디지털산업정보학회 논문지 제17권 제1호-2021년 3월
http://dx.doi.org/10.17662/ksdim.2021.17.1.015

제4차 산업혁명시대의 테러에 악용되는 첨단 정보통신기술*

심 세 현**·엄 정 호***

Advanced ICT abused by Terror in the 4th Industrial Revolution Era

Sim Se-Hyeon·Eom Jung-ho

〈Abstract〉

The 4th industrial revolution technology has brought many changes not only in human life but also in the industrial field. ICT such as 5G and artificial intelligence and convergence/complex systems such as drones and robots are convenient for humans, and automation of all processes in the industrial field. However, these advanced information and communication technologies also have adverse functions. As advanced ICT was incorporated into military and terrorist weapon systems, more powerful and highly destructive weapon systems began to be developed. In particular, by applying advanced ICT to the production and use of terrorist tools, the terrorist method became more sophisticated and caused more damage. In this paper, we derive advanced ICT that can be abused according to the terror patterns in the 4th industrial revolution era, and present a method that is applied from preparation to execution of terrorism. The abuse of advanced ICT makes terrorism more stealthy and subtle, and increases its destructive power.

Key Words : Terrorism, Terror Means, Terror Pattern, ICT Abuse, 4th Industrial Revolution Technology

Ⅰ. 서론

포스트 IS 시대의 테러 양상은 냉전 종식 이후의 테러 방식과는 주체, 수단, 목표 등의 측면에서 다른 면모를 보여준다. 냉전 종식 직후에 테러 주체자는 국가, 준국가 독립체, 테러조직이었으나, 포스트 IS 시대에는 개인부터 테러조직의 지령을 받은 준조직원 등 다양하다. 테러 수단도 군사적 무기체계에서 총기, 폭탄, 급조폭발물 등 다양한 형태의 테러 수단이 출현하였다. 특히, 급조폭발물은 사람의 눈에 띄지 않게 숨길 수도 있고, 설치도 용이하여 최근까지도 많이 사용하는 테러 수단이기도 하다. 테러 대상은 특정 인물이나 기간시설이 주요 표적이었으나, 테러 수단이 다양해지면서 테러 대상은 불특정 다수, 시민 밀집 지역 등으로 확대되었다[1].

최근에는 테러에 다양한 수단이 사용되고 있는데, 대표적인 예가 드론이다. 드론에 폭탄을 적재하고 공

* 이 논문은 2020학년도 대전대학교 교내학술연구비 지원에 의해 연구되었음.
** 대전대학교 안보융합학과 조교수
*** 대전대학교 군사학과&안보융합학과 부교수(교신저자)

격 대상이 위치한 지역으로 비행하여 폭탄을 투하하거나 자폭하는 방식으로 테러가 발생하고 있다. 2018년에는 베네수엘라 군 창설 행사 도중에 여러 대의 드론이 행사장을 공격하였으며, 2019년에는 예멘 반군이 무인기 10대에 폭탄을 탑재하여 사우디 국영석유회사의 최대 석유 탈황/정제시설을 공격한 바 있다[2, 3].

과학기술과 정보통신기술 발달로 인해서 테러 수단이 첨단화되고 이를 활용한 테러 방식이 점점 지능화되고 있다. 특히, 제4차 산업혁명시대의 테러 방식은 첨단 정보통신기술을 테러 수단에 접목시키거나 융/복합화하여 더욱 정교하고 신속한 형태로 진화할 것으로 보인다.

첨단 정보통신기술이 테러 대응 기술에도 활용되지만, 테러 수단으로도 활용되기 때문에 테러 수단에 적용되는 첨단 정보통신기술 종류와 활용 방식을 파악하여 사전에 대응 기술 개발에 참고함으로써 효과적인 대응책을 마련할 수 있다. 본 논문은 2장에서 4차 산업혁명기술과 제4차 산업혁명시대의 테러 양상을 분석하고 3장에서 테러에 악용될 수 있는 정보통신기술을 도출한다. 4장에서는 첨단 정보통신기술이 테러에 악용되는 방식을 분석하며, 마지막 5장에서 결론을 맺는다.

Ⅱ. 관련연구

2.1 4차 산업혁명기술

제4차 산업혁명시대에는 5G와 같은 초고속 이동통신 기술, 인공지능 기술 등과 같은 첨단 정보통신기술이 일상생활뿐만 아니라 생산 공정에도 활용되면서 매우 빠르고 광범위하게 일상생활 패턴을 변화시키고 있다. 수많은 첨단 신기술들이 융합되고 통합되면서 새로운 방식의 삶을 영위하게 해주고 있다. 상상을 초월하는 5G의 속도와 광범위한 데이터, 인간처럼 생각하고 행동하는 인공지능 기술, 인간이 조작하지 않아도 스스로 동작하는 무인체계, 이러한 체계들을 통합시키고 융합하는 인터넷 기술, 모든 사물을 하나의 네트워크로 연결하는 사물인터넷 기술 등은 인간의 삶에 반드시 필요한 요소로 부각되고 있다. 대표적인 4차 산업혁명기술 중에 첨단 정보통신기술의 종류는 다음 표와 같다[4, 5].

<표 1> 4차 산업혁명기술 중 첨단 정보통신기술의 종류

종류	내 용
드론 (Drone)	지상에서 원격조종, 사전 프로그램된 경로에 따라 자동 또는 반자동으로 자율비행하거나 인공지능을 탑재하여 자체 환경 판단에 따라 임무를 수행하는 무인 비행체
로봇 (Robot)	사람과 유사한 기능을 가진 기계, 또는 무엇인가 스스로 작업하는 능력을 가진 기계로 제조공장에서 조립, 용접, 핸들링 등을 수행하는 자동화된 로봇을 산업용 로봇이라 하고 환경을 인식하고 스스로 판단하는 기능을 가진 로봇을 지능형 로봇이라 함
3D 프린터 (3D Printer)	3차원 형상을 구현하기 위한 전자적 정보를 자동화된 출력장치를 통하여 입체화하는 프린터. 실제 물체의 형태나 외형을 디지털 데이터로 수집해 그것을 기반으로 디지털 모델을 제작한 후 제품 특성에 따라 조형하는 장비
인공지능 (Artificial Intelligence)	컴퓨터가 경험을 통해 학습하고 새로운 입력 내용에 따라 기존 지식을 조정하며 사람과 같은 방식으로 문제를 해결하거나 과제를 스스로 수행할 수 있도록 지원하는 기술
사물인터넷 (Internet of Things)	모든 사물을 연결하여 인간의 개입을 최소화하고 지능적으로 사물간의 정보를 교류하며 가공하여 인간에게 더 나은 서비스를 제공함.

이 밖에도 대용량 데이터를 신속하고 정확하게 분석할 수 있는 빅데이터 기술, 가상현실 기술 기반으로 실제 환경과 유사하게 구현할 수 있는 증강/혼합현실 기술도 있다.

2.2 제4차 산업혁명시대의 테러 양상

포스트 IS 시대의 테러 사례를 분석해 보면, 과거

전통적 테러 위협과는 대조적인 모습으로 변화하였다. 우선, 테러의 주체가 불명확하고 테러 주체자의 정체를 사전에 확인할 수 없어서 테러 징후를 탐지하기가 힘들었다. 또한, 공격 대상도 불특정 개인부터 시민 밀집 지역과 건물까지 소프트 타깃과 하드 타깃 모두 공격 대상이었다. 테러조직이 전 세계적으로 수평적으로 분포하며 동시다발적으로 테러를 감행으로써 이에 대한 대처 시간이 절대적으로 부족하였다. 아울러 과학기술과 정보통신기술의 발달로 테러 주체자들이 테러 수단(도구) 제작 방법도 쉽게 획득하고 제작할 수 있게 되면서 로우테크(Low-Tech) 방식으로 확산되었다[6].

제4차 산업혁명시대에서는 4차 산업혁명기술의 핵심이라고 할 수 있는 정보통신기술의 획기적인 발전으로 테러리스트나 조직들이 테러 방식에 첨단 정보통신기술을 활용할 것으로 예상된다. 현재에도 테러 실행에 필요한 정보 수집부터 테러 계획 및 실행까지 첨단 정보통신기술의 활용도가 높아지고 있다. 이러한 첨단 정보통신기술이 본격적으로 테러에 활용될 경우에는 테러 방식이 기존과는 현격히 다른 방식으로 진행될 것으로 예상되며, 위협 수준도 높아질 것으로 예측된다[7]. 제4차 산업혁명시대에 4차 산업혁명기술의 핵심인 첨단 정보통신기술이 테러에 악용된다면, 테러는 다음과 같은 양상을 보이게 될 것이다.

첫째, 4차 산업혁명기술의 등장은 테러 발생 가능성을 더욱 확대시키고 있다. 실제로 4차 산업혁명기술 중에 정보통신기술의 복합체라고 할 수 있는 드론을 악용한 테러 및 범죄행위는 지속적으로 증가하는 추세이다[2]. 드론을 테러에 악용할 경우에는 공간적 제약을 극복할 수 있고 테러리스트가 테러 지역과 이격된 원거리에서 통제가 가능하며, 드론에 사제 폭발물이나 폭탄 탑재가 용이하다는 장점이 있다. 또한, 인터넷 다크 웹사이트를 통해서 잠재적 테러리스트들도 테러 도구 제작 방법을 쉽게 획득할 수 있으며, 3D 프린터를 이용하여 제작도 할 수 있다[1,8]. 테러 도구 제작과 테러 방식에 대한 정보를 쉽게 습득할 수 있다는 것은 테러 발생 확률을 높이는 주요 원인이 된다.

둘째, 테러가 발생할 수 있는 공간적 범위가 확대될 수 있다. 기존의 테러 방식이 테러 주체자가 직접 테러 목표 지역으로 이동해서 정찰한 후 직접 폭탄, 총기 등을 소지하고 테러 지역으로 이동한 후에 테러를 감행했다. 하지만, 드론이나 무인 로봇 등을 활용하면 테러 지역에 테러 주체자 직접 가지 않더라도 정보 수집이나 정찰이 가능하며, 원거리에서 테러를 감행할 수 있게 된다.

셋째, 기존의 테러 도구와 정보통신기술의 융/복합화 현상이 나타나고 있다. 전통적인 테러 도구에 첨단 정보통신기술을 접목시킨다거나 여러 개의 테러 도구를 융합하는 새로운 방식의 테러가 발생하기 시작했다. 인공지능을 적용한 드론에 폭탄을 탑재하여 목표물까지 정확하게 도달하게 한다거나 정찰 및 탐색을 위해서 초소형 로봇에 고해상도 카메라를 장착할 수도 있다. 테러 도구의 융/복합화 현상은 잠재적 테러리스트들의 테러 감행을 부추기거나 테러 효과를 극대화시킨다.

마지막으로, 첨단 정보통신기술을 접목시킨 테러 도구에 의한 테러는 더욱 정교하고 은밀하게 발생하면서 파괴력도 상상을 초월하게 될 것이다. 과거의 테러는 테러 주체자가 특정한 정치적 목표를 가지고 핵심 대상이 되는 목표물을 분명히 선정하고 직접 실행하는 경우가 많았다. 하지만, 첨단 정보통신기술의 복합체라고 할 수 있는 드론과 로봇을 활용하게 되면, 테러 주체자가 직접 나서지 않고 테러 대상에 대한 접근, 실시간 목표물 정찰 및 감시 등 원거리에서도 전반적 상황을 관찰하며 테러를 감행할 수 있다. 보이지 않는 곳에서 테러를 감행할 수 있다면, 불특정 다수를 대상으로 한 테러의 발생 가능성은 더욱 높아질 수 있으며, 직접 테러를 감행하지 않기 때문

에 죄의식이 상당 부분 감소하여 보다 대담한 테러 행위를 시도할 가능성이 높아진다[9].

Ⅲ. 테러에 악용 가능한 첨단 정보통신기술 도출

제4차 산업혁명시대의 테러리즘은 포스트 IS 시대의 뉴테러리즘의 양상과 특징에 비해 크게 다르지 않지만, 4차 산업혁명기술의 핵심 정보통신기술이 적용된 테러 수단으로 인해 보다 치밀하고 정교하면서 표적화된 테러 방식으로 변모할 것으로 보인다. 또한, 첨단 정보통신기술을 접목시키거나 활용한 테러 도구나 인터넷에서 제공하는 테러 도구 제작 정보를 활용한 비형태적인 테러 도구가 빈번하게 활용될 것이다. 실제로 최근에는 드론에 폭탄을 장착하여 시설물이나 밀집 지역으로 비행하여 폭파시킨다거나 드론에 악성코드를 탑재하여 공격 대상 정보 통신체계에 접근하여 해킹을 시도하는 사례가 발생하기도 했다. 또한, 산업용, 재난구조용, 군사용으로 활용되고 있는 로봇이 테러 수단으로 활용되는 경우도 증가할 것이다[10].

이처럼 제4차 산업혁명시대의 테러는 드론, 로봇, 인공지능 기술, 인터넷 등을 통해 더욱 치밀하게 이루어질 것으로 예상되며, 3D 프린터로 제작된 비형태적 테러 도구가 일반 시민들에게는 쉽게 발각되지 않아 테러조직들에게 매혹적인 테러 수단으로 여겨지고 있다. 아울러 세계를 하나로 연결하고 막대한 정보를 전송하고 공유할 수 있는 네트워크와 이동통신 체계를 마비시킴으로써 테러에 대한 정보 공유를 차단하고 대응활동을 지체시키는 통신 테러도 증가할 것이다[8,10]. 최근에는 시중에서 쉽게 구할 수 있는 전파교란기로 정찰용, 교통 감시용 드론을 추락시킨 사례도 있다[11]. 아울러 지능적인 해킹 도구를 이용하여 공격 대상 지역의 CCTV를 해킹하여 주변 정보를 획득하거나 테러 진행사항을 파악하며, 대테러 조직의 운영 시스템을 해킹하여 대응 활동을 지연시키거나 추적을 피하는 경우도 있을 수 있다. 테러 수단에 접목시키거나 활용할 수 있는 첨단 정보통신기술의 종류와 기능은 다음과 같다.

첫째, 드론은 운송/배송, 수색/정찰/감시, 촬영 및 오락, 군사 분야 등 다양한 분야에서 활용되고 있다. 특히, 4차 산업혁명기술인 인공지능, 5G 등의 기술이 드론 비행제어에 적용됨으로써 자율 비행이 가능해지기 시작했다. 첨단 정보통신기술이 적용된 드론은 군사용으로 활용이 증대되고 있는 가운데 적 감시, 매복이나 은밀 침투, 정찰, 폭탄 투하, 전파 교란 등의 임무를 수행하는 다목적 전투 드론으로 진화하고 있다[12]. 이러한 군사용 드론은 테러조직에게 가장 유용한 테러 수단으로 활용될 수 있다. 정병수의 '드론 테러의 사례 분석 및 효율적 대응방안[2]'에서 제시한 것처럼 드론이 새로운 유형의 테러 방식을 창출하고 효율적이고 정교한 전술을 펼치기 위해서 드론을 악용하는 사례가 증가하고 있다. 고해상도 카메라가 장착된 드론은 테러 대상 지역을 정찰하거나 경찰의 이동을 감시하며, 가장 적합한 테러 위치를 식별하는데 활용될 것이다. 아울러 드론에 스마트 경량 전파교란기를 탑재하여 공격 대상 지역의 감시 통신망 주파수를 마비시킬 수도 있다. 악성코드를 탑재하여 공격 대상 정보통신체계에 근접하여 감시/추적 시스템을 해킹하거나 드론 자체를 무기화하여 테러 대상 지역으로 비행하여 공격할 수도 있다.

둘째, 지능형 로봇은 로봇에 인공지능 기술과 첨단 센서 기술을 접목시켜서 외부환경을 인식하고 스스로 상황을 판단하여 자율적으로 동작하는 로봇을 의미한다[4]. 최근에 논란이 되고 있는 군사용 킬러 로봇은 인공지능 기술을 적용한 로봇으로 인간의 직접적인 개입 없이도 프로그램에 따라서 스스로 공격 대상을 적으로 판단하여 공격하는 로봇이다[13]. 이러한 로봇을 일반 시민을 표적으로 프로그램하여 테러용

으로 사용한다면, 제압하기도 힘들고 인명피해도 막대할 것이다. 그리고 초소형(곤충 형태)으로 제작하여 테러 실행 이전에 테러 대상 지역을 정찰하는 임무를 수행할 수도 있다. 이만종의 '인공지능을 악용한 테러 가능성과 대응전략[10]'에서는 인공지능로봇이나 킬러 로봇 등에게 테러를 학습시킨 뒤에 테러에 활용할 것으로 예측하고 있다.

셋째, 3D 프린팅은 프로그램을 통해 형상을 3차원적으로 모델링하여 프린터로 전송하면, 모델링한 형상대로 3차원 물체를 제작하는 기술이다. 3D 프린팅은 성형이라든지, 가공 방식보다 훨씬 더 정교하여 자동화 방식으로 편리하게 제품을 제작할 수 있는 장점이 있으며, 자동차 용품, IT 액세서리, 의류, 항공기 엔진 부품, 인공장기 등 다양한 분야에서 활용되고 있다. 그러나 3D 프린팅 기술이 확산되면서 이에 따른 역효과도 나타나고 있다. 대표적인 것이 총기류 제작인데, 3D 프린터로 제작한 권총은 인명 살상도 가능하고 기존 금속 탐지기로 탐지가 어려우며, 테러 수단으로도 사용되고 있다[8]. 실제로 미국에서 발생한 총기 난사 사건에 사용된 몇몇 총기류는 고스트건으로 조립세트나 3D 프린터로 제작된 것이다[14]. 또한, 3D 프린팅 기술을 이용하면 급조 폭발물을 기존의 급조 폭발물보다 정교하게 소형으로 제작이 가능하며, 일반 가정용품으로 교묘하게 위장하는 것도 가능하다. 더욱이 인터넷 기술의 발달로 잠재적 테러리스트들도 웹사이트(다크 사이트)를 통해 급조 폭발물이나 총기류 제작 정보를 쉽게 습득할 수 있으며, 이를 3D 프린터를 통해 실제로 제작할 수 있게 되면서 테러 발생 가능성이 증대되고 있는 실정이다.

넷째, 스마트 재밍 또는 전파교란은 전파가 강한 주파수를 방사하여 디바이스가 기존 주파수와 연결되지 못하고 강한 전파의 주파수와 연결되어 오작동을 발생시키는 기술이다. 스마트 재밍기를 테러용으로 사용할 경우에 GPS로 동기를 맞추는 발전소에서 시간적 오류를 발생시켜 손실을 유발시키거나 항공교통에서 잘못된 정보 입력으로 항공통제에 혼선을 유발시킬 수 있다. 스마트 재밍 중에서 잡음기법은 위성 신호보다 40dB 이상의 강한 잡음 신호를 방출하여 수신기가 GPS 신호를 제대로 수신하지 못하게 방해하는 기법이다[15]. 이 기법을 활용한 재밍기는 재밍 장치의 제작이 용이하고 고출력으로 방사하기만 하면 되는 단순한 교란 방법이어서 테러조직이나 테러리스트들에게 매혹적인 테러 수단이 될 수 있다. 스마트 재밍기가 테러에 이용될 경우에는 테러리스트들의 추적이나 동선 파악을 방해할 목적으로 사용될 수 있다. 즉, 감시/추적 위성 시스템에서 송출하는 신호를 제대로 수신하지 못하게 하는 것이다. 또한, 스마트 재밍을 통해서 이동통신 기지국의 통신을 방해할 수 있으며, 테러 목표 대상자가 탑승한 비행기와 자율주행 차량에 탑재된 주행(비행) 제어 시스템의 GPS 신호를 교란시켜 사고를 유발할 수도 있다.

마지막으로 인공지능 기술은 지능, 추론 능력에 기반하여 기계가 스스로 상황을 판단하고 행동할 수 있는 기술이다. 인공지능 기술은 항공기나 차량의 비행/주행 제어 시스템에 적용하여 비행경로나 주행 도로 주변의 상황을 스스로 학습하여 비행경로나 주행 도로를 판단하는데도 활용되고 있다. 또한, 로봇에 적용하여 인간처럼 생각하고 인간처럼 행동할 수 있는 지능형 로봇을 생산하기도 한다[16]. 인공지능 기술이 테러용 드론이나 로봇에 적용된다면 공격 대상 지역까지의 이동 경로를 스스로 학습하고 판단함으로써 감시망을 우회하여 안전하게 도달할 수 있으며, 정확하게 표적을 공격할 수 있게 한다. 또한, 테러조직이 테러 계획부터 실행까지의 과정까지 인공지능 기술을 통하여 필요한 정보를 획득할 수 있으며, 가장 성공률이 높은 테러 수단과 방식을 추천할 수도 있다. 많은 언론에서 인공지능 기술이 탑재된 로봇에 테러 알고리즘을 학습시켜서 다중이용 시설을 공격하거나 생화학 테러도 가능하다고 지적하고 있다[17]. 최근에는 해킹 기술에 인공지능이 적용되면서 지능적인 사

이버 공격이 가능하게 되었다[18, 19]. 테러리스트들은 테러 주변 정보 확인과 테러 진행사항을 파악하기 위해서 테러 대상 지역에 설치된 CCTV를 해킹할 수 있다. 그리고 테러 이후에 대테러 조직으로부터 추적을 회피하기 위해서 대테러 운영 시스템을 해킹하여 대테러 활동을 지연시키거나 GPS 추적 장치를 해킹하여 위치를 찾지 못하도록 할 것이다. 이러한 인공지능 기술이 본격적으로 테러 수단에 적용된다면, 테러 징후를 사전에 포착하거나 테러를 탐지하고 테러리스트를 검거하기가 쉽지 않을 것이다.

<표 2> 테러에 악용될 수 있는 첨단 정보통신기술의 종류

종류	활 용
첨단 드론	- 초소형 드론에 첨단 영상장비를 탑재하여 테러 대상 지역이나 건물에 대한 영상정보 획득 - 드론에 폭탄을 장착하여 공격 대상으로 비행하여 낙하 - 다수의 드론을 군집 비행시켜 여러 테러 대상에 대한 자폭 - 악성코드를 탑재하여 공격 대상 네트워크로 접근하여 정보 유출
지능형 로봇	- 급조 폭발물을 테러 지역으로 운반하는 이동 수단으로 활용하거나 총기류를 탑재하여 인명살상 수행 초소형 비행 로봇(곤충형 로봇)을 이용하여 공격 대상 지역 정찰 및 감시 - 고성능 카메라, 도청 장비 등을 장착한 초소형 로봇을 통해 국가 주요 기밀 탈취 - 도체 물질 전파 교란기를 탑재, 전선이나 랜선 등으로 이동, 합선이나 통신 두절 유발
3D 프린터	- 웹사이트에서 제공하는 급조 폭발물/총기류 제작법을 습득하여 비형태적 테러 도구 제작 - 3D 스캔, 형상 복제를 통해서 테러 도구가 적발되지 않도록 일상 사물과 유사하게 제작
소형 스마트 전파 교란기	- 강한 주파수를 사용하여 감시/경계 드론의 기능을 중단시킨다거나 오작동 유도 - GPS 교란을 통해 대테러 대응 관련 경찰 통신 장애 발생
인공 지능	- 드론이나 로봇에 자가 학습과 판단 기능을 적용, 공격 대상 지역까지 자율 비행/이동함으로써 감시망 우회 - 동시 다발적 테러 실행 시에 테러 수단간 통신, 의사결정 등을 통해 감시체계 혼선 초래

Ⅳ. 테러 과정 단계별 첨단 정보통신기술의 악용

테러를 실행하기 위해서는 준비부터 실행까지 몇 단계를 걸쳐야 한다. 테러 정당성 확보를 위한 홍보, 테러리스트들의 모집, 필요한 자금 조달 등의 준비 단계, 테러 대상 지역에 대한 정보 수집 및 정찰과 정보 공유 단계, 테러 수단과 방식을 선택하는 단계, 테러 모의훈련 단계, 그리고 실질적으로 테러를 감행하는 실행 단계가 있다. 본 장에서는 테러 과정 단계별 첨단 정보통신기술의 악용 방식을 도출하여 향후 대응 전략 수립에 도움을 주고자 한다.

테러 준비단계에서는 테러의 정당성을 확보하고 시민들을 선동하기 인한 홍보 활동, 테러를 실행할 테러리스트 모집, 인건비 마련, 테러 도구 및 필요한 장비 구매 등에 필요한 자금을 조달해야 한다. 홍보 활동에는 지금도 활용하고 있는 방법으로 포스터나 동영상을 제작하여 인터넷의 웹사이트에 업로드하거나 불특정 다수에게 이메일을 전송하는 방법을 계속 사용할 것이다. 조직원 모집도 현재 사용하는 방법으로 트위터, 페이스북, 유튜브, 채팅 등 소셜 네트워킹 플랫폼을 통해 조직원을 모집할 것이다. 테러 자금 조달은 현재 다크웹 사이트를 통해서 무기나 마약을 거래하거나 가상화폐 기반의 크라우드 펀딩을 받는 방법[8]을 사용하고 있는 가운데 보다 진보된 방법으로 랜섬웨어 공격, 금융회사 해킹 등 지능형 해킹을 통해서 불법 자금을 마련할 것으로 보인다.

정보 수집 및 공유 단계에서는 공격 대상 지역에 대한 정보를 수집하고 테러리스트 간에 수집한 정보를 공유하는 단계이다. 우선 테러 대상 지역에 대한 정보는 고해상도 카메라를 장착한 드론을 통해 테러 지역을 정찰하여 영상정보를 획득할 수 있다. 또한, 저렴한 가격으로 인터넷 웹사이트에서 제공하는 인공위성 영상도 활용할 수 있다. 그리고 인근 지역에 있는 CCTV를 해킹하여 24시간 감시할 수 있으며, 경

비나 경찰 순찰 경로와 시간을 확인할 수도 있다. 테러리스트들 간에 수집한 정보는 앱이나 이메일을 통해서 암호화 통신으로 교환한다.

테러 수단과 방식 선택 단계에서는 테러 도구를 제작하고 테러 실행 방식을 수립하는 단계이다. 테러 도구 제작은 소셜 네트워크나 포털 사이트 등의 온라인 서비스, 특히 다크웹과 같은 익명성이 보장된 사이트에서 실제 테러를 감행하는데 요구되는 사제폭탄 등의 제조 방법과 사용 방법, 폭탄 제조 재료에 대한 정보와 부품을 조립하는 방법 등을 습득하여 3D 프린팅 기술로 폭탄을 제작할 수 있다. 그리고 앞 단계에서 수집한 정보를 기반으로 테러 대상 지역에 설치된 시설물이나 물품들과 유사하게 제작함으로써 시민들에게 적발되지 않고 은밀하게 설치할 수 있다. 3D 프린터로 활용하여 드론 낙하용 폭탄을 제작할 때는 가볍고 폭발력이 강한 경량화 재질로 제작할 수 있다. 테러 방식은 테러리스트, 테러 지역 정보, 테러 수단에 대한 정보를 갖고 시뮬레이션 기술을 활용하여 테러 시나리오를 만들 수 있다. 그리고 인공지능 기술이 접목된 의사결정 시스템을 활용하여 가장 성공률이 높고 피해를 많이 줄 수 있는 시나리오를 선택하게 한다. 인공지능 기술을 적용한 시뮬레이션은 테러 목적, 테러 수단, 테러 대상, 예상 피해 등을 입력하면 최적의 테러 경로를 선정할 수 있으며, 감시망을 뚫고 추적을 피할 수 있는 방법까지 제공받을 수 있다.

테러 모의훈련 단계에서는 앞 단계에서 선택된 테러 시나리오대로 훈련을 수행한다. 테러 목표물과 주변 환경에 대해 3D 모델링 기술을 이용하여 모델링하고, 가상현실/증강현실 기술을 이용하여 모델링된 환경을 마치 실제 상황인 것처럼 시뮬레이터를 구축하여 직접 훈련을 진행할 수 있다. 휴먼인터페이스 기술을 이용해 실제와 같은 동작이 적용되게 하고, 인공지능 기술을 이용해 발생 가능한 상황을 모두 분석해 보는 등 테러를 실제 상황과 유사하게 훈련할 수 있다. 이미 다양한 분야에서 이러한 시뮬레이션 기술이 적용되고 있기에, 테러리스트들도 이러한 기술을 활용하여 테러의 성공률을 높이려 할 것이다.

테러 실행 단계에서는 테러 진행사항을 파악하고 분석하며, 돌발 상황 발생시에는 테러 방식을 변경하거나 중지할 수 있도록 지속적으로 감시하는 단계이다. 최근 기술이 진화하고 있는 지능형 CCTV, 드론, 초소형 로봇, 그 밖의 다양한 IoT 센서 장비를 이용하면, 수집된 다양한 데이터(영상)를 기반으로 실시간 테러 진행사항을 파악할 수 있다. 또한, 이러한 정보를 인공지능 기술로 분석하면 상황에 대해서 신속하고 정확하게 판단할 수 있으며, 빅데이터로 축적하면 현실적이고 경험적인 테러 정보를 쌓을 수 있다. 그리고 대테러 대응관련 조직의 감시/통제 시스템을 해킹하여 테러 대응 활동을 감시하거나 시스템을 마비시켜 대테러 활동을 지연시키고 혼란을 초래할 수 있다. 이는 기존의 정보통신기술로는 어려웠던 일이지만, 4차 산업혁명기술의 발전으로 이를 가능케 하고 있다.

테러 과정 단계별 첨단 정보통신기술의 악용하는 현황을 요약하면 다음 표와 같다.

<표 3> 테러 단계별 첨단 정보통신기술의 악용

단계	활동	첨단 정보통신기술 악용
준비 단계	홍보	웹사이트(유튜브, 페이스북 등) 동영상, 포스터 게재, 이메일 전송 등
	모집	소셜 네트워크 플랫폼을 통해 모집 활동
	자금 조달	다크웹 사이트 불법 거래 크라우드 펀딩 랜섬웨어 공격으로 금전 요구 지능형 해킹으로 자금 불법 인출
정보 수집 /공유 단계	수집	고해상 카메라 장착 드론 이용 영상 정보 획득 웹사이트 제공하는 인공위성 영상 활용 주변 CCTV 해킹으로 주변 정찰
	공유	앱이나 메일을 통한 암호화 통신
수단 /방식 선택 단계	제작	다크웹 등에서 제작 정보 습득 3D 프린터로 제작
	방식 선택	첨단 시뮬레이션과 인공지능 기술이 적용된 의사결정 시스템을 통해 방식 선택

모의 훈련 단계	모의 훈련	3D 모델링 기술 활용하여 목표물과 주변 환경 묘사 VR/AR 기술 활용한 가상 훈련 시스템을 이용한 모의 훈련
실행 단계	진행 사항 파악	스마트 CCTV, 드론, 초소형 로봇, 그 밖의 다양한 IoT 센서 장비를 활용한 실시간 테러 진행 사항 파악 지능형 해킹으로 주변 CCTV 화면 감시 및 대테러 운영 시스템 사용 지연

4차 산업혁명의 핵심기술이 테러의 전 과정에서 활용되는 만큼 이에 대한 대비가 시급하다. 최근에는 여러 대의 드론을 활용하여 공격하는 스웜 전술까지 나타나고 있으며, 3D 프린트로 제작된 총기류에 의한 살상도 증가하고 있다. 이렇게 진화되고 있는 테러 양상에 대비할 수 있는 대응 기술 개발, 방호체계 개선, 법/제도 개선이 필요하다. 특히, 인공지능이 탑재된 드론이나 로봇, 전파교란 및 해킹 등은 일단 발생하면 엄청난 피해가 발생할 수 있기 때문에 단계적 심층 방어체계로 방호체계를 구축하여 예방 및 억제 단계에서 공격 진행이 이루어지지 못하게 해야 한다.

Ⅴ. 결론

제4차 산업혁명시대에 발생 가능한 테러는 기존의 테러 수단과 방식을 벗어나 최첨단 테러 수단과 정교한 테러 시나리오에 의해서 감행될 것으로 보인다. 4차 산업혁명기술 중의 첨단 정보통신기술이 테러 준비단계부터 실행단계까지 모든 과정에 적용됨으로써 테러 공격 대상이 광범위하게 선정할 수 있으며, 테러 수단을 쉽게 제작할 수 있으며, 신속하게 이동시킬 수 있다. 또한, 테러 방식도 수동적으로 진행하는 것이 아니라 치밀하게 계획하고 은밀하게 실행할 수 있다. 특히, 지능형 해킹 도구를 활용하여 테러 실행 이후에 대테러 관련 조직이 추적하지 못하도록 흔적을 지울 수 있으며, 대테러 시스템을 사용하지 못하도록 하는 사이버테러와 물리적 테러가 융/복합 형태의 지능형 테러도 발생할 수 있다.

4차 산업혁명시대의 테러 양상은 포스트 IS 시대의 테러 양상에 비해 크게 변화하지는 않겠지만, 첨단 정보통신기술을 악용함으로써 테러 수단 제작과 획득의 용이성, 테러 대상으로의 접근 편리성, 테러 방식의 정교화 및 은밀성, 테러 진행의 신속성, 피해효과의 증대, 추적 회피성, 테러 형태의 융복합화 등의 특징을 갖게 될 것이다. 그리고 이러한 이유로 인해서 잠재적 테러리스트들의 테러 감행을 부추기게 될 것이다.

테러에 첨단 정보통신기술이 악용되는 현황을 테러 단계별로 제시함으로써 대테러 기술 개발과 대응 전략을 수립할 때 참고할 수 있다. 특히, 첨단 정보통신기술이 융합되거나 복합된 기술의 악용은 대테러 활동 영역을 넓히게 되기 때문에 보다 포괄적이고 기술적인 대테러 체계를 구축해야 한다. 향후에 본 연구 결과를 기반으로 첨단 정보통신기술이 적용된 테러 수단별 탐지, 차단, 무력화할 수 있는 대응 기술 개발 관련 연구를 진행할 것이다. 또한, 현재의 테러 방호체계의 개선점을 도출하여 지능화된 테러 공격을 효과적으로 방어하기 위한 단계적 심층 방어체계에 대해서도 연구할 계획이다.

참고문헌

[1] 윤민우, “최근 국/내외 테러 동향과 테러공격 방법에 대한 분석,” 경찰학논총, 제9권, 제3호, 2014, pp.221-249.

[2] 정병수, “드론 테러의 사례 분석 및 효율적 대응 방안,” 경찰학논총, 제14권, 제2호, 2019, pp.147-176.

[3] 박보라, “사우디에서 드러난 드론테러의 위협,” 국가안보전략연구원 이슈브리핑, 제151호, 2019,

pp.1-5.
[4] 윤경배 외 17명, 4차 산업혁명의 이해, 일진사, 서울시, 2021. p.344.
[5] 김인철·조재한·김한흰, 4차 산업혁명 핵심기술과 기업활용에 관한 연구, 산업연구원, 세종시, 2019, p.82.
[6] 오세연, "자국 내 테러발생 요인 및 테러사건의 특성분석을 통한 테러발생 위험 가능성에 관한 연구," 한국융합과학회지, 제7권, 제3호, 2018, pp.112-120.
[7] 윤해성, 사이버 테러의 동향과 대응 방안에 관한 연구, 한국형사정책연구원, 서울시, 2012, p.333.
[8] 함중영·장정현, "테러조직의 인터넷과 소셜 미디어 활용전략 분석 및 대응방안 연구," 국가정보연구, 제12권, 제2호, 2019, pp.5-53.
[9] 이진·강소영, "뉴테러리즘의 최근 양상과 유형 분석," 한국범죄심리연구, 제15권, 제3호, 2019, pp.173-190.
[10] 이만종, "인공지능을 악용한 테러 가능성과 대응 전략," 경찰학논총, 제12권, 제1호, 2017, pp.193-220.
[11] 김원규 외 다수, 저고도 소형드론 식별/주파수 운용요구 및 제도 개선 사항 도출 연구, 국립전파연구원, 나주시, 2019, p.204.
[12] 나성후 외 3명, 군수품 수송용 드론 OMS/MP 연구, 육군본부, 계룡시, 2017, p.160.
[13] "ICT 융합 동향 리포트: 인공지능 킬러로봇지대 개막, 우리에게 릴러로봇은?," 정보통신산업진흥원, 융합동향 2018—1호, 2018, pp.6-8.
[14] [무기와 표적] 미국의 골칫거리 고스트건, https://www.hankookilbo.com/News/Read/201911281545384433.
[15] 황선한, "GPS 전파교간 동향 및 대응 기술," 정보통신기술진흥센터, 주간기술동향, 2018, pp.14-24.
[16] 국경완, "인공지능 기술 및 산업 분야별 적용 사례," 정보통신기획평가원 주간기술동향, 2019, pp.15-27.
[17] 테러도 AI가 하는 세상, https://news.joins.com/article/23931580.
[18] 김남욱·엄정호, "A Situation-Flexible and Action-Oriented Cyber Response Mechanism against Intelligent Cyber Attack," 디지털산업정보학회 논문지, 제16권, 제3호, 2020, pp.69-80.
[19] 김남욱·엄정호, "APT 공격 탐지를 위한 공격 경로 및 의도 인지 시스템," 디지털산업정보학회 논문지, 제16권, 제1호, 2020, pp.67-78.

■ 저자소개 ■

심 세 현
Sim, Se-Hyeon

22020년 9월~ 현재 대전대학교 안보융합학과 조교수
2015년 2월 중앙대학교 정치외교학과(박사)
2008년 8월 중앙대학교 정치외교학과(석사)
2004년 2월 대구대학교 영어영문학과(학사)
국제관계학과(학사)
관심분야 : 국가(국방)안보, 한국정치(한미동맹, 자주국방), 복합안보
E-mail : shsim@dju.kr

엄 정 호
Eom, Jung Ho

2011년 3월~ 현재 대전대학교 군사학과&안보융합학과 부교수
2011년 3월 성균관대학교 정보통신공학부 BK21 연구교수
2008년 2월 성균관대학교 컴퓨터공학과(박사)
2003년 2월 성균관대학교 컴퓨터공학과(석사)
1994년 2월 공군사관학교 항공공학과(학사)

관심분야 : 네트워크/시스템 보안, 사이버전, 내부자보안, 4차 산업혁명기술
E-mail : eomhun@gmail.com

논 문 접 수 일 : 2021년 1월 22일
수 정 일(1차): 2021년 2월 17일
수 정 일(2차): 2021년 2월 25일
게 재 확 정 일 : 2021년 3월 3일