 유도하는 무선조정 급조폭발물로써, 전문지식이나 첨단기술 없이도 제작/설치가 용이하고, Shooter의 피해를 최소화하면서 수십-수백m 거리 밖에서 주요시설을 파괴하거나 핵심인물을 수 암살할 수 있어 2000년대 이후 이를 이용한 세계 곳곳의 테러/게릴라가 급증하고 있다[2].

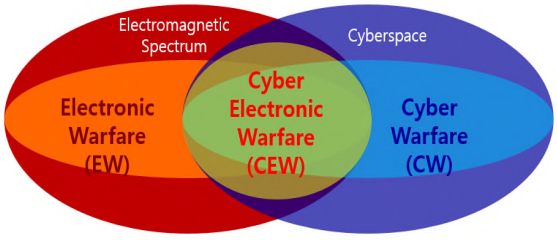
최근에는 RC-IED를 드론에 장착하여 수백m-수km 원거리에서 목표물을 공격하는 방식이 등장했다. 대표적인 예는 2018년 6월 니콜라스 마두로(베네수엘라 대통령) 드론 암살미수 사건으로, 국가방위군 창설 81주년 행사에서 마두로 연설 도중 공중에서 드론 2대가 폭발하였으며 군인 7명이 부상당했다. 드론 위협에 대한 가장 큰 관심을 불러일으킨 사건은 2020년 1월 거셈 솔레이마니(이란軍 사령관) 암살이다. 사령관 일행이 시리아에서 바그다드 국제공항에 도착하여 출발한 직후 무장한 드론의 조준폭격에 의해 솔레이마니를 포함한 5명이 사망하였다. 미국은 중형급 무장드론(MQ-9/리퍼)을 본토에서 인공위성을 이용하여 원격 운용하고 정밀타격을 지시한 것으로 추정된다.

[그림 2] 무인기에 의한 이란 솔레이마니 암살[3]

이와 같은 세계 각국의 비정규/국지戰 추세로 미루어 볼 때, 미래에는 더욱더 초연결 네트워크를 이용한 물리적 사이버 위협 공격이 증가되고 가속화될 것이다. 따라서 이에 대한 대응 방안이 무엇보다도 시급하며 이를 위해서는 물리적 사이버 위협의 특징을 면밀히 파악하여 그 진화속도를 뛰어 넘는 대응 기술을 개발하여야 할 것이다.

3. 사이버전자전 개념 및 기술

3.1 사이버전자전 개념 및 필요성



[그림 3] 사이버전자전(CEW) 개념[4]

사이버전자전이란 전자기 스펙트럼을 이용하여 적의 무선 네트워크 공간을 비롯한 사이버 공간을 교란, 파괴, 통제하는 군사적 행위를 의미한다.

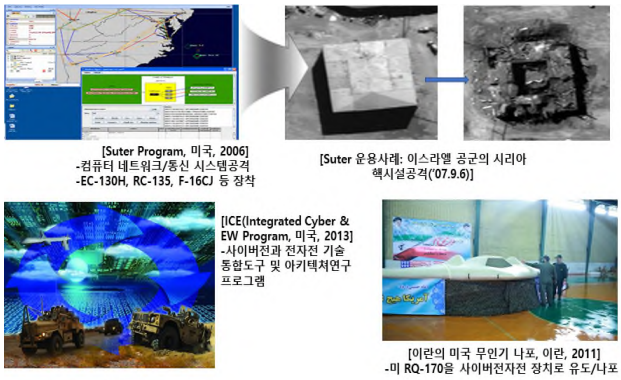
사이버전(CW: Cyber Warfare), 전자전(EW: Electronic Warfare), 사이버전자전(CEW: Cyber Electronic Warfare)의 특징을 비교. 분석하면 다음과 같다[5][6].

[표 1] 사이버전, 전자전, 사이버전 특징

구분	사이버전(CW)	전자전(EW)	사이버전자전(CEW)
목표 대상	사이버 공간	물리적 공간 (전자기 스펙트럼 공간)	물리적 공간+ 사이버 공간
공격 수단	악성코드	고출력 전자기 스펙트럼	고출력 전자기 스펙트럼+악성코드
효과	지속적/장기적 사이버 공간 정보교란/조작	일시적 시스템 방해	지속적/장기간 사이버 공간 및 시스템 교란

표 1에서 알 수 있듯이 사이버전 기술은 정보교란 능력에서 전자전보다 우위에 있다. 즉, 악성코드(예> 허위메시지, 바이러스) 등으로 사이버 공간의 정보를 지속적 또는 장기적으로 조작하고 교란할 수 있다. 반면에 전자전 기반 기술은 고출력 무선전파 송출능력에서 사이버전보다 우위에 있다. 따라서 물리적 전자기 스펙트럼 공간에서 수십-수백km 밖의 위협을 공격할 수 있다. 사이버전자전은 사이버전과 전자전 기술의 장점을 취합하여 물리적 무선 네트워크(스펙트럼) 공간과 사이버 공간에서 공격 시너지 효과 창출을 할 수 있으므로 물리적 사이버 위협대응을 위한 핵심적인 기술이 될 수 있을 것이다[6].

3.2 해외 및 국내 사이버전자전 동향



[그림 4] 해외 사이버전자전 사례[7]

2000년대 이후, 군사 선진국들에서는 사이버작전과 전자전을 교리, 조직, 기술 등의 측면에서 융합하고 통합하려는 동향들이 있으며, 사이버전자전 무기체계/SW개발, 다양한 CEW 통합도구/프로그램들을 운용중이다.

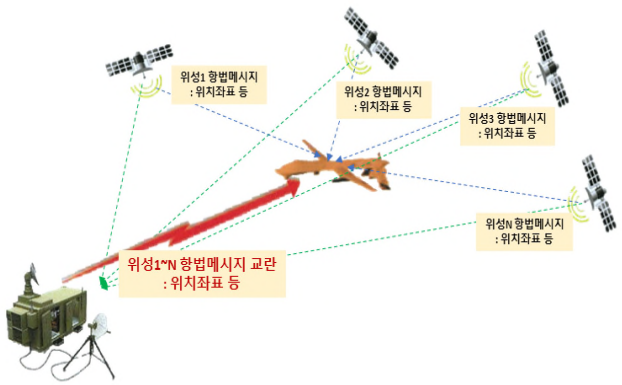
이에 반해 국내 사이버전자전은 개념연구 단계로써, 전

자전의 원거리 고출력 전자파 탐지/송출능력과 사이버전의 정보(메시지) 조작/교란능력을 통합하여 시너지 효과를 발휘할 수 있는 기술로 발전되어야 한다.

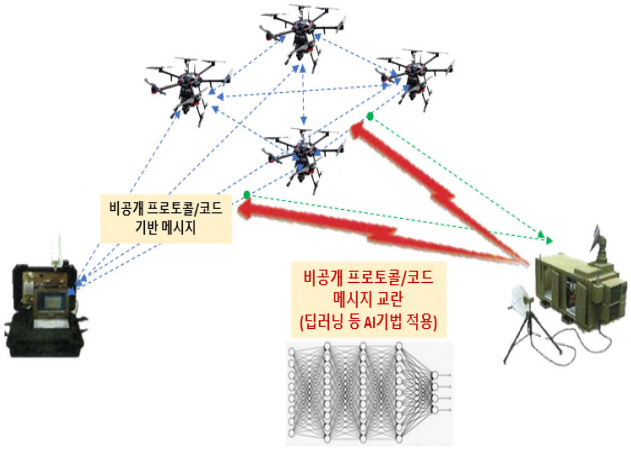
3.3 사이버전자전 핵심기술 및 발전전망

사이버전자전 기술의 핵심은 보안에 취약한 무선 네트워크 접점을 공격하는 것이 될 수 있다. GPS 수신기 탑재 무기체계(드론/무인기, GPS유도 미사일 등), 공개/보안취약 무선네트워크 체계, 위성체계 등이 현실적인 공격대상이 될 수 있다. 이에 필요한 핵심기술로는 위성 항법신호 교란기술, Radio Control 신호 교란기술 등이 있다.

위성 항법신호 교란 기술은 항법신호로 유도되는 물리적 사이버 공격 위협에 대응하기 위해 필요하다. 기존 전자전 기술이 잡음전파 송출로 위성 항법신호로 유도되는 드론/무인기 등을 궤도이탈/추락시켰다면 사이버전자전에서는 항법위성 메시지를 탐지/분석하고 허위/기만 메시지를 생성하고 송출하여 사이버 위협을 특정경로/안전지역으로 유도한다. 이는 폭발/화학무기를 장착한 물리적 사이버 위협 대응을 위해 매우 긴요한 기술이다.



[그림 5] 위성 항법신호 교란기술



[그림 6] Radio Control 신호 교란기술

Radio Control 신호는 RC-IED 의 기폭장치 제어 및 무인 위협들의 제어를 위해 이용된다. 따라서 Radio Control 교란기술은 Shooter(사수)의 제어신호로 유도되는 물리적 사이버 공격위협에 보다 적극적으로 대응하기 위해 반드시 필요하다. Radio Control 신호는 공개된 위성 항법신호와는 달리 비공개 프로토콜/코드 신호를 기반으로 한다. 따라서 딥러닝 등 AI 기법을 이용하여 이를 추정한 뒤, Radio Control 신호를 탐지/분석하고 허위/기만 메시지를 생성·송출할 수 있는 핵심기술 개발과 적용이 필요하다.

4. 결론

본 논문에서는 초연결 사회와 사이버 위협, 특히 점차 증가되고 있는 물리적 사이버 위협에 대해 언급하였다. 그리고 그 대응책으로 전자전의 고출력 전자파송출 기술과 사이버전의 메시지 조작/교란 기술을 융합한 사이버전자전 기술을 소개하고 물리적 사이버 위협 진화추세에 맞추어 중점 개발되어야할 주요 핵심기술들에 대해 다루었다.

결론적으로 사이버전자전의 발전을 위해서는 사이버전자전 공격에 취약한 현실적인 위협, 무기체계를 우선 식별한 뒤, 이에 필요한 핵심기술을 도출하고 이를 중점적으로 개발하여야 한다.

참고문헌

[1] Rabia Khan, et al., “A survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future directions”, IEEE Communications Surveys & Tutorials, July 2019.

[2] 미 태평양 육군, “급조 폭발물 대응”, 아시아 태평양 급조 폭발물 융합센터 특집기사, 2018. 01. 18

[3] 손진석, “본토서 조종한 美드론... 닌자폭탄 장책해 ‘핀셋 타격’”, 조선일보, 2020. 01. 06

[4] Nurgul YASAR, et al., “Operational Advantages of using Cyber Electronic Warfare(CEW) In the Battlefield”, Cyber Sensing, Proc. Of SPIE Vol. 8408, 2012.

[5] 김소연 외, “스마트 전자전: 사이버 전자전”, 국방신기술 동향분석, 2016. 1.

[6] 김성표, “미래 능동적 사이버전 수행개념”, 한국군사과학기술학회 추계학술대회, 2017.

[7] 이광일, 이승근, “사이버전자전 기술 개발동향”, 국방신기술동향분석, 2014. 09.