미래전 수행을 위한 국방정보보호 구축 및 발전방안

윤지원*

Ⅰ. 미래전 수행을 위한 국내외 이슈 및 동향 분석
Ⅱ. 국방정보보호 구축 및 발전방안 모색

요 약

본 보고서는 미래전 수행을 위한 국방정보보호에 대한 이슈에 대해서 기술동향과 향후 발전방향에 대해서 다룬다. 이와 관련하여 크게 두 개의 장으로 이루어지며 제 1장은 미래전 수행을 위한 국내외 이슈 및 기술동향분석이 주를 이룬다.

1장에서는 크게 세부적으로 3개의 절로 나누어서 미래전에 대한 개념과 미래전에서의 작전개념들을 살핀다. 이때 본 논문에서는 네트워크 중심 작전(Network Centric Warfare)에 대해서 주로 언급하면서 신속한 지휘통제를 위한 작전개념이 사이버공간상에서 복잡도가 증가하면서 발생하는 사이버 위협이 존재함을 언급한다. 이러한 사이버공간에서의 위협은 미래전에서 가장 큰 이슈가 될 수 있고 이것이 바로 사이버전으로의 연결 가능성을 보인다. 미래전으로서의 사이버전의 중요성을 언급한 후에 어떤 종류의 미래의 사이버공간상의 위협이 존재할 수 있는지 위협요소를 보였다. 다양한 악성코드의 시간에 따르는 위협 변화와 함께 위협 수준을 살펴보고 가장 현재와 미래의 군 네트워크에 가장 큰 피해를 입힐 수 있는 두 가지 유형의 악성코드를 살펴본다. 그 첫 번째 악성코드는 지능형 지속 위협 (APT)공격이다. 국방에서 APT공격은 아주 주의 깊게 접근해야 한다. 그 이유는 국방에서 일어날 수 있는 공격의 대다수가 APT공격일 가능성이 높기 때문이다. 일반적으로 APT공격은 고도의 기술력을 갖춘 해킹 조직이 치밀하게 준비해서 정해진 타켓을 장기간에 걸쳐 다양한 우회기술을 통해 타겟이 인지 못하도록 하여 공격하는 방식이므로 적국이나 국방에 해를 끼치고자

* 고려대학교

하는 조직에 의해서 이용될 가장 적합한 사이버위협 유형이다. 또다른 악성코드 유형은 최근에 사회적 이슈를 낳고 있는 랜섬웨어이다. 랜섬웨어는 APT공격과 달리 금전적인 요구를 목적으로 한다는 점에서 차이를 두고 금전적인 요구가 직접적으로 국방과 관련이 없어 보이지만, APT공격과 달리 국방시스템이 랜섬웨어의 공격을 받을 경우 모든 시스템이 암호화되거나 유실됨으로서 APT공격보다 더 큰 피해를 야기할 수 있으므로 이 악성코드 유형 역시 주의 깊게 관찰되어야 한다. 이러하듯 국방정보보호관점에서 중요한 두 가지 악성코드의 특징을 알아본 후 다양한 악성코드에 의해서 국내외적으로 발생한 사이버 테러 관련 사건사고들을 살펴보았다. 이러한 악성코드의 특징과 사건사고를 살펴봄으로서 현재 운용중인 악성코드 등의 사이버위협에 대한 대응의 한계와 그 해결방안에 대해 살펴본다. 그리고 1장을 마무리 함에 앞서 미래전 수행을 위한 국방정보보호의 국내외 기술동향 분석을 수행하였다. 이를 위해서 UN에서 미래전 수행을 위한 국방정보보호를 어떻게 진행하고 있는지를 기술한 뒤 미국의 국방 연구를 담당하고 있는 DARPA에서 최근에 수행했거나 수행하고 있는 다양한 미래전 수행을 위한 국방정보보호 기술들을 설명하였다.

1장이 미래전 수행을 위한 국내외 이슈 및 기술 동향이었다면 2장은 국방정보보호 구축 및 발전방안 모색으로 1장보다 보다 현실적인 문제를 언급하고 새로운 방안을 제안하는데 그 초점을 두었다. 2장은 크게 두 개의 절로 이루어져 있다. 1절은 인공지능 기반 미래전을 수행하기 위한 국방정보보호 기술이고 2절에서는 OSINT기반 미래전을 수행하기 위한 국방정보보호 기술을 언급한다. 우선 즉, 1절과 2절의 핵심단어는 인공지능과 공개정보분석(OSINT)이다. 우선 1절에서는 인공지능이 결코 새로운 단어가 아니지만, 최근의 주된 이슈로 떠오르는 자동취약점 분석과의 오해와 그 관련성을 살펴본다. 보다 정확한 관련성을 살펴보고 또한 인공지능 기술이 국방 기술에 어떻게 사용될수 있을지를 논하기 위해서 인공지능에 대한 정의와 인공지능의 미래를 살펴본다. 인공지능에 대한 분류와 정의를 마친후 실질적으로 사이버보안에 사용되었던 인공지능 응용사례가 어떠한 것들이 존재했는지를 알아보고 이와 함께 자동취약점 분석이 어떻게 인공지능과 엮어질 수 있는지를 알아본다. 마지막으로 인공지능의 기술적 설명을 마친 후에 국방정보보호 개념에서 보다 능동적으로 복잡한 환경에서 중요 정보를 획득할수 있는 방법인 공개정보분석(OSINT) 기술에 대해서 개념에서부터 현재 영국과 미국과 같은 정보선진국에서 진행하는 각종 프로젝트들과 수집에서 분석에 이르는 일련의 과정을 설명한다. 이후 공개정보로써 익명네트워크인 Tor의 유용성을 알아보고 마지막으로 국방정보보호를 위해서 두 가지의 OSINT활용 방안을 모색한다.

- OSINT를 이용한 악성코드나 악성코드 개발자들에 대한 프로파일링 기술 구축
- OSINT를 이용한 세계정세 파악 및 국내 사건사고 신속 대응 및 예측 시스템 구축

Ⅰ. 미래전 수행을 위한 국내외 이슈 및 동향 분석

제1절 미래전과 사이버전

1. 미래전과 작전 개념들

미래전이라 함은 미래에 닥칠 전쟁을 의미한다. 미래전 수행을 위한 대응 및 대책은 미래전장의 모습을 예측함으로서 가능하다. 미래전장의 모습은 군내 작전개념의 변화와 과학기술의 진보에 의해서 시간에 따라 변화하고 있다. 즉, 미래전장의 모습을 예측함에 있어서 군은 전장에서 작전을 수립하고 그 작전을 실제로 가능하게 만드는 무기 체계 소요를 제기한 후 그 시기의 과학기술의 뒷받침아래 해당 무기체계와 무기들을 개발한다.[1]

이러한 관점에서 전장에서 작전을 수립하기 위한 작년 개념이 미래전을 위해서 새롭게 요구되어 왔다. 최근 들어서 전장의 효율성을 높이기 위해서 아래와 같은 다양한 작전 개념들이 도입되었다.

- 네트워크 중심 작전 (Network-centric Warfare, NCW)
- 효과 기반 작전 (Effects Based Operations)
- 신속 결정 작전 (Rapid Decisive Operations)

이러한 신개념 기반 작전들은 효율성 극대화라는 측면에서, 빠른 공격, 정확한 목표물 파악과 그리고 신속한 정보 전파 및 판단이라는 세 가지 요소를 공통분모로 두고 있다는 점에서 기존의 작전들과 차이점을 둔다. 이 중에서 미래전에 가장 가까운 작전 개념으로 네트워크 중심 작전 (NCW)를 둘 수 있다. NCW는 네트워크를 활용한 작전 수행방식으로 무기체계 중심으로 이루어지는 과거의 플랫폼 중심 작전(Platform Centric Warfare, PCW)에서 전쟁의 개념을 탐지, 식별 및 추적체계에 이르는 영역을 담당하는 센서(sensor)들과 결정권자 (Decision maker)그리고 타격체계(Shooter)를 네트워크로 연결함으로서 동시간대에 신속한 작전지휘 및 통제 능력을 효율적으로 높이는 새로운 작전개념으로 1998년 도입된 작전개념이다. 미군은 군사변혁을 위하여 네트워크 작전 (Network Operations)이라는 교리를 정립하고 이를 네트워크 중심작전을 수행하기 위한 중요한 군사적 작전으로 인식하여 이미 합동작전 개념서에 포함하였으며 연합사내에 연합 합동 네트워크 작전 통제센터 (Combined Joint Network operation Control Center)를 설치하였다. 한국군의 경우도 미래전에서의 네트워크 중심전이 차지하고 있는 중요성을 인식해왔다고 볼 수 있다. 예를 들어 합동전술데이터링크, 광대역 광통신망, 차기전술통신체계, 위성통신체계 등의 네트

워크 중심 작전 수행에 용이한 환경을 구축해왔다. 이러한 네트워크 중심작전이 지휘통제의 효율성과 신속성을 극대화하는데 그 목적을 두고 있다. 그러한 면에서 과학기술의 뒷받침은 최신 작전개념의 현실화에 있어서 중요하다. 핵이 개발되면서 핵에 대한 전장기술이 뒷받침되었고 네트워크와 각종 센서들의 네트워크 환경기술이 뒷받침되면서 실질적인 네트워크 중심 작전역시 가능해졌다. 다시 정리하자면, 미래전쟁의 모습은 두 가지 요소에 의하여 예측 가능하다. 그 하나는 작전수립에 따르는 무기 체계 수요 제기이고 나머지 하나는 기술적으로 현실화할 수 있는 과학기술의 지원 가능성이다.

2. 미래전에서의 사이버전의 중요성

미래 전에 대해서 다양한 각도와 다양한 토픽이 존재할 수 있다. 하지만, 본 과제에서는 전 세계적으로 이슈가 되고 있는 사이버공간의 미래전인 사이버전에 대한 이슈와 이에 대한 국방정보보호이슈를 주로 다루고자 한다.

이러한 복잡한 연결성이 존재하는 인터넷이라는 사이버공간이 기존에 존재하지 않던 새로운 공간이 형성되었다. 즉, 인터넷이라는 거대한 네트워크로 연결되어 있음으로 인해 공간적이거나 시간적인 제약이 더 이상 존재하지 않게 되었다. 최근 들어서는 사물인터넷(Internet of Things)이라는 기존의 연결시스템의 복잡도를 넘어서는 초연결사회로 이동하고 있다. 이러한 초연결 사회에서 더욱더 중요해지고 주목받고 있는 것이 바로 사이버공간에서의 발생하는 다양한 사회적 이슈이다. 이러한 사이버공간은 기존의 물리적 공간과 그 태생부터 성격이 분명이 다르다. 그렇기에 기존의 물리적이거나 시공간적 공간에서 존재하던 위협과는 사뭇 다른 종류의 위협이 사이버 공간에서 역시 존재한다. 예를 들어, 기존에는 사이버공간이 아닌 각 개인의 제한된 공간이었던 단말기(Terminal)나 호스트단(host)에서만 존재하던 정적인 악성코드들이 초연결 네트워크상에 이동하고 확산 및 재생산되면서 증식가능하고 손쉽게 확산되며 사이버공간의 특성을 이용한 새로운 공격양상이 보여지며 다양한 위협이 사이버 공간상에 존재하고 있다. 이러한 사이버 공간의 도입과 함께 발생되어 온 위협 변화에 대해서 기민하게 움직이고 있는 것은 인터넷이라는 공개된 네트워크에 맞물려있는 민간에서 보다 활발히 이러한 위협을 탐지, 식별 예방 처치에 이르는 다양한 노력이 이루어지고 있다.

본 과제에서 주목해야하는 부분은 이러한 초연결 사회에서 발생한 사이버공간에서의 위협이 단순히 인터넷을 사용하고 있는 민간에서만 발생하는 문제로 치부할 수 없다는 점이다. 군에서도 역시 해당 문제는 충분히 존재 가능하다. 이러한 문제에 대해서는 다양한 이유가 존재한다.

1) 이미 군 내부의 인트라넷 환경역시 복잡도가 충분히 높기에 관리의 문제점과 취약점이 그 복잡도와 함께 비례적으로 증가한다.
2) 군내에서 운용하고 있는 다양한 장비들이 민간에서 개발되었던 장비들이다.
3) 운용상의 편의성을 위해서 군내의 Intranet과 외부 Internet망과의 접점 지역이 존재한다는 점이다.

우선 군 내부의 인트라넷의 높은 복잡도와의 연결성을 살펴보자. 이것은 현재 군이 추구하는 네트워크 중심작전으로 지휘통제의 효유성을 높이기 위해서 지속적으로 복잡도가 높여온 것에 기반한다. 즉, 군의 인트라넷 환경 내에서 각종 센서와 장비들이 네트워크 중심작전을 이루기 위해서 서로 복잡하게 물려있기 때문이다. 이러한 군내부의 장비들간 복잡한 연결은 지휘 통제의 신속성과 효율성을 극대화하기 위하여 필요 불가결할 수 있다. 하지만, 효율성의 극대화는 동시에 시스템의 안정성과 안전성이나 정보보호 이슈를 야기할 수 있다. 왜냐하면 군네트워크로 연결된 내부망(Intranet) 환경이 이미 사이버공간이기 때문이며 이러한 군사이버 공간에서도 악성코드나 DDoS 문제와 같은 다양한 문제들이 발생가능하기 때문이다.

또 다른 이유로는 군내에서 운용하고 있는 다양한 장비들이 민간에서 개발되었던 기술들 바탕위에서 만들어졌다는 사실이 군의 사이버공간상의 위협에 대한 우려이다. 기존의 기계장비나 전자장비에 비해서 컴퓨터장비와 소프트웨어들은 해마다 그 발전 속도가 빠르다. 이러한 급속하게 발전하는 특징 때문에 군 내부의 노력에 의해서 개발되기보단 민간에서 주로 연구되고 개발되었다. 이러한 이유로 민간에서 개발된 다양한 사이버방어기술이 군내부로 유입되게 되었다. 하지만, 이러한 이유로 민간의 특징과 약점이 군내부에 그대로 이어질 수 밖에 없다. 즉, 민간기술의 약점은 이미 민간에 존재하는 해커들에게도 공유될 수 있기에 언제든 군의 장비와 소프트웨어 시스템에 위협이 될 수 있다.

또한 단절되었다고 여겨지는 내부망과 외부망이 종종 운용의 편이성 때문에 강제로 연결함으로서 또한 이러한 문제들이 발생가능하다. 내부망(Intranet)과 외부망(Internet)을 분리시킴으로서 공공기관이나 중요시설에 대한 보호를 망분리를 통해서 이룰수 있다. 일반적으로 악성코드들이 인터넷 망을 통해서 유입되는 사례가 많기에 효과적인 기술이라고 볼수 있다. 하지만, 문제는 망분리를 시켜서 악성코드의 유입을 막을순 있으나 개발환경이나 서비스 제공에서 제약을 갖게 된다. 이러한 이유로 특이한 상황을 고려한 망연계 작업이 분리된 망분리 시스템에 한시적으로 또는 영구적으로 추가적으로 수행된다. 하지만, 이러한 망연계 과정은 본래의 망분리 작업의 취지에서는 벗어나는 과정이다. 이러한 다양한 이유로 인해 군의 시설과 사이버공간은 다수의 공격을 당해왔다. 이와 관련하여 기존에 보고된 다양한 사이버 공격사례들은 아래와 같다. [11]

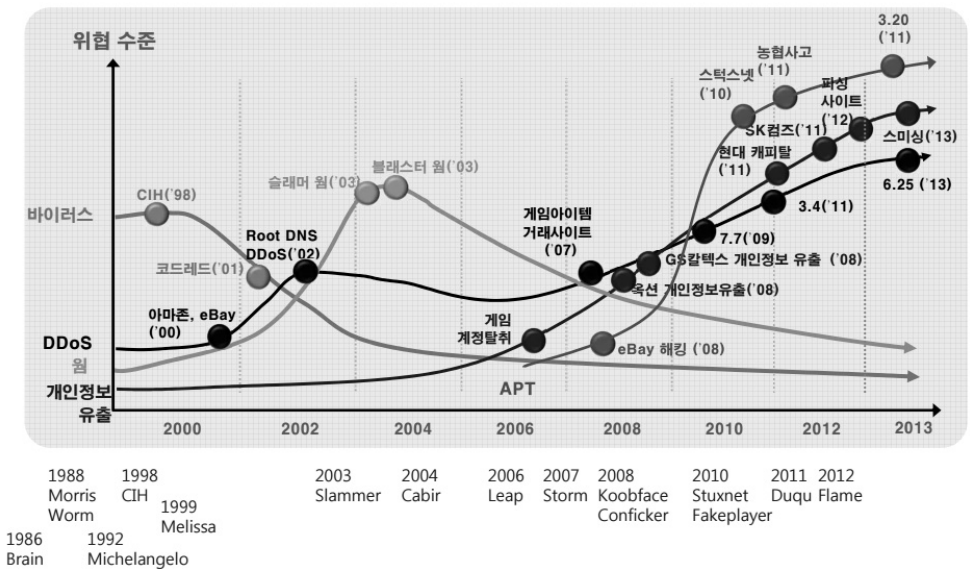
제2절 사이버공간상의 미래전 관련 국내외 이슈

1. 사이버전과 악성코드

1.1. 사이버공간의 위협요소인 악성코드

특히 아래 그림은 최근의 시대별 악성코드와 사이버 공간상의 위협들의 트랜드를 보인다. 아래 그림에서 볼 수 있듯이, 바이러스와 웜은 각각 2000년, 2004년에 가장 극렬하게 사이버공간에서 위협요소로 있다가 차차 그 위협수준이 감소되어가고 있는 것을 확인할 수 있다. 하지만, 2006년경에 나왔던 APT공격은 다른 어느 위협유형들보다 급격하게 그 위협수준이 증가하고 있다. 특히, APT공격은 일개 개인이 아닌 정부기관이나 스카다 같은 국가 인프라 시스템에 대한 정보 수집 및 시스템 파괴에 목적을 둠으로 그 어느 위협보다 더 치명적이라고 말할 수 있다.

시대별 공격 변화 : 최근 APT 공격의 증가 (출처 : KISA)



1.2. 지능형지속위협(APT)

최근의 사이버공간상의 위협중 가장 큰 위협중 하나는 지능형 지속 위협 (APT)이다. 용어의 이름 그대로 오랜 기간 특정 타켓을 대상으로 은닉형으로 악성코드를 이용하여 적 시스템을 공격을 하거나 중요 정보를 탈취하는데 그 목적을 두는 사이버 공간상의 표적 공격 유형 중 하나이다.

이러한 지능형 지속 위협에 대한 다양한 보안기업들의 정의를 잠시 살펴보면 아래와 같다.

- IBM: 특정대상의 기밀정보를 탈취하거나 또는 정치적 목적을 위해서 최신의 복합적인 공격 기법을 사용하는 형태의 일련의 공격이다.
- Symantec: 드라이브 바이 다운로드(Drive-by Download), Microsfot SQL인젝션, 악성코드, 스파이웨어, 피싱, 스팸을 포함한 다양한 기법을 활용하여 특정 타겟을 공격하는 표적 공격이다.
- McAfee: 다양한 탐지우회 기술을 이용하여 장기간에 걸쳐서 특정 조직이나 혹은 사용자의 중요한 자산을 비밀리에 탈취하는데 그 목적을 두고 수행되는 공격이다.

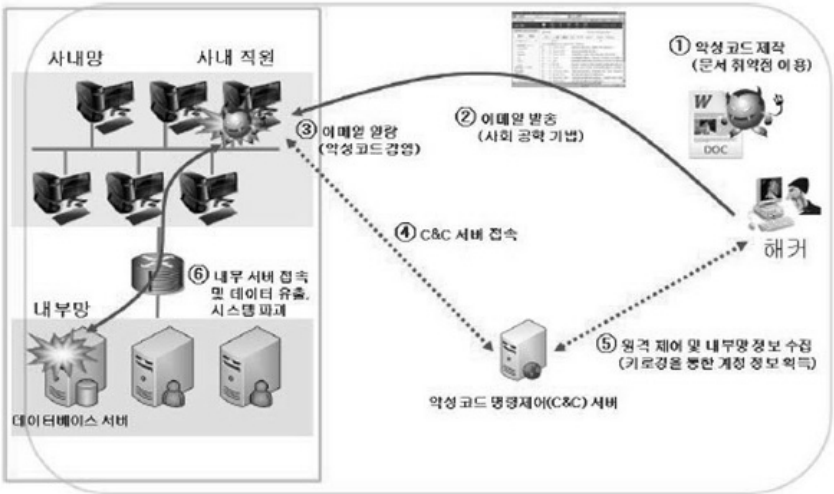
즉, 지능형 지속 위협은 기존의 불특정다수를 타겟으로 주로 금전적 목적을 두는 단순 공격성 악성코드와 여러 가지 차이점을 두고 있다.

* 지능형 지속 위협(APT) 악성코드들의 특징[3]

1) 커스터마이즈된 공격: 특정 타겟에 대해서 표적형 공격이다.
2) 장기간에 걸쳐 비밀리에 진행되는 공격: 오랜기간에 걸쳐 수행되며 공격자는 은닉형으로 잠입하여 공격을 수행하므로 사이버 범죄의 대부분들이 표적공격에서 사용하는 돌파식 전술과 달리 APT의 목표는 공격자가 목적을 달성할 때까지 비밀리에 수행하는 특징을 갖는 공격이다.
3) 정부기관 또는 공공 시설 공격: 신속하게 경제적 이익을 추구하는 일반적인 표적공격과 달리 APT는 국제적인 정보 수집 또는 파괴활동을 하기 위해서 국가 비밀 세력들에 의해 운용되곤 한다. 일반적으로 APT 조직적으로 국가나 특정 조직이 배후세력으로 존재하여 공격주체를 지원하는 경향이 있다.
4) 탐지를 우회하기 위한 다양한 기법을 포함하고 있다.

위의 4가지 APT공격의 특징을 살펴보면 알 수 있듯이, APT공격은 특정 타겟에 대해서 고도화된 기술을 보유한 적대 세력에 의해서 운용 가능한 공격기술로서 적국에 의해서 이용될 때 우리 군에게 가장 위협적인 공격방법이 될 수 있다.

APT공격 유형 (출처: 블루투데이[12])



1.3. 랜섬웨어 (Ransomware)

1.3.1. 랜섬웨어 정의와 피해상황

최근에 사이버 공간에서 가장 큰 위협으로 알려지고 있는 악성코드는 바로 랜섬웨어이다. 랜섬웨어란 몸값(Ransome)과 소프트웨어(Software)의 합성어로 시스템을 잠그거나 시스템내의 데이터를 암호화함으로서 사용자가 해당 시스템이나 데이터를 사용할 수 없도록 아래와 그림과 같이 인질화함으로서 금전을 요구하는 악성 프로그램이다.

랜섬웨어 감염화면 (출처: 안철수연구소 [9])

금전적 목적을 갖는 이러한 랜섬웨어는 그 목적을 이루기 위해서 개인사용자와 기업들을 두로 타겟으로 삼고 있다. 시멘텍(Symantec)의 자료에 의하면 랜섬웨어에 감염된 개인사용자와 기업대상의 2015년 1월부터 2016년 4월까지 통계치로 볼 때 사용자의 감염사례가 57%인 반면 기업대상의 감염이 43%에 이른다.

좀 더 자세히 랜섬웨어의 피해상황을 살펴본다면 FBI의 문서에 의하면 2015년에 2400여 건의 랜섬웨어가 접수되었으며 그 손실액이 미국에서만 300억가량이 된다고 밝히고 있다. 특히 랜섬웨어의 피해산업군을 보면 아래와 같이 인터넷 서비스와의 통합과 접촉이 많은 기업일수록 감염 위험에 대한 노출정도가 증가함을 볼 수 있다.

랜섬웨어 피해 산업군 (출처: 시멘텍)

서비스	제조업	정부/공공기관	금융/보험/부동산	도매유통	운송/통신	소매유통	건설	광업	농업/임업/수산업
37.8%	17.2%	10.2%	9.8%	8.9%	6.6%	4.3%	3.9%	1.0%	0.5%

1.3.2. 랜섬웨어의 감염경로

이러한 랜섬웨어는 여러 가지의 경로에 의해서 감염이 되고 있는데 이 역시 일종의 악성코드 이므로 기존의 악성코드들의 감염경로와 일치하고 있다. KISA에서 구분한 세 가지 주요 감염경로는 아래와 같다[6].

1) 신뢰할 수 없는 사이트를 통한 감염: 신뢰할 수 없는 사이트를 방문함으로서 랜섬웨어에 감염될 수 있으며, 드라이브 바이 다운로드(drive-by-download)[1] 기법을 통해 유포된다.
2) 스팸 메일을 통한 감염: 출처가 확실치 않은 이메일을 수신하여 해당 이메일에 첨부되어 있는 파일이나 URL link를 클릭하는 부주의를 통해서 감염된다.
3) 파일 공유 사이트를 통한 감염: 토렌토와 같은 p2p 사이트를 통해서 동영상 등의 파일을 다운로드 받을 때 감염된다.

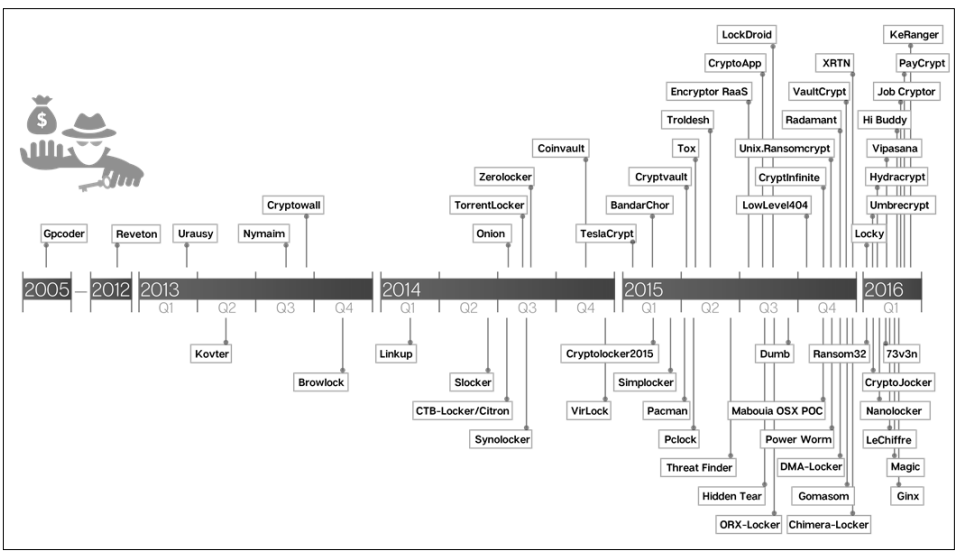
[1] Drive-by-Download 는 취약한 웹사이트를 방문하였을 뿐인데 사용자도 모르게 악성 스크립트가 실행되어 취약점을 유발시키는 코드를 비밀리에 실행하여 악성코드를 자동으로 다운로드하도록 하는 악성코드 감염 방식이다.

랜섬웨어의 감염 (출처: 안철수연구소 랜섬웨어 보안센터)

1.3.3. 랜섬웨어 패밀리

지금까지 다양한 랜섬웨어들이 사이버 공간에서 위협이 되어 왔다. 2005년 GPcoder부터 사실상의 랜섬웨어가 시작된 이후 최근 들어 그 수와 위협수준이 높아지고 있다. 아래 그림은 해당 랜섬웨어 패밀리를 나타낸다. 랜섬웨어 패밀리 그래프를 보면 알 수 있듯이 시간이 흐름에 따라 보다 다양한 랜섬웨어들이 창궐하고 있음을 알 수 있다. 시만텍(Symantec Corporation)에 따르면 2015년 신규로 발생된 랜섬웨어만 100개의 패밀리가 있으며 2016년 발생된 랜섬웨어 중 단 1개를 제외하고는 모두 크립토 랜섬웨어라는 점이다

2016년 4월까지의 랜섬웨어 패밀리: 시간이 흐름에 따라 보다 다양한 랜섬웨어들이 창궐하고 있다. (출처: 시멘텍)



이 중 대표적인 3가지 주요 랜섬웨어는 록키(Locky), 크립트XXX (CryptXXX), 케르베르(CERBER)를 둘 수 있다. 좀 더 해당 랜섬웨어들을 알아보면 아래와 같다.

1) 록키 (Locky): Locky는 2016년 3월 이후에 이메일을 통해서 유포가 되고 있으며 사회공학(Social Engineering)[7]적 공격으로 수신인을 속이기 위해서 청구서(Invoice)나 환불(Refund)등의 제목을 이용하여 사용자의 PC로 침투한다. 이 랜섬웨어는 이렇게 침투를 함으로서 자바 스크립트(Java script)파일이 들어있는 압축 파일들을 첨부하고 이를 실행시 랜섬웨어에 감염되도록 한다. 특히, Locky 랜섬웨어에 감염되면 모든 파일들이 암호화되며 확장자가 .locky로 변하고 바탕화면이 복구관련 메시지들이 아래 그림에서처럼 보여진다.

Locky Ransomware 팝업창 (출처: 보안뉴스 [8])

2) 크립트XXX (CryptXXX) : 크립트XXX는 2016년 5월에 해외 백신 회사의 복호화 툴 공개 이후에 취약한 암호화 방식을 보완한 크립트XXX3.0이 유포되었으며 이 랜섬웨어에 감염되면 파일의 확장자가 .crypt등으로 변하고 바탕화면 복구안내 메시지가 변경된다. 특히 크립트XXX는 아래의 그림에서 볼수 있듯이, 한글화된 번역을 제공하여 비트코인 지불 안내 페이지를 통해 금전요구를 하며 네트워크 연결없이도 파일들을 암호화하는 기능을 갖는다.

크립트XXX 랜섬웨어의 메시지 (출처: ZDNet Korea)

3) 케르베르(CERBER) : CERBER역시 악성코드들과 유사하게 웹사이트 방문시 취약점을 통해 감염되며 감염즉시 파일을 암호화하고 확장자를 .cerver로 변경한다. 이역시 CryptXXX와 같이 네트워크가 연결되어 있지 않아도 파일 암호화가 가능하며 윈도우즈 쉐도우 (Windows Volume Shadow)를 삭제하여 윈도우 시스템 복구가 불가능하게 만든다.

2. 사이버전과 관련한 국내외 사건사고들

2.1. 국가 간의 이슈로 인한 사이버전 사고 사례

최근에 국가간 이해관계 및 정치적 갈등과 분쟁으로 인해 사이버전의 일환으로 국가기관에 대한 다양한 사이버 공격과 위협들이 발생하였다. 이스라엘과 팔레스타인 간 분쟁이 있었던 2000년 10월부터 2011년 1월 사이에 23개 국가에서 이스라엘에 대한 40여건의 사이버 공격을 시도하여 전자상거래와 국가기관의 서비스의 혼란과 파괴를 노리는 사이버 공격이 확인되었다. 또한 이란의 스카다(SCADA) 시스템 마비를 목표로 한 산업시설 공격용 악성코드인 스턱스넥(Stuxnet, 2010)의 공격도 있었다. 또한 2012년에는 중동지역 국가간의 사이버전을 위해서 제작하여 대규모로 컴퓨터들을 감염시킨 것으로 추정되는 플레임이 있었

으며 국내에서는 공중파 방송사 및 금융기관을 대상으로 한 사이버 테러로 전산망 및 국민들이 ATM 기계를 사용하지 못하는 등 국가안보를 위협하는 다양한 사이버 공격 사례가 있어왔다. 이러한 해외에서의 사이버전 관련 공격사례를 정리한 것이 아래의 표이다 [11].

사이버 공격 사례[11]

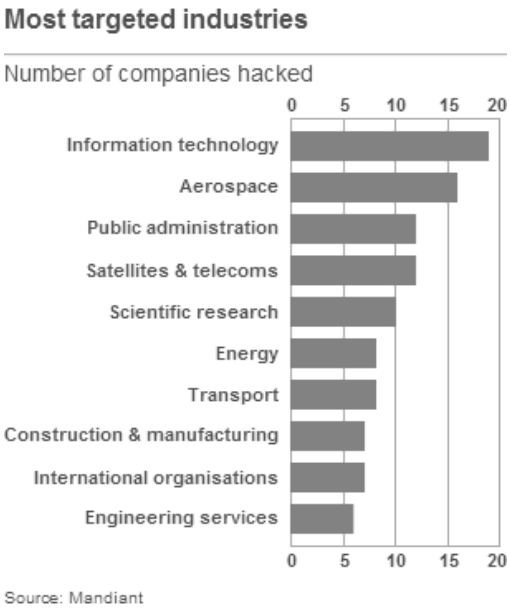
연 도	주 요 내 용
2004년	중국 해커, 한국 국방연구소, 외교부 등 웹사이트 집중 공격
2007년	러시아 해커, 에스토니아 정부, 언론, 방송, 금융전산망 집중 공격
	중국 해커, 미국 국방부 동아태국 집중 공격으로 초토화, 로버트 게이츠 국방장관 컴퓨터까지 침입
2008년	러시아 '러시아비즈니스네트워크' 사이버범죄 조직이 그루지아 대통령 홈페이지를 비롯한 의회/국방부/외교부 사이트에 대해 서비스 거부 공격 집중
	이스라엘-하마스 분쟁시 아랍권 해커집단 '팀 이블'이 이스라엘 일간지 와이네트 등 400개 이상의 사이트를 해킹·변조했으며, 이스라엘의 가자 침략 부도덕성을 선전하는 정치적 도구로 이용
2009년	16개국 86개 IP 이용 DDoS 공격으로 국가 주요 전산망 공격
	한/미 연합사 USB 저장 작계 5027 해킹으로 유출
2010년	스턱스넷을 이용하여 이란, 중국 등 국가 SCADA관련 시스템 감염
2011년	해외 70개국 746개 서버 이용 디도스 공격으로 10만여 대 PC 감염 * 09년 7월 7.7디도스 대란 공격 양상과 유사하나 진화된 DDoS 공격으로 평가
	DDoS 공격으로 농협 전산망 마비
	미군 시스템 개발 중이던 미 군수업체 컴퓨터 해킹으로 2만 여개의 파일 유출

2.2. 특정 조직이나 해커에 의한 사이버테러 사례

이러한 공격은 주로 국가나 조직간의 이해관계나 정치적인 이념 충돌에서 비롯되곤 한다. 그러한 면에서 최근에 일어나는 사이버전 위협은 지능형 지속 위협 (APT) 공격기술을 이용하여 많은 사건 사고가 발생하였다. 예를 들어, 1990년대 이후 해커들은 정치 이념을 내걸고 그들의 정치적인 색깔을 드러내었다. 자신들 정치적 이념에 반하는 정책을 집행하는 국가기관이나 정부기관에 대해서 사이버 테러들을 일으키곤 했다. 가장 대표적인 예로는 1993년에 발생한 포르투갈 해커들의 인도네시아 정부 웹사이트의 해킹 사례이다. 이들은 인도네시아의 동티모르 탄압에 대해서 반대하는 의사 표시로서 이러한 공격을 시도하였다. 또한 카슈미르의 해방을 지지하는 해커들이 인도정부의 웹사이트를 공격한 사례도 있었다. 가장 최근의 사례를 보자면 2015년 해커조직인 어나니머스가 파리 테러의 주범으로 알려진 이슬람국가(ISIS)를 상대로 사이버 공격을 개시하여 IS조직원 트위터 계정 5500여개 이상을 수집하여

폐쇄시키는 사건이 있었다. 이렇듯 최근에는 해커들이 정치적인 이념을 내세우며 정치적인 집단으로 움직이고 있는 것이 보이며 또한 동맹을 결성하여 조직적으로 행동하는 경향이 있다. 이렇듯 사이버 테러나 공격을 시도하는 국제적인 조직이 최근에 늘었으며 그중 국가단위로 지원 받고 운영되는 조직이 20여개로 파악되고 있다. 특히 중국의 61398부대로 알려진 특수부대는 미국 방위산업체인 록히드 마틴사를 해킹하여 스텔스 전투기를 개발하였으며 미국의 기술적 우위를 낮추는 결과를 초래하였다[4][5].

Mandiant사가 발표한 중국의 61398부대의 해킹 대상 추정 수



3. 기존 악성코드 탐지 기술의 한계, 그리고 해결 방향

악성코드를 탐지하는 기술로는 수집된 악성코드들의 특징을 분석하여 시그니처를 기반으로 탐지하는 기술, AV스캔으로 알려진 악성코드를 판정하거나 파일 헤더 및 바이너리 내 문자열을 분석하는 등의 정적 분석을 기반으로 하는 방법과 디버거를 통한 API 호출 관계 분석 등의 동적 분석 기반의 방법이 존재한다. 이외에도 최근에 연구된 방법들로는 행위기반 탐지 동적 콘텐츠분석, 클라우드를 이용한 평판 기반 탐지 등의 다양한 기술이 보안 솔루션 시장에 선보이고 있지만, 여전히 새로운 형태의 악성코드 탐지에는 취약하거나 정확도가 떨어지고 있다.

그러므로 악성코드를 보다 제대로 분석하기 위해서는 악성코드를 개발하는 집단에 대해서도 분석이 필요하다. 특히 최근에 정부기관이나 군으로의 위협이 될 수 있는 지능형지속 위협(APT) 악성코드 같은 경우 개인이 아니라 고도화된 기술력과 자본력을 갖춘 조직에 의해서 이루어지기 때문이다. 그러므로 악성코드 개발자나 해커들의 특성을 인지하고 공격대상이 되는 시스템의 취약점 및 전송경로로 사용되는 네트워크 등에 대한 이해와 함께 악성코드 분석이 이루어질 때 효과적인 수행능력을 얻을 수 있다.

특히, 3.20 전산 대란의 경우 해킹 공격에 활용된 IP의 소재지 추적을 통해서 북한 정찰총국의 소행으로 추정을 내리는 등 사이버 공격은 주로 IP추적이나 악성코드를 분석하여 추적이 가능하다. 하지만, 단순히 IP만을 이용하지 않고도 사이버 공격의 적 식별이 가능할 수 있다. 즉, 해킹을 위해서 개발된 악성코드의 코드 자체를 분석하는 방법을 갖고 공격주체 식별이 가능하다. 어떤 해킹 형태를 갖더라도, 개발자들은 편중화된 개발도구의 사용 및 코드의 일반적이고 전체적인 패턴은 유지하는 경향이 있기 때문에 코드의 패턴을 읽어들어 어느 해커집단에 의해서 개발되었는지를 가늠할 수 있다. 즉, 보다 효과적이고 효율적으로 악성코드를 분석하기 위해서 악성코드 개발자들의 코딩 패턴과 개발 패턴 등에 대한 프로파일링이 필요하다. 즉, 단순히 악성코드 자체를 분석하는 것만으로는 빠르게 발전하고 변화하는 악성코드에 기민하게 대응하는 것이 불가능하므로 악성코드가 생성되는 환경을 파악하고 네트워크와 시스템에서의 악성코드의 전주기적 분석과 SNS등을 이용한 국제 정세 변화에 따른 악성코드 변화의 흐름을 파악하는 보다 근본적인 연구가 필요하다. 이를 위해서 필요한 기술로 크게 사이버 프로파일링 기술과 함께 Open Source Intelligence (OSINT)기술을 이용하는 것이다. 사이버 프로파일링 기술과 OSINT기술에 대해 보다 상세한 내용은 다음 장에서 기술하고자 한다.

제3절 미래전 수행을 위한 국방정보보호의 국내외 기술 동향 분석

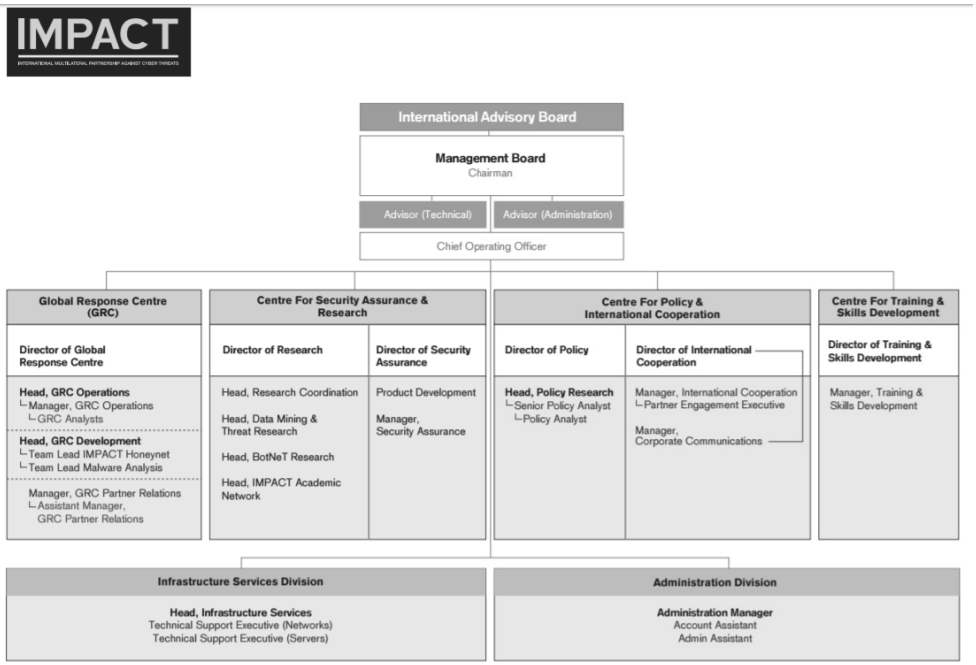
1. UN의 미래전 수행을 위한 국방정보보호

유럽은 우선 UN을 중심으로 2008년도에 국방 사이버 보안을 위한 국가간 협력강화를 위한 추진 기구인 국제 사이버보안 다자간 협력기구인 IMPACT(International Multilateral Partnetship Against Cyber Threats)[2]를 설립하였다. 본 기관은 그림 1)에 보이듯이 크게 4개의 분과로 나뉘어서 국제사회에 일어나는 사이버 위협에 대한 방어적인 연구에서부터 대응에까지 이른다.

---

2) IMPACT (International Multilateral Partnership Against Cyber Threats): www.impact-alliance.org/home/idex.html

UN의 국제 사이버보안 다자간 협력 기구 (IMPACT)의 4개 조직도



(출처: www.impact-alliance.org/home/idex.html)

IMPACT의 4개의 분과를 소개하면 아래와 같다.

1) Global Response Centre (국제 대응 센터, GRC): 전 세계에서 발생하고 있는 사이버 공격 및 위협 정보 데이터들을 수집하고 분석하며 각국 정부 기관과 산업계(Symantec Corporation, Kaspersky Lab, F-Secure, Trend Micro, Microsoft 등)와 협력하여 사이버보안 관련 최전방 사이버 위협 정보 센터이다. 이 센터는 실시간 사이버 위협에 대한 초기 경고 시스템(Network Early Warning System)을 제공하여 사이버 위협을 식별하여 소속 국가에 제공하여 국제적으로 사이버 위협을 대응하도록 하는 국방정보보호 센터이다. GRC 센터는 Network Early Warning System라는 주된 기술이외에 아래와 같은 기술들을 포함한다.

- Network Early Warning System
- Automated Threat Analysis System (ATAS)
- Trend libraries
- Global visualization of threats
- Country specific cyber threats
- Incident and case management

- Trend monitoring and analysis

2) Centre for Police & International Cooperation (정책 및 국제협력 센터): 미래전에서의 사이버전은 사이버공간에서 이루어지는 각종 위협을 포함한다. 이러한 사이버공간상에서의 위협은 인터넷 및 IoT환경에서의 기술들의 증가에 따라 보다 긴밀하게 국가간 안보와 사회 인프라에서부터 국제 경제에까지 영향을 미친다. 그러므로 이러한 다국적인 관계속에서 사이버 공간상에 일어나는 다양한 사이버 위협을 여러 국가간 협력을 통해서 해결하는 방안을 제시하기 위해서 정책과 국제협력을 담당하는 센터이다. 이 센터에서 국가 정보보호 정책과 관련해서 아래와 같은 사항들에 초점을 두고 있다.
- 사이버 법 추진 및 국가간 사이버 범죄 입법의 세계적인 조화 (Promotion of cyber laws and the global harmonisation of national cybercrime legislation)
- 사이버 범죄와 다양한 사이버 위협에 대한 인식 제고 및 위협완화 (Awareness raising and mitigation of cyber crime and other forms of cyber threats)

3) Centre For Training & Skills Development (교육센터): 해당 센터는 사이버위협 및 사이버 안보에 필요한 국방정보보호에 필요한 정책과 기술 두 가지 분과를 갖고 교육을 담당하고 있다. 아래 그림에서 볼 수 있듯이 각 분과별로 세부 분과들이 나누어진다. 우선 정책기술로는 크게 세 가지로 항목을 구분할 수 있다.
- 보안관리 (Security Management): 해당 항목은 각종 보안정책과 과정을 개발하고 ISO 27001 정보보호관리에 있어서의 개념정립에서부터 구축까지 다룬다.
- 보안 심사 (Security Audits): 해당 항목은 ISO 27001 정보보호관리에서의 심사에 대한 부분을 다룬다.
- 정책 및 법률 프레임워크 (Policy and Legal Framework): 이 항목은 국내외의 사이버 위협에 대한 협력을 통한 해결 모델과 새롭게 나타나는 신종 사이버 위협에 대한 법적인 대응안에 대한 노력을 포함한다.

이러한 정책항목에 대한 사이버위협에 대한 다국적 협력방안에 대한 항목과 함께 기술적인 교육과 지원이 이루어진다. 이와 관련하여 IMPACT에서는 크게 네가지 항목을 포함한다.
- 네트워크 보안 (Network Security): 이 항목은 네트워크 시스템 보안 및 감사, 고도화된 허니팟과 악성코드 수집과 보안이 가미된 ISP 네트워크 그리고 자동화 사고대응팀 (Computer Incident Response Team, CIRT)의 구성과 구축을 포함한다.

이렇듯, 정책과 기술 두 가지를 포함하는 IMPACT에서의 교육내용의 요약을 아래의 그림에서 찾을 수 있다.

IMPACT의 교육센터 내 정책 및 기술 항목들

(출처: http://www.impact-alliance.org/)

4) Centre for Security Assurance & Research (정보보안 보증과 연구 센터): 이 센터는 사이버 위협에 효과적인 대응을 위한

2. 미국의 DARPA 기반 미래전 수행을 위한 국방정보보호

인터넷의 원형인 ARPANET를 개발했던 미방위고등연구계획국 (Defense Advanced Research Projects Agency, DARPA)은 미국방성의 연구 및 개발 부문을 맡고 있다. 그렇기에 미래전 수행을 위해서 미국은 어떠한 기술들을 연구하거나 개발하는지를 한눈에 볼 수 있는 곳이 바로 DARPA이다.

2.1. 자동취약점 분석과 Cyber Grand Challenge

최근의 가장 큰 이슈중 하나는 Cyber Grand Challenge (CGC)로서 기존의 사이버공간에서 전문 해커들에 의해서 이루어지던 해킹을 사람이 아닌 자동화된 컴퓨터 시스템에 의해서도 수행될 수 있음을 일종의 경진대회이다.

현재까지 사이버공간상에서 작동하고 있는 네트워크 침입탐지 시스템, 소프트웨어 보안패치, 취약점스캐너 등 다양한 시스템들이 모두 해커나 보안 전문가들이 시스템을 이해하여

얻어낸 일종의 인간지식(Signature)기반의 방어기술이다. 하지만, 이러한 방어기술들이 인간의 도움이 아닌 직접 시스템이 그 자신의 지식을 재창출하면서 인간지식과 유사한 방식으로 방어기술을 만들어 낼 수 있다는 데 그 의미를 둔다. CGC는 특히 타켓 시스템의 취약점을 자동으로 찾아주는 방식으로 운영이 되고 있으며 이러한 자동시스템이 이후 Defcon에 참가하는 자격까지 얻어지며 이제 해킹도 시스템화할 수 있다는 것을 보여주었다.

DARPA의 Cyber Grand Challenge

Machine vs. Machine: Lessons from the First Year of Cyber Grand Challenge

이 프로그램의 목적은 아래 표에 있는 Area of Excellence (AoE)에 언급되는 효과적이면서 통합적인 자동취약점 분석 도구를 개발하는 것이다. CGC에 대한 보다 자세한 사항은 http://cybergrandchallenge.com 에서 얻을 수 있다.

Area of Excellence (출처: DARPA)

	Areas of Excellence (AoE)	CGC Qualification Event (CQE)	CGC Final Event (CFE)
1	**Autonomous Analysis**: The automated comprehension of computer software (e.g., CBs) provided through a Competition Framework.	✓	✓
2	**Autonomous Patching:** The automatic patching of security flaws in CBs provided through a Competition Framework.	✓	✓
3	**Autonomous Vulnerability Scanning:** The ability to construct input which when transmitted over a network provides proof of the existence of flaws in CBs operated by competitors. These inputs shall be regarded as Proofs of Vulnerability.	✓	✓
4	**Autonomous Service Resiliency:** The ability to maintain the availability and intended function of CBs provided through a Competition Framework.	✓	✓
5	**Autonomous Network Defense:** The ability to discover and mitigate security flaws in CBs from the vantage point of a network security device.		✓

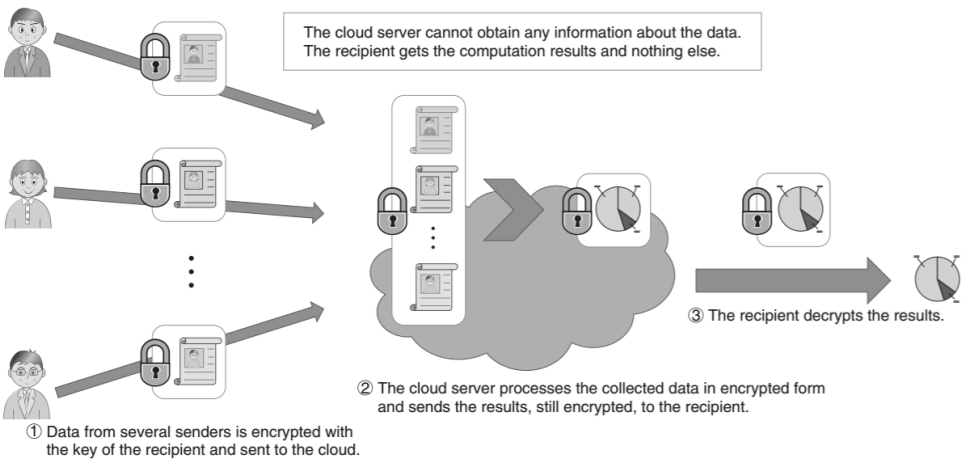
2.2. DARPA의 다른 국방정보보호 프로젝트들

DARPA에는 이러한 자동취약점 분석과 같은 사이버공간상의 방어기술만을 논하지 않고 다양한 국방기술들을 다루고 있다. 현재 DARPA에서 언급된 다른 기술들을 정리하면 아래와 같다.

2.2.1. PROCEED (PROgramming Computation on Encrypted Data)

첫 번째로 클라우드 환경에서 컴퓨팅환경을 고려한 PROCEED (PROgramming Computation on Encrypted Data)이라는 프로젝트가 있다. 사이버공간상에서 증가하는 데이터를 효과적으로 저장 및 관리하며 컴퓨터 자산을 물질형태가 아닌 서비스 형태로 제공하는 클라우드 컴퓨터 환경이 확산되고 있다. 이 방식은 시스템의 유지 보수비용은 적게 들면서 유연성, 가용성 및 확장성의 증가를 가져온다는 점에서 효율성이 극대화된 시스템이라고 볼 수 있다. 하지만, 이러한 효율성 제공과 함께 데이터의 보안과 키정보의 유실과 같은 취약점이 클라우드 환경에 존재한다. PROCEED 프로젝트는 바로 이러한 클라우드 환경에서의 취약점을 극복하기 위한 프로젝트로서 암호화된 데이터를 복호화 없이도 연산할 수 있도록 함으로서 공격자들이 바이러스를 쉽게 클라우드 환경에서 만들 수 없도록 만든다. 이를 위해서 완전동형암호(Fully Homomorphic Encryption)이라고 불리는 암호기술을 이용하여 클라우드에 클라이언트가 업로드하기 전에 데이터를 암호화한다. 이렇게 암호화되어 업로드된 암호문은 클라우드에서 별도의 복호화 과정없이 연산이 가능하고 연산 결과는 암호화된 채로 클라이언트에게 반환된다. 복호화 키는 오직 클라이언트만이 소유하고 있으므로 클라이언트만이 복호가능하기에 클라이언트가 갖고 있는 취약점을 제거해준다는 데 그 의미가 있다. 하지만, 현재의 동형암호기술은 여러 가지 한계를 갖고 있다. 그중 가장 큰 한계는 이론상으로는 가능하지만, 보통 일반적인 연산보다 10배 이상 느리고 비현실적으로 작동한다는 점이다. PROCEED프로젝트에서 이와 연관된 연구로는 단순히 완전동형암호 이론 자체의 연구가 아니라, 다자간 계산, 최적화된 하드웨어의 수학적 기초, 소프트웨어 구현 및 프로그래밍 언어, 알고리즘 및 자료형에 이르는 다방면의 연구가 이루어진다. 이 연구는 다양한 국방관련 데이터들의 저장과 관리에 있어서도 혁신적인 방안을 제공할 수 있다는 점에서 국내에서도 주의 깊게 바라봐야 할 기술이다.

클라우드 환경에서 동형암호 연산 (출처: NTT Technical Review)



2.2.2. Fundamental Limits of Learning (FunLoL)

두 번째 이슈는 DARPA에선 인공지능과 기계학습에 대한 연구를 진행하고 있다. 최근 데이터 홍수 시대에서 가장 큰 이슈로 부각되고 있는 것은 바로 빅데이터 분석기술이다. 이러한 빅데이터 분석 기술의 핵심이 바로 기계학습으로서 최근에 딥러닝(Deep Learning)이라는 기술역시 이러한 대용량 빅데이타 속에서 중요한 정보를 추출하는데 이용되었다. 그런데 최근에 DARPA에서는 보다 효과적이고 효율적으로 정보를 추출하기 위해서 기계학습 기술의 한계가 어디까지인지를 좀 더 명확히 설정하고 정형화하려는 노력이 시도되었다. 이를 대변하는 DARPA가 지원하는 프로젝트는 Fundamental Limits of Learning (FunLoL)이다. 이 프로젝트는 기계학습의 한계에 대한 인지에서부터 시작한다. 컴퓨팅 파워의 발전으로 대용량 데이터를 다룰 수 있게 되고 복잡한 연산도 빠른시간내에 계산해냄으로서 자율주행 자동차, 스마트 시티나 로봇 등의 복잡한 주제에도 모델기반시스템(model based approach)이 아닌 데이터 기반 시스템(data driven approach)을 사용할 수 있게 되었다. 하지만, 이러한 기계학습 기술을 사용할 때 발생하는 수학적 한계나 기술적 한계를 간과하곤 한다. 이러한 한계에 대한 이해가 없이는 어떤 업무를 기계에게 맡길 수 있는지 아니면 없는지를 결정짓기 어렵다. 이런 점에서 FunLoL프로젝트는 학습시스템 능력을 평가하고 그것들의 성능의 한계를 수학적으로 정형화하여 현실적인 적용방법을 제시하는 방법론을 연구하고 제시한다. 즉, 이러한 증명이 가능한 설계는 기계학습의 근본적인 한계를 특징화하고 결과의 신뢰도를 높이는데 큰 기여를 할 것이다.

인공지능과 기계학습의 한계 (출처: TBS magazine)

2.2.3. Aerial Dragnet

또 다른 연구로는 공중위협으로부터 도심지내 모든 요소를 보호하기 위한 혁신적인 추적 기술로서 Aerial Dranet이라는 프로젝트를 2016년 9월 13일에 새롭게 시작했다.

매일 매시간 수천대의 일반적인 비행기들의 움직임은 항공교통관리 시스템에 의해서 추적되고 있다. 하지만, 최근에 많은 관심을 받고 있고 향후 미래전에서 가장 큰 역할을 하게 될 Drone과 같은 소형 무인항공시스템 (UAS)에 대해서는 포괄적인 추적시스템이 존재하지 않는다. 하지만, 이러한 UAS가 가격이 저렴하고 다루기도 쉽기 때문에 테러리스트나 군사 목적에 적합해지고 있다. 하지만, 군 방어 시스템으로서 시야가 제안된 도심지에서 신속하게 UAS를 탐지하고 식별하는 것은 쉽지 지 않다. 이러한 제약을 극복하기 위해서 2016년 새롭게 시작된 UAS탐지 및 식별 프로젝트인 Aerial Dragnet 프로젝트는 대도시에서 1000피트 이만에서 작동하는 모든 UAS에 대해 지속적이고 광범위한 지역감시를 제공하는 혁신적인 기술이다. 지형지물이 많은 미래의 시가전이나 도심내 테러리스트의 무인기 활용을 이용한 공격을 탐지하는데 용이할 수 있는 프로젝트이다.

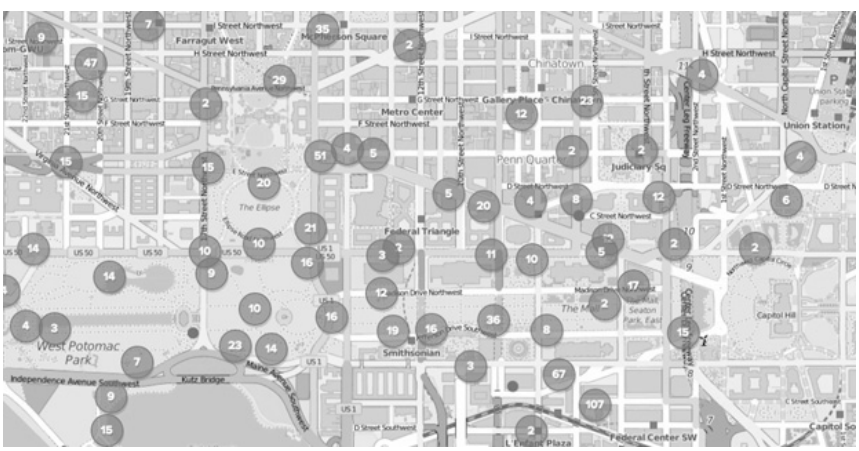
A notional Aerial Dragnet system (출처: DARPA)

2.2.4. SIGMA project

DARPA는 2014년부터 SIGMA라는 프로젝트를 통해 도심내 방사능위협을 신속하게 탐지하는 기술역시 연구에 들어갔다.

가방에 스마트폰 크기의 방사능 탐지장비가 도심내의 이곳저곳을 돌아다니면서 테러리스트가 이용할수 있는 Dirth bomb을 찾기 위해 방사능을 측정하고 있는 것이다. SIGMA프로젝트는 도심내 넓은 범위에 걸쳐 실시간으로 유동적인 방사능 탐지를 목표로 하고 있다. SIGMA의 행심은 저비용 고효율의 센서를 개발하여 감마선과 중성자 방사선을 감지해내는 것이다. 탐지 장비는 도시와 주, 연방 사무소들에서 파괴력이 강한 Dirth bomb와 같은 핵과 방사성 위협요소들을 실시간으로 신속히 탐지지하여 스마트폰을 통해 전송하는 방식으로 구성되어 있다.

도심내 Dirth Bomb 탐지를 위한 DARPA의 SIGMA 프로젝트 (출처: DARPA)



2.2.5. A-Teams project

A-Teams라는 프로젝트를 DARPA는 새롭게 시작했다. Agile Human-Machine Teams (A-Teams)를 설계하는 데 그 목적을 두며 국가안보를 위해서 사람과 기계로 이루어진 팀을 최적화시키기 위한 툴을 개발하기 위한 수학적 방법론을 찾는 프로젝트이다.

현대의 군사시스템은 앞장에서 언급하였듯이 신속한 지휘 통제를 위해서 네트워크중심작전 및 다양한 군사적 활동들이 역동적이면서 복합적으로 물리적 공간을 넘어서 사이버 공간 및 전자기 분야에까지 이어지고 있다. 이러한 복잡한 환경 속에 과학기술의 발달로 인해 미래의 전투기에는 사람과 기계가 한 팀을 이루어서 군임무를 수행할 수도 있게 될 것이다. 이러한 환경에서 가장 중요한 부분은 빠르게 변화하는 상황에 대응하기 위해서 인간의 인지능력과 기계만의 능력을 적절히 혼합하는 것이다.

이러한 최적화된 팀을 설계하기 위해서 DARPA는 예측가능하면서 폭넓게 사용가능한 인간과 기계간의 팀에서의 상호 협력을 원활하게 할 수 있도록 만드는 수학적 방법론을 개발하기 위해서 Agile Teams (A-Teams)라는 프로젝트를 발표했다.

DARPA의 A-team (출처: DARPA)

여기서 주목해야 할 것은 A-Teams프로젝트는 인공지능의 새로운 기술을 개발하는데 그 목적을 두고 있지 않다는 것이다. A-Teams 프로젝트의 목적은 사람과 기계로 이루어진 팀의 팀워크를 최적화할 수 있는 새로운 프레임워크를 개발하는데 그 목적이 있다. 만약 해당 프레임워크가 개발된다면 해당 프로젝트의 결과물은 국방에서의 기계와 인간의 팀워크만이 아니라, 과학, 의약품 개발, 소프트웨어 엔지니어링, 군수기획 등의 복잡한 문제를 해결하는데도 용이해질 수 있다. 즉, A-Teams은 미래에 기계가 단순히 자동화된 결과만을 제공하는 것을 넘어 팀 멤버들과의 상호작용을 통해 문제를 해결해내는데 그 목적을 두고 있다.

Ⅱ. 국방정보보호 구축 및 발전방안 모색

이번 장에서는 국방 정보보호 구축 및 발전방안에 대한 모색을 다루고자 한다. 우선 사이버공간상에서 국방정보보호 이슈와 관련하여 최신 기술로 소개되고 있는 빅데이터 분석 및 인공지능에 대한 소개를 하고 이들의 관계에 대해서 언급하고 이후 국방정보보호에서 필요한 기술들을 언급하고자 한다. 본 장은 세 개의 절로 구성되어 있다. 1절은 빅데이터 시대의 핵심 분석 기술인 기계학습과 인공지능이라는 제반 기술에 대해서 언급하고 어떻게 국방정보보호에 적용될 수 있는지를 다룬다. 2장에서는 빅데이터 분석의 결과물로 여겨질 수 있는 Open Source Intelligence (OSINT)라는 기술에 대해서 어떤 발전방향이 있어야 하는지를 기술하고자 한다. 마지막 장은 미래전을 수행하기 위한 다양한 국방정보보호 기술로 국내에서 어떤 기술들이 요구될지에 대한 소개를 한다.

제1절 인공지능 기반 미래전을 수행키 위한 국방정보보호 기술

1. 빅데이터와 인공지능

1.1. 자동취약점분석과 인공지능의 오해

사이버전과 관련하여 최근에 민간 기업, 학계 및 군에서 가장 이슈인 주제는 “자동취약점 분석”과 “인공지능(AI)”이다. 자세한 설명에 앞서 안타깝게도 현재 군에서 미래기술로 여겨지는 자동취약점 분석과 인공지능이 현재까지는 큰 연결고리를 갖고 있지 못한 실정이다. 더 큰 문제는 이렇듯 연결고리가 없는데 군에서 현재 자동 취약점 분석 기술이 인공지능으로 만들어진 것으로 오해하고 있다. 물론 자동취약점 분석이 인공지능 기술로 만들어질 날이 머지않아 다가올 것임은 분명하다. 하지만, 현재 버전의 자동취약점 분석은 그야말로 기존 취약점 분석 기술들의 조합에 불과할 뿐 인공지능의 기술이 포함되지 않았다는 것을 우선 밝히고자 한다.

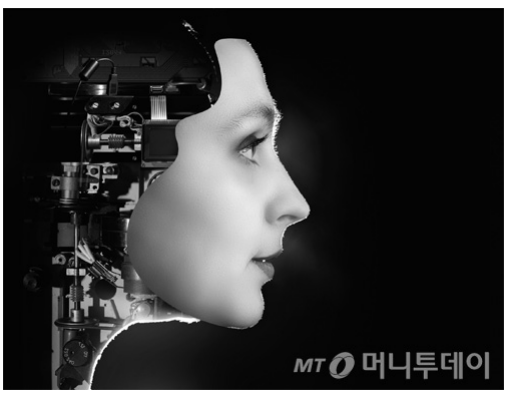
그렇다면 이번 보고서에서는 향후 만들어질 인공지능 기반의 자동취약점 분석에 대해서 어떻게 다가가야 하는지를 작성코자 한다. 이를 위해서 사이버보안 분야에서 최근 가장 큰 이슈인 자동취약점 분석을 논하기 앞서, 인공지능이란 무엇이며 인공지능 기술이 왜 최근에 이슈가 되는지를 먼저 살펴야 한다.

1.2 인공지능의 정의

우리는 호모사피언스(Homo sapiens)라고 우리자신을 칭하는데 그 이유는 지능을 갖았다는 부분에서 기존의 등장했던 인류의 조상들과 차이를 갖는다. 이렇듯, 인류를 정의하는

기준에서도 중요한 이슈가 바로 지능을 소유하고 있는지에 대한 여부이다. 이러한 점에서 인류가 살아온 수 천년동안 인류가 인류를 이해하기 위해서 생각에 대한 그 방법론에 관심이 있었다. 인류의 사고에 대한 이해에 대한 노력과 함께 같이 연구되기 시작한 분야가 바로 인공지능(Artificial Intelligence, AI)이다. 인공지능은 인류가 어떻게 생각을 하는지에 대한 이해와 함께 오직 인류만이 갖고 있는 생각과 지능을 만들 수 있는지에 대한 성찰로부터 시작한다.

인공지능이란 (출처: 중앙일보 머니투데이)



스튜어트 러셀과 피터 노빅의 인공지능 저서에 의하면 인공지능은 2차원 요소로 정의가 가능하다[13]. 그 하나는 생각과 행동 이고 다른 하나는 인간적인지 아니면 이성적인지로 나눌 수 있다.

4가지 분류로 나눌 수 있는 인공지능에 대한 정의[13]

Thinking Humanly	Thinking Rationally
Acting Humanly	Acting Rationally

즉, 인공지능이라 함은 단순히 지능을 만들어 내는데 그 목적이 있는 것이 아니라, 총 4가지 관점중 하나를 만족하면 인공지능이라고 정의할 수 있다.

(1) Thinking Humanly: 인간처럼 생각하도록 만들어 보려는 접근 방법으로 인공지능을 정의한다. 가장 인공지능에 대한 원천적인 질문에 대한 답을 찾는다고 볼수 있다. 인간이 갖고 있는 '지능'이라는 부분을 모사하고자 하는 노력이기 때문이다. 그러한 점에서 Thinking humanly라는 표현은 종종 인지과학(cognitive science)이나 인지모델링(cognitive modeling) 접근 방법으로 여겨지고 있다. 이 영역은 심리학적인 부분과 정말로 뇌가 어떻

게 지능을 만들어내는지에 대한 이해가 필요하며 이를 모사하기 위한 노력을 함으로서 인공적으로 지능을 이해하고 만들고자 하는 모든 노력을 포함한다.

(2) Acting Humanly: 인간처럼 행동하게 만들 수 있냐의 문제로서 일종의 Turing Test 관점에서 인공지능을 정의한다. 일반적으로 이 접근 방법이 가장 보편적인 인공지능에 대한 정의라고 볼 수 있으며 기존의 컴퓨터공학과과 전자공학등 공학자들에 의해서 이루어진 접근 방법이라고 볼 수 있다. 기계로 사람이 행동하는 것과 유사하게 접근하겠다는 방식이다. 즉, 인간처럼 생각하고자 하는 것이 아니라 인간처럼 행동하는데 초점이 맞춰있기 때문에 지능과는 거리가 멀 수도 있다. 하지만, 실질적으로 중요한 문제들을 해결하는데 가장 유용한 방식으로 알려져 있으며 이러한 Acting humanly관점에서 인공지능의 분야로 여겨질 수 있는 것들은 아래와 같은 분야들이다.

- 자연언어처리 (Natural language processing)
- 지식 표현 (Knowledge representation)
- 자동 추론 (Automated Reasoning)
- 기계 학습 (Machine Learning)
- 컴퓨터 비전 (Computer Vision)
- 로봇 (Robotics)

이렇듯, Acting Humanly는 인간이 사고하는 방식이나 지능보다는 인간의 행동 자체의 모사에 관심이 있다고 볼 수 있다. 예를 들어, 최근에 세계적 주목을 끌었던 DeepMind사의 알파고와 같은 프로그램은 인간처럼 바둑을 둘 수 있기 때문에 인공지능에 기반한 시스템이라고 말할 수 있다.

(3) Thinking rationally: 이성적인 사고를 어떻게 만들 수 있냐의 문제로서 일종의 사고의 법칙(Laws of thought)을 만들 수 있냐에 대한 질문을 함으로서 인공지능을 정의한다. 올바른 사고란 무엇인지에 대해서 접근하는 방식으로 현재 통용되는 AI와는 사뭇 거리가 존재함을 알 수 있지만 논리(Logic)라는 개념을 이용하여 AI를 접근하는 방식이다.

(4) Acting rationally: 이성적으로 행동하는 것을 목표로 한다는 점에서 인공지능을 정의한다. Thinking rationally라는 이성적 사고와 이성적 행동은 유사하면서도 다른 점이 존재한다. 이성적 사고란 정확한 사고를 의미하고 이성적 행동이란 주어진 환경에서 최선의 행동을 추구한다는 점에서 꼭 올바른 사고나 정확한 사고를 수반할 필요가 없다.

이러한 4가지 목록화한 인공지능의 정의를 볼 때 현대사회에서 바라보는 인공지능은 주로 Thinking Humanly와 Acting Humanly로 압축될 수 있으며 국방기술에서 직접적으로 쓸 수 있는 기술은 Acting Humanly 즉 사람처럼 행동하게 하는 부분에서 인공지능을 논할 수 있다. 특히 최근에 생겨난 빅데이터 분석 기술에서 사용되는 인공지능 기술은 Acting Humanly에서의 접근 방법으로 사람이 대량의 데이터들로부터 유의미한 정보를 뽑아내는 행동을 사람이 아닌 기계가 대신한다는 점에서 작금의 데이터 마이닝, 빅데이터 분석 기술 등은 인공지능기술과 민첩한 관련성을 갖는다.

특히 이러한 인공지능의 중요성이 나날이 증가하고 있는데 그 이유는 데이터나 시스템의 불확실성이 시스템의 복잡도가 증가하면서 사람이 하던 일들을 더 이상 사람이 직접 하기 불가능한 상황에 이르렀기에 이제는 사람의 행동을 모사하는 것(Acting Humanly)을 넘어서고 있다. 이러한 변화에 대한 요구는 사이버 보안과 국방정보보호에서도 일어나고 있는 이슈이다. 아래의 표는 최근에 한국정보화진흥원에서 발표한 AI관련 기술 분야의 목록화이며 많은 항목들이 사이버 보안과 많은 관련성을 갖고 있는 것을 볼 수 있다.

AI관련 기술 분야의 분류 (출처: 한국정보화진흥원 2010년)

구분	내용
패턴 인식 (Pattern Recognition)	▪ 기계에 의하여 도형, 문자, 음성 등을 식별 시키는 것 ▪ 제한된 분야에서 실용화 되고 있으며, 지속적으로 발전 중
자연어처리 (Natural language Processing)	▪ 인간의 평상 언어를 컴퓨터에 인식 시켜 특정 Task를 처리 하는 것 ▪ 정보검색, 질의응답 시스템, 자동 통·번역 등
자동제어 (Automatic Control)	▪ 제어대상에 미리 설정한 목표 값과 검출된 Feedback 신호를 비교하여 그 오차를 자동으로 조정하는 방식
인지로봇공학 (Recognition Robotics)	▪ 로봇에 관한 과학이자 기술학으로 제한된 시간과 계산자원을 활용해 복잡한 환경의 복잡한 목표를 달성하도록 하는 인지 능력을 로봇에게 부여하는 기술
컴퓨터비전 (Computer Vision)	▪ 로봇의 눈을 만드는 연구 분야로 컴퓨터가 실세계 정보를 취득하는 모든 과정을 다룸
가상현실 (Virtual Reality)	▪ 특정한 환경이나 상황을 컴퓨터로 구현하여 그것을 사용하는 사람이 실제 주변 환경과 상호작용을 하는 것처럼 만들어주는 I/F 기술
자동추론 (Automated Reasoning)	▪ 계산기 과학의 한 분야로 추론의 다양한 측면을 이해함으로써 컴퓨터에 의한 완전한 자동추론을 가능하게 하는 소프트웨어 개발을 목표로 함
사이버네틱스 (Cybernetics)	▪ 생물과 기계사이의 제어와 통신 문제를 종합적으로 연구하는 분야
데이터마이닝 (Data Mining)	▪ 많은 데이터 가운데 숨겨져 있는 유용한 상관 관계를 발견하여 미래에 실행 가능한 정보를 추출해 내고 이를 의사 결정에 활용하는 과정
지능엔진 (Intelligent Agent)	▪ 인공지능적 기능을 가진 소프트웨어 엔진 ▪ 사용자를 보조하고 반복된 컴퓨터 관련 업무를 인간을 대신하여 실시하는 소프트웨어
시멘틱 웹 (Semantic Web)	▪ 컴퓨터가 정보자원의 뜻을 이해하고, 논리적 추론까지 할 수 있는 차세대 지능형 웹

1.3 오늘날의 인공지능의 방향

2015년 알파고가 한국사회에 인공지능의 붐을 일으켰다. 하지만, 바둑대회를 통해서 일어난 인공지능의 붐은 이미 시나브로 우리사회에 다가와 있었다. 갑자기 알파고가 나온 것이 아니란 것이다. 사실, 알파고가 나오기 전에 IBM의 왓슨 컴퓨터가 있었으며 그 이전에 다양한 인공지능 기술들이 개발되어 소개되어 왔다. 그런데 왜 지금에 와서 갑자기 사회 전 분야에 AI라는 단어가 온 인류를 강타하는 사회의 핵심 단어처럼 사용되는 것일까? 그 이유는 빅데이타, 사물인터넷, 스마트 시티 등 다양한 단어들에서 손쉽게 찾을 수 있다.

이미 앞에서 살펴본 인공지능에 대해서 4가지 정의에 대한 관점에서 볼 수 있듯이, 인간처럼 사고하고, 인간처럼 행동하고, 이성적으로 행동하고 이성적으로 사고하는 것이 바로 인공지능이다. 이러한 관점에서 인공지능을 바라본다면 우리가 사용하고 있는 다양한 기계 전자 기술들은 거의 모두 인공지능 기술을 피해가기 어려워진다. 그런데 최근에 산업과 학계를 강타했던 빅데이터, 클라우드 컴퓨팅 환경은 인공지능 기술을 극대화하는 조건을 갖고 있던 기술들이다. 빅데이터는 사실상 대용량 데이터를 분석함으로서 기존에 찾기 어려웠던 숨겨진 중요정보를 추출할 수 있다는 점에서 새로운 패러다임과 기술로 받아들여졌다. 그리고 이러한 대용량 데이터를 효과적으로 저장 관리하기 위해서 클라우드 환경이 제시되었다. 그런데 흥미로운 것은 기존에 적은 양의 데이터에서 중요한 정보를 추출하는 것은 인간이 직접 수행하던 일이었다. 하지만 데이터의 용량이 빅데이터라고 불릴 정도로 거대해지면서 더 이상 인간이 할 수 없는 수준에 이르게 되었다. 이런 점에서 인간이 수행하던 정보추출 기능을 빅데이터 시대가 되면서 기계에게 넘기게 된다. 이러한 빅데이터의 홍수속에서 인공지능은 그 가치를 인정받기 시작했다. 또한 빅데이터 시대를 가속화하는 사물인터넷이라는 장비간의 복잡한 네트워크는 복잡도가 높아진 스마트시티와 같은 지역간 또는 국가간 모든 장비들이 엮어짐으로서 복잡도는 극한으로 치닫게 된다. 결국 이러한 극도의 높은 복잡도를 갖는 시스템을 사람이 직접 분석하기 어려운 수준으로 결정이 나며 인간의 힘이 아닌 기계의 힘으로 인간이 하던 행동을 하도록 개발되었다. 바로 이것이 인공지능이 왜 필요했었는지를 상세히 밝히게 되는 요소이다.

결론적으로 인공지능은 기계를 통해 양질의 인간의 삶이 주어진다면 인공지능에 대한 사회적 수요는 앞으로도 지속될 것이다. 하지만, 단순히 Acting Humanly를 넘어서 Thinking Humanly, Thinking rationally, Acting rationally까지 폭넓게 연구가 될 것이다. 예를 들어, 기계나 로봇이 특정 전투상황에서 부상을 당한 적군을 총으로 공격해야 할지 아니면 말아야 인간답게 또는 이성적으로 판단할지에 대한 인공지능까지도 갖추게 될 날이 멀지 않다.

2. 인공지능 기반 사이버전과 국방 정보보호 발전방안

2.1 인공지능 기반 기존 사이버 보안 기술들

사이버 보안이나 미래전 관련 기술에서 인공지능이 과연 사용되었는가하는 질문은 종종 듣는 질문이다. 그에 대한 대답은 항상 Yes이다. 사실상, 그 어떤 분야보다도 사이버보안 분야에서는 인공지능 기술이 많이 사용되었다. 이러한 점에서 최근에 붐이 일어나는 인공지능 기반 사이버방어 기술 연구들은 기존의 연구의 맥을 유지할 뿐 새로운 것은 전혀 아닌 것이다. 사이버보안 분야에서 가장 대표적인 인공지능 사례는 다름 아닌 컴퓨터 바이러스 백신(Computer Virus Vaccine)과 침입탐지시스템(Intrusion Detection System) 기술이다. 이뿐만이 아니다. 이메일(E-mail)에서 Phishing을 걸러내거나 스팸(spam)과 햄(ham)을 구분 짓는 방식 역시 인간을 대신해서 기계가 그 차이를 구분을 짓는다는 점에서 인공지능의 개념이 들어갔다고 볼 수 있다. 특히 이러한 Acting Humanly개념에서 접근한 기존의 사이버보안 이슈들은 크게는 기계학습의 세 가지 기술 분야로 세분화가 가능하다.

(1) 분류법 (Classification): 이것은 일반적으로 Supervised Learning이라는 방식으로 각 데이터마다 일종의 클래스 값이 주어진 상태로 기계학습에 의해서 학습되어 이후 새로운 질의문(query)이 생길 경우 학습된 모델에 해당 질의문을 넣어 클래스를 찾아내는 방식으로 만약에 학습시키고자 하는 데이터가 충분하다면, 스팸과 햄을 구분을 짓거나 바이러스 백신을 통해 악성코드와 정상코드를 구분을 짓는 문제 또한 Phishing을 찾아내는 문제에 적용가능하다.

(2) 그룹화 (Clustering): 그룹화는 Unsupervised Learning이라는 방식으로 사용되는 경향이 있다. 이것은 기계학습에 사용할 학습 데이터에 클래스나 Label이 존재하지 않는 상태에서 학습을 한다. 그러므로 주어진 데이터들을 그룹핑을 함으로서 새로운 Query가 발생할 경우 그 그룹을 찾아내는데 그 목적을 두고 있다. 이 방식은 분류법 (Classification)과 많은 부분에서 유사하다.

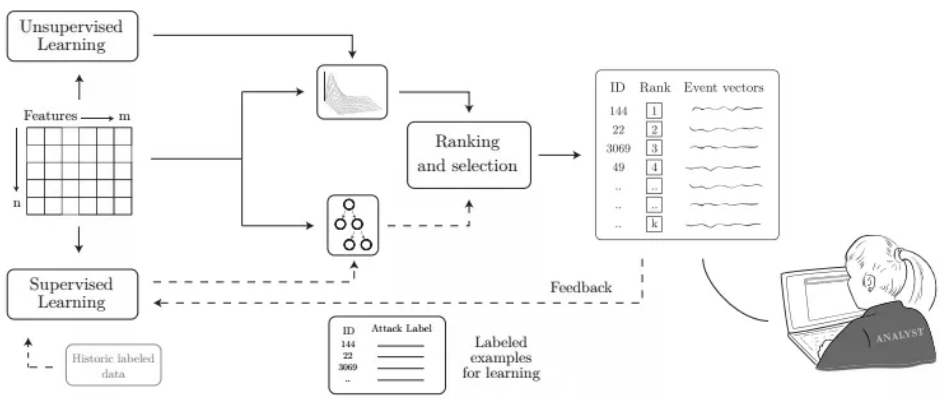
(3) 예측 (Prediction): 인공지능에서 예측행위는 사이버공간상에서 발생하는 여러 가지 사고를 예측하는 시스템에 사용될 수 있다. 예측과 관련해서는 크게 두 가지 방식이 존재하는데, 첫 번째 방식은 과거의 축적된 데이터를 이용하여 미래를 예측하는 시스템이고 또 다른 하나는 변화되는 패턴을 이용하여 미래를 예측하는 시스템이다.

	Computer Virus Vaccine	Intrusion Detection System (IDS)	Spam Filter	Phishing	DDoS detection
Classification	O	O	O	O	O
Clustering	O	O	O	O	
Prediction	-	-	-	-	O

하지만 이러한 다양한 기계학습 기법은 사이버 보안에서 사용되는 데이터들이 갖는 특이성 때문에 적용에 많은 어려움을 갖곤 한다. 그 가장 큰 이유는 사이버 보안에서 AI를 사용되는 대부분의 문제들은 이상치 탐지(anomaly detection) 에 기반하는데 이러한 비정상신호(abnormal signal)는 일반적으로 정상신호(normal signal)에 비해서 대단히 적은 양이 존재하는 비균형적 데이터(Unbalanced data)이기 때문이다. 이렇듯 비균형적 데이터에서 이상신호를 찾는 문제는 비정상신호들이 갖는 특징에 대한 충분한 정보를 얻는 것이 거의 불가능에 가까우기에 의미 있는 결과를 얻는 것이 결코 쉽지 않다. 이러한 불균형적 데이터의 문제는 지능형지속위협(APT)공격 기반 악성코드를 탐지하는데 더 큰 난관을 제공한다. 또 다른 기계학습기술의 한계점으로 특징점 추출의 어려움이다. 일반적으로 기계학습에 입력 데이터를 적용하기 이전에 효과적인 결과를 얻기 위해서 특징점 추출(Feature Extraction)과 차원축소(Dimension Reduction)라는 기술을 이용한다. 하지만, 대부분의 문제에서 효율성을 극대화하는 최적의 특징점 추출과 차원축소가 쉽지 않다.

이러한 기계학습의 문제들을 해결하기 위해서 최근에 다양한 방법론이 시도되었다. 그중 하나는 AI2 기법이고 또 다른 하나는 딥러닝(Deep Learning) 기술이다. AI2기법은 MIT의 인공지능 그룹에서 개발한 기술로 기존의 Unsupervised Learning기법에 인간의 추가적인 Supervised Learning 기술이 추가됨으로 인해서 사이버 공격의 85%를 막아내는 성과를 보인 기술이다.

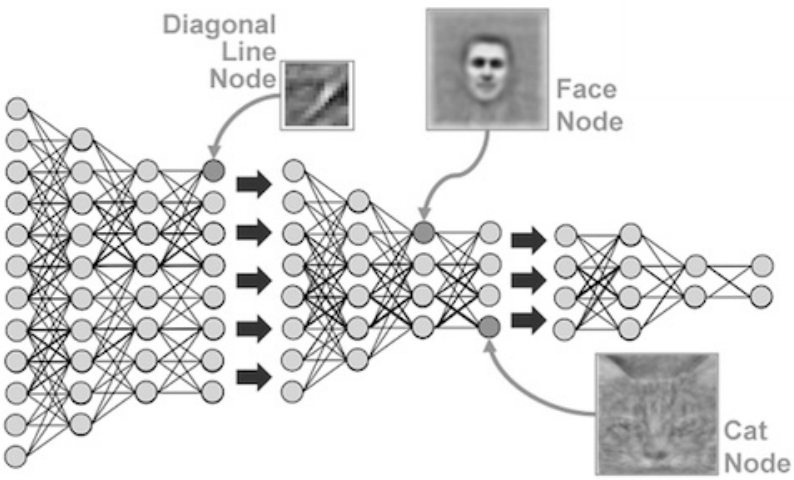
AI2 알고리즘을 이용한 사이버공격 탐지[14]



또 다른 기술로는 알파고 이후 유명세를 떨치고 있는 바로 딥러닝(Deep Learning) 기술이다. 딥러닝은 데이터 분류나 식별등의 기계학습영역에서 사용하던 기존의 인공신경망이론[15]의 한계인 특징점 추출의 어려움을 제거함으로서 기존의 한계를 넘어선 새로운 기술로

인식되고 있다. 구글브레인팀인 Andrew Ng와 Jeff Dean은 유투브 비디오에서 얻은 라벨이 부여되지 않은 이미지들로부터 고양이와 같은 객체를 식별하는 딥러닝 기반의 신경망을 아래와 같이 구축하였다 [16]. 특히 특징점 추출과정이 제거되었다는 점에서 기존의 기계학습 기법들의 한계를 극복하게 되었으며 이는 미래전의 사이버전에서 다양한 응용분야에 적용 가능성을 보였다.

딥러닝 (Deep Learning)을 통한 이미지 분석



(출처: http://scyfer.nl/what-is-deep-learning/ 구글 인용)

2.2 자동취약점 분석

최근에 사이버보안분야에서 가장 큰 이슈가 바로 자동취약점 분석 기술이다. 기존에는 취약점 분석을 함에 있어서 고도로 훈련된 화이트 해커나 보안 전문가들이 그들의 축적된 노하우를 이용하여 타겟 시스템의 취약점을 찾아내었다. 하지만, 최근에는 시스템의 취약점을 다양한 자동화 기술을 통해 사람의 힘을 빌리지 않고 직접 기계가 찾아내는 연구가 진행되고 있다. 하지만, 이미 언급하였듯이 현재의 자동취약점 분석은 어떠한 시스템내의 어려움이나 불확실성을 내포하지 않고 단순히 작업들의 조립에 불과하므로 아직까지는 인공지능 기술이라고 말하기는 어렵다. 하지만, 머지않아 자동취약점 분석 기술은 인공지능의 기술이 적용될 것으로 예상된다. 가장 큰 이유는 복잡한 시스템에 대한 해석과 판단에 있어서 더 이상 단순한 조합으로는 그 한계를 보일 것이며 또한 더 이상 사람이 직접 판단하고 분석한다는 것이 불가능하다고 여겨질 것이기 때문이다.

제2절 OSINT 기반 미래전을 수행키 위한 국방정보보호 기술

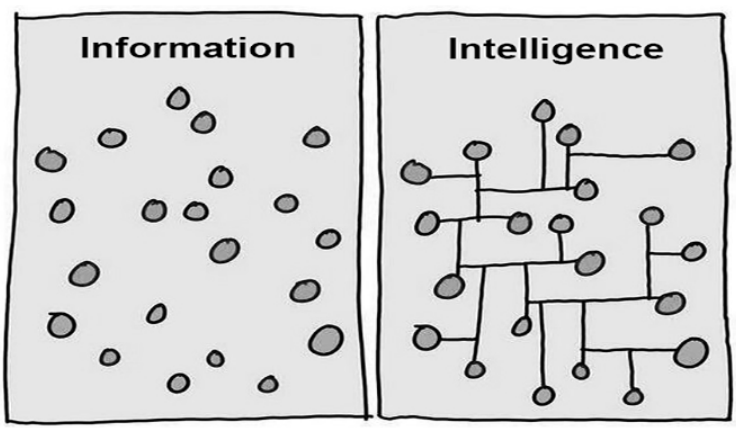
1. OSINT 기반 사이버전과 국방 정보보호 발전방안

OSINT는 공개된 정보들을 분석하여 숨겨져 있는 중요 정보를 추출하는 방법을 의미하는데 이미 많은 정보선진국에선 이 기술의 중요성을 인지하고 오래전부터 관련 기술에 대한 플랫폼 구축부터 다양한 주제로 연구를 국가적으로 진행해왔다. 특히 본 보고서에서 OSINT 기술을 언급하는 이유는 OSINT기술이 미래전에서 긴급하게 변화하는 환경과 상황에 대한 정보수집에서 다른 어떤 정보수집기술보다 효과적일 수 있기 때문이다. 또한 사이버전에서 가장 큰 문제로 여겨질 수 있는 랜섬웨어 공격이나 지능형지속위협(APT)공격등을 단순한 악성코드분석이 아닌 정치사회공학적으로 분석하기 위해서 악성코드 개발자들의 프로파일링 및 사이버 테러리스트들의 프로파일링부터 범죄예측에 이르기까지 다양한 방면에서 공개정보분석(OSINT)기술이 적용이 가능해 보인다.

1.1 OSINT 정의 및 개념

정보라는 단어에 대해서 영어표현으로는 두 가지 단어가 존재한다. 그 하나는 Information이고 또 다른 단어는 Intelligence이다. 이 두 가지 단어의 차이점은 가치 있는 정보를 드러내었느냐 아니냐에 따라 나눌 수 있다. 즉, Information은 의미 있는 정보를 갖고는 있으나 아직 정제되어 드러나지 않은 정보를 의미하고 Intelligence는 의미 있는 정보가 드러나서 바로 사용가능한 정보를 의미한다고 볼 수 있다. 이러한 점에서 Intelligence라는 정보는 주로 국가의 정보기관에서 사용하는 단어로 여겨져 왔다.

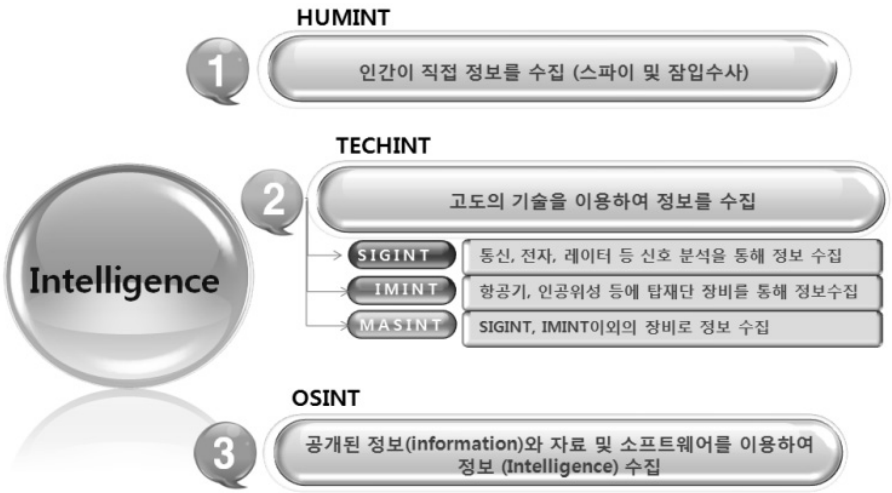
Information vs. Intelligence



일반적으로 정보(Intelligence)를 수집하는 방식으로는 크게 3가지 방식이 존재한다. 사람이 직접 수집하는 HUMINT, 다양한 장비와 기술을 이용하여 수집하는 TECHINT, 공개정보를 이용하여 정보를 수집하는 OSINT(Open Source Intelligence)로 나눌 수 있다.

1) HUMINT는 정보원이나 내부 협조자 등의 다양한 인적 네트워크를 이용하여 얻은 정보를 수집하는 방법을 말하며 일반적으로 첨단 기술의 의한 첩보 활동만으로 파악이 어려운 경우에 이 방식을 사용한다.
2) TECHINT는 과학 기술을 이용하여 정보를 수집하는 방식을 의미하며 이 역시 작게는 세 가지로 세분화가 가능하다. 신호를 분석하는 SIGINT, 영상정보를 수집하는 IMINT, 징후계측정보를 수집하는 MASINT로 세분화할수 있다.
3) 마지막으로 OSINT는 신문, 책, TV, SNS 등의 공개된 자료를 수집하는 일련의 정보수집 방법이다. 특히 본 보고서에서는 OSINT기술에 대해서 집중적으로 다루고자 한다.

정보(Intelligence)를 수집하는 세 가지 방법론



Open Source Intelligence (OSINT)라는 것은 일반적으로 공공에서 접근가능한 공개정보 (Open sources)를 이용하여 정보활동을 하는 것을 말한다. 여기서 공개정보란 다원적인 다양한 공개출처 매체를 통해 수집된 모든 정보를 가리키며 아래와 같은 정보들이 공개정보라고 말할 수 있다.

- 신문, 간행물, 방송, 민간 및 공공기관의 보고서
- 연구논문, 공개된 회의록, 단행본, 기자회견 및 연설문 등 전통적 매체로부터 얻어지는 정보들

- 인터넷, 데이터베이스, On-line 등 사용 정보를 포함하는 디지털 매체로부터 얻어지는 각종 공개된 정보들

즉, OSINT는 공공에서 접근할 수 있는 정보(Information)를 이용하여 정보활동을 한다는 점에서 기존의 비밀정보수집 방법과 그 차이점을 보인다고 말할 수 있다.

이러한 공개정보를 이용한 정보 수집과 분석에 대한 요구는 각국의 주요 정보기관들의 정보수집활동의 변화로부터 시작되었다. 과거에 미국 대통령과 각료들은 HUMINT와 TECHINT를 통해 획득된 정보를 포함하는 비밀보고서의 내용을 매우 귀중하게 여겨왔으나, 신문이나 방송에서 읽거나 청취하게 되는 내용들이 비밀보고서에서 다시금 읽게 되는 경우가 많아지면서 공개정보의 중요성을 알게 되었다. 특히, 인터넷의 발달과 함께 공개된 매체에서 중요한 정보들이 넘쳐나게 되고 이러한 공개된 정보를 수집 분석함으로서 효율적으로 중요 정보를 수집하게 되었다. USA 투데이에서는 이러한 공개정보만으로도 미국 기관들이 첩보활동에 필요한 정보량의 약 90%를 알아내는 것이 가능하다고 발표하였다.

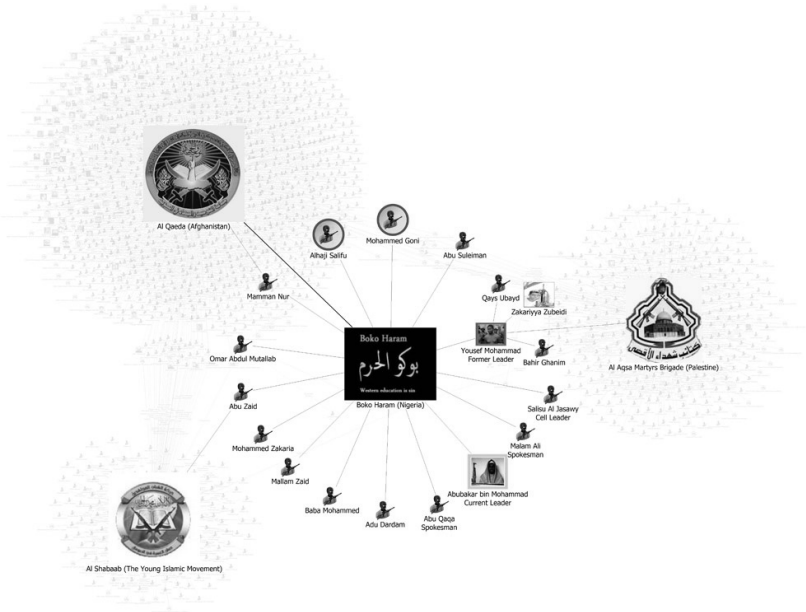
1.2 정보선진국들의 OSINT 활용 및 투자

OSINT를 이용하여 중요한 정보를 획득할 수 있음을 알게 된 정보선진국들은 이와 관련하여 다양한 연구나 기관을 설립하게 된다. 우선 미국의 사례를 보면 미국은 일찌감치 공개정보 분석의 유용성을 인식하고 다양한 곳에서 해당 기술이 적용되고 있다.

1.2.1 미국의 ISVG (Institute for the Study of Violent Groups)

ISVG는 미 연방정부의 연구 자금을 지원받아 공개 정보를 이용하여 테러리즘과 폭력그룹에 관련한 데이터베이스를 구축하기 위해서 만들어진 연구프로젝트이다. 이 프로젝트는 초창기 샘휴스턴 주립대학에서 주도하여 시작하였으나, 현재는 뉴해븐 대학으로 옮겨서 활발하게 활동이 이뤄지고 있다. 특히 2004년부터 현재에 이르기까지 야가 15만건 이상의 전 세계에서 발생한 각종 테러사건에 대한 데이터베이스를 구축하였다는데서 기존의 데이터베이스와 차이점을 갖는다. ISVG프로젝트의 구현 원리는 간단하다. 우선 온라인상에서 이용가능한 각종 공개정보들을 수집하여 전 세계에서 발생하는 테러 사건과 테러조직, 주요 테러리스트들에 관한 정보들을 데이터베이스화한다. 온라인상의 공개정보들을 일차적으로 수집한 이후 동일 사건, 인물, 조직 등의 관계형 데이터(Relational database)의 원칙에 따라 유사성 기준으로 연결시키는 등 비정형 데이터를 정형화한다. 이후 다양한 시각화 기법을 통해 정제된 데이터나 분석 정보를 전달해 주는 서비스를 제공한다.

테러리스트간의 유사성을 엮어서 본 시각화 (출처: ISVG)



1.2.2 미국의 START (Study of Terrorism And Response to Terrorism)

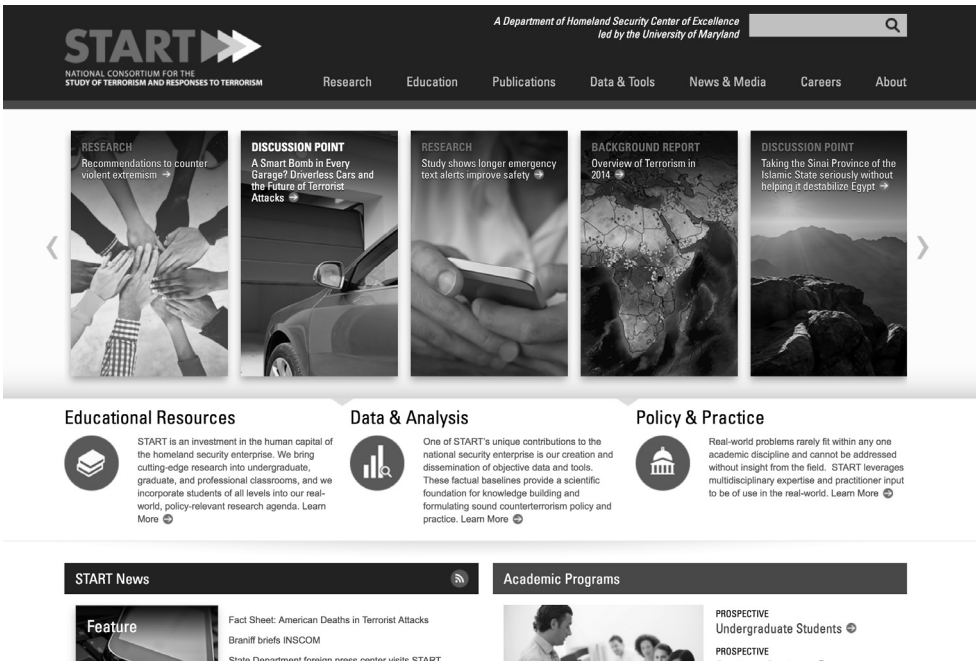
미 국토안보부의 지원을 받아 2005에 메릴랜드 대학교에서 시행중이며 2008년부터 ISVG와 통합하여 시너지 효과를 내고자 하였다.

START 프로그램은 효과적인 대테러 활동에 필요한 테러리즘과 테러리스트와 관련된 다양한 행동패턴 및 심리적 영향 등의 다양한 분야에 관한 사회과학적, 행동과학적인 이해를 목표로 하고 있다. ISVG가 일차적인 정보 수집에 보다 초점이 맞추어져 있었다면 START는 수집보다는 연구와 분석에 초점을 맞추고 있다는 점에서 그 차이를 보인다. 일례로 테러리스트에 대한 프로파일링도 수행하면서 이에 대한 데이터베이스를 구축하고 서비스를 제공하고 있다. 또한 이러한 효과적인 대테러 활동을 위해 필수적인 테러리즘과 테러리스트와 관련된 행동 패턴과 심리적 영향 등의 다각도의 분석을 통해 정보활동이 이루어지게 되었다.

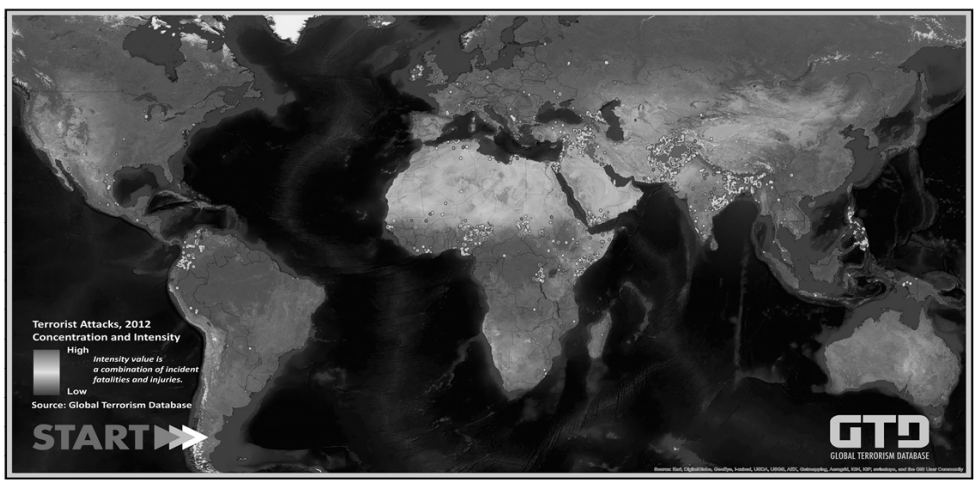
특히, START는 전 세계에서 발생하는 테러와 함께 다양한 위험들에 대해서도 분석을 하고 연구를 진행하고 있다. 이와 관련하여 다양한 연구 분야를 갖고 있다.

- Terrorism and Violent Extremism
- Counterterrorism and Countering Violent Extremism
- Radicalization and De-radicalization
- Risk Communication and Resilience
- Unconventional Weapons and Technology

START project (출처: START)



공개정보분석을 통한 테러에 대한 START 프로젝트와 GTD (출처: START)



START 프로그램은 효과적인 대테러 활동에 필요한 테러리즘과 테러리스트와 관련된 다양한 행동패턴 및 심리적 영향 등의 다양한 분야에 관한 사회과학적, 행동과학적인 이해를 목표로 하고 있다. ISVG가 일차적인 정보 수집에 보다 초점이 맞추어져 있었다면 START는 수집보다는 연구와 분석에 초점을 맞추고 있다는 점에서 그 차이를 보인다. 일례로 테러리스트에 대한 프로파일링도 수행하면서 이에 대한 데이터베이스를 구축하고 서비스를 제공하고 있다. 또한 이러한 효과적인 대테러 활동을 위해 필수적인 테러리즘과 테러리스트와 관련된 행동 패턴과 심리적 영향 등의 다각도의 분석을 통해 정보활동이 이루어지게 되었다.

특히, START는 전 세계에서 발생하는 테러와 함께 다양한 위험들에 대해서도 분석을 하고 연구를 진행하고 있다. 이와 관련하여 다양한 연구 분야를 갖고 있다.

- Terrorism and Violent Extremism
- Counterterrorism and Countering Violent Extremism
- Radicalization and De-radicalization
- Risk Communication and Resilience
- Unconventional Weapons and Technology

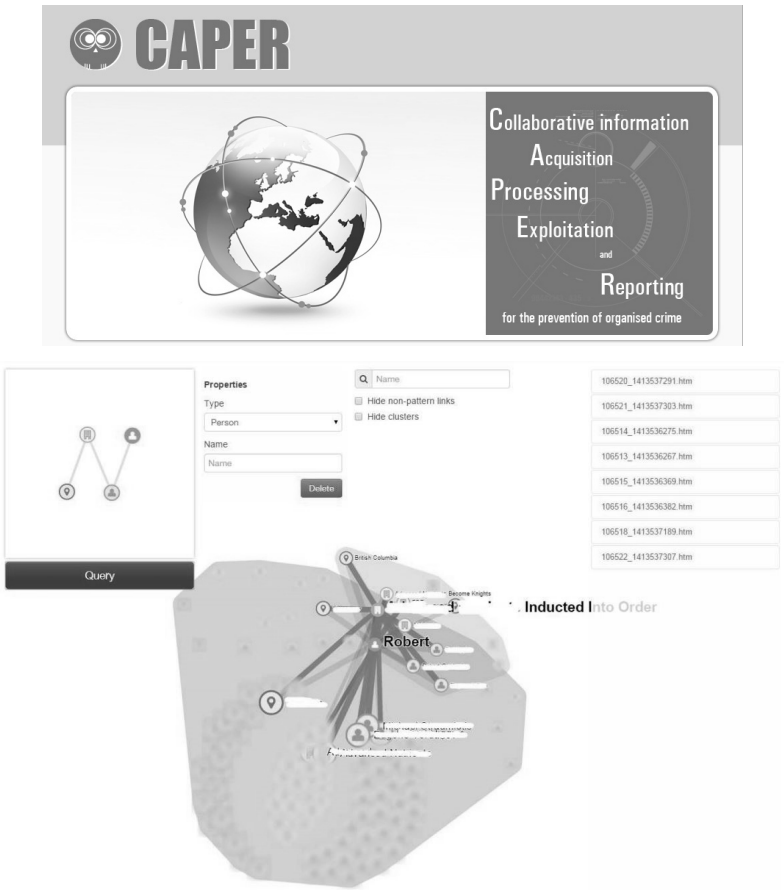
1.2.3 유럽의 OSINT프로젝트

유럽에서는 Open Source Intelligence의 유용성을 유럽연합 내에서 대규모의 예산을 여러 개의 FP7 프로젝트들을 지원함으로서 구축하고자 하였다.

(1) CAPER프로젝트: 이 프로젝트 역시 유럽연합에서 지원한 공개정보 분석 프로젝트이다. 2011년부터 2014년까지 약 3년 6개월간 EU의 지원을 받아 수행된 FP7 프로젝트인 CAPER는 법집행기관(LEAs)간의 정보공유를 위한 공동의 OSINT 플랫폼 개발을 목표로 두고 있다. 이러한 플랫폼을 구축함으로서 온라인 환경에서의 조직적 범죄를 효과적으로 탐지하고 예방하고자 하였으며 다양한 시각적 분석법, 자연언어처리 및 데이터 마이닝 기술을 이용하였다.

(2) RECOBIA 프로젝트: 또 다른 FP7 프로젝트로는 Reduction of Cognitive Biases in Intelligence Analysis (RECOBIA)가 있으며 이 프로젝트는 2012년부터 2015년까지 수행되었으며 정보를 분석할 때 발생하는 인지편향의 부정적 효과를 제거하여 분석의 품질향상을 꾀하는데 그 목적을 둔다.

CAPER project



(출처: http://www.fp7-caper.eu/)

(3) VIRTUOSO 프로젝트: 이 프로젝트는 2010년부터 2013년에 수행된 프로젝트로서 정보수집 및 분석시스템을 위한 표준화된 플랫폼 구축이 그 목적이다. 세부적으로는 공개출처정보를 이용하여 개방형 구조의 통합 툴킷을 개발하였으며 EU의 군, 사법당국, 및 주요부처와 협조하여 진행된 프로젝트이다.

(4) Search Engines for Military Intelligence 프로젝트: 군대를 위한 전략적 및 전술적인 차원의 정보 분석 도구에 대한 초기 연구가 그 목적이며 유럽 방위국 (EDA)의 의뢰로 독일의 Parmenides 재단과 공동연구를 진행하였다.

(5) Universal Intelligence Analyst Tool (UIA)프로젝트: 이 프로젝트 역시 EDA에 의해 2008년에 지원되었으며 군사적 사용을 위한 OSINT 어플리케이션에 대한 연구가 주된 연구목표였다.

1.3 OSINT를 통한 정보 수집과 분석

공개정보를 분석함으로서 다양한 중요정보를 추출할 수 있다는 사실이 OSINT의 중요성을 보여준다. 최근 인터넷 사용의 증가로 가장 유용하게 사용할 수 있는 공개정보는 Social Network Service 데이터로서 각국의 정세 파악이나 위협 정보를 취득가능하다.

각종 Social Network Service (출처: 해럴드 경제)

이러한 Social Network Service로부터 광대한 양의 정보를 수집하기 위해서 필요한 수집기술은 웹크롤링(Web Crawling) 기술이다. 웹크롤링 기술은 사이버상에서 얻을 수 있는 데이터가 증가함에 따라 사람이 수동으로 웹상의 데이터를 탐지하거나 수집이 어렵기에 이용되고 있다. 또한 빅데이터 분석을 위해서 활용되는 데이터가 뉴스, 블로그, 논문 및 특허 등 다양한 형태의 비정형 데이터들이 많기 때문에 이에 대한 선별적 데이터 수집과 함께 사이버상의 데이터들을 자동으로 가져오고 필요한 부분만을 추출하는 선택적 수집기술이 필요하기에 성능이 좋은 웹크롤러 개발이 OSINT기술에 있어서 성공의 잣대가 될 수 있다.

1.4 익명네트워크 Tor에서의 OSINT

이렇듯, 공개정보를 분석함으로서 다양한 중요정보를 추출할 수 있다는 사실이 OSINT의 중요성을 보여준다. 하지만, 우리가 간과하기 쉬운 사실이 한 가지 더 존재한다. 바로 공개정보라는 것이 인터넷의 기사나 논문 SNS와 같은 접근이 쉬운 정보들만을 의미하지 않는다는 점이다. 즉, 공개는 되었으나 접근이 상당히 어려운 정보들도 역시 공개정보라는 점이다. 이 점은 접근이 어려운 데이터나 인터넷상의 정보를 이용하여 원거리 통신을 수행하는 적국에 대응할 미래전과 관련하여 상당한 연관성을 제공한다. 최근의 정보보호 기술의 방향은

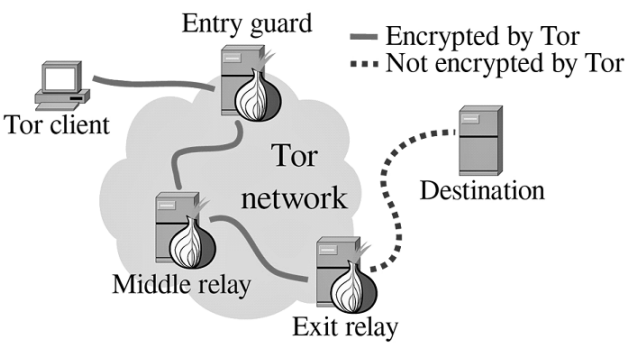
복잡도가 증가하는 환경에서의 정보보호 이슈와 함께 개인정보보호 및 프라이버시 보호이다. 기존에는 정보의 공개와 정보의 공유가 중요한 이슈였으나 최근 들어 프라이버시가 존중되는 환경에서의 정보 공유가 더 큰 이슈가 되고 있다. 이러한 전세계적인 분위기 속에 다양한 기술들이 나왔는데 그중 대표적인 기술이 바로 익명성을 보장하는 네트워크인 The Onion Routing (Tor, 토르)이다.

익명네트워크인 Tor

Tor 네트워크는 본래 정부의 온라인 통신 내용을 보호하기 위해서 미국 해군 연구소(The US Naval Research Laboratory)의 3G Onion Routing Project라는 이름으로 시작하였다. 하지만, 이후에 전 세계에서 온라인상의 익명을 보장하고 검열을 피하기 위한 목적으로 활용되었으며 아래와 같은 특징을 갖는다.

- Tor 네트워크의 사용자들은 그룹내의 다수의 서버들을 경유하여 목적지로 연결됨
- 사용자의 정보를 비밀로 지키며 일반적인 네트워크에 접속 가능
- 익명성 보장이 되는 환경에서 인터넷 연결과 이메일 송수신이 가능하다.

Tor 네트워크의 작동방법



(출처: https://fossbytes.com)

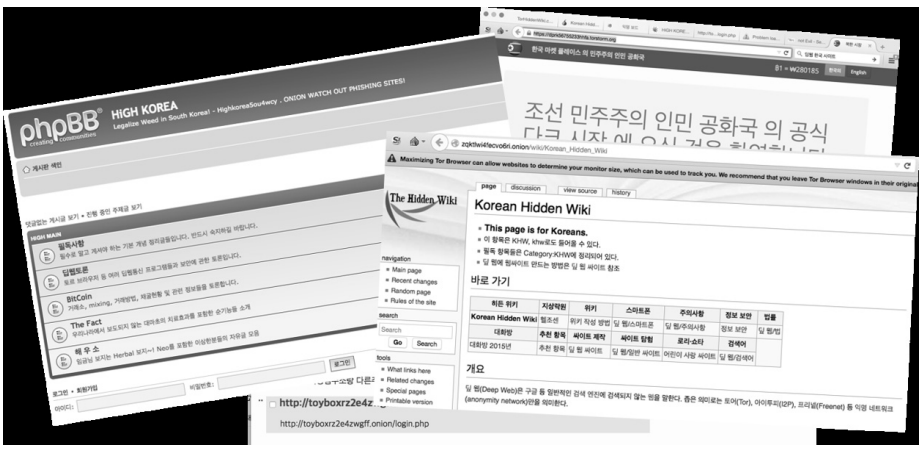
위의 그림에서 볼 수 있듯이 Tor 네트워크는 세 번의 암호화된 Path를 이동함으로서 익명성이 보장되는 네트워크이다. 그런데 본 보고서에서 기존 인터넷에서의 국방정보보호 이슈보다 Tor네트워크에서의 국방정보보호에 대한 이슈를 보다 중요하게 기술하고자 한다. 그 이유는 크게 두 가지가 존재한다. 첫째는 익명성을 보장하는 인터넷 문화가 확장하고 있다는 점이다. 아래의 그림을 보면 알 수 있듯이 전세계적으로 상당히 많은 이들이 익명네트워크를 이용하고 있다. 즉, 이렇게 사용자들이 증가함에 따라 보다 은밀하면서 비밀스러운 중요정보들이 이러한 익명네트워크에서 보다 잘 발견될 수 있다는 것을 역설적으로 표현하는 것일 수 있기 때문이다.

Tor Network내에서 현재 활동중인 노드수 (국내 27개)

또 다른 이유는 현재 각종 사이버 범죄나 블랙 해커나 적국의 스파이들이 범죄를 은폐하고 은밀하게 임무를 수행하고자 Tor와 같은 익명네트워크를 활용하고 있다는 점이다. 비록 Tor 네트워크가 익명성을 보장하고 내부적으로 특정 link를 찾는 것이 대단히 어려울 수 있겠으나 여기서 중요한 것은 바로 Tor와 같은 익명네트워크 역시 공개정보이라는 점이다. 그러므로 이러한 비밀 네트워크들로부터 중요 정보를 수집하는 방식을 찾아낸다면 보다 양질의 중요정보를 효과적으로 수집할 수 있다. 아래의 그림을 보면 세 개의 웹사이트를 볼 수 있다. 각각의 웹사이트는 북한의 대남사이트, 마약사이트 및 은닉정보를 갖는 사이트를 나타내며 이 모든 사이트가 익명네트워크인 Tor네트워크 내에서 엄연히 운영 중에 있다. 이러한 익명화된 네트워크는 운영자를 추적하기 어렵기 때문에 직접 수사를 해서 운영진을 잡는 것이 거의 불가능에 가까우므로 대남사이트와 같은 불법을 저지르는 운영자들은 그들

의 목적을 이러한 익명네트워크로부터 취할 수 있다. 비록 이들을 체포하거나 수사하는 것은 어려운 일이나 이러한 Tor내에 공개된 정보들을 이용하여 각종 범죄자들의 동향에 대한 첩보를 수집할 수 있다. 또한 이러한 테러범들이나 산업스파이 등의 비밀리에 움직이는 조직들도 이러한 익명 네트워크를 사용할 수 있으므로 이러한 공개정보가 국가안보 및 국방정보보호 개념에서 중요한 위치를 차지한다고 볼 수 있다.

Tor네트워크에 존재하는 다양한 불법 공개정보들



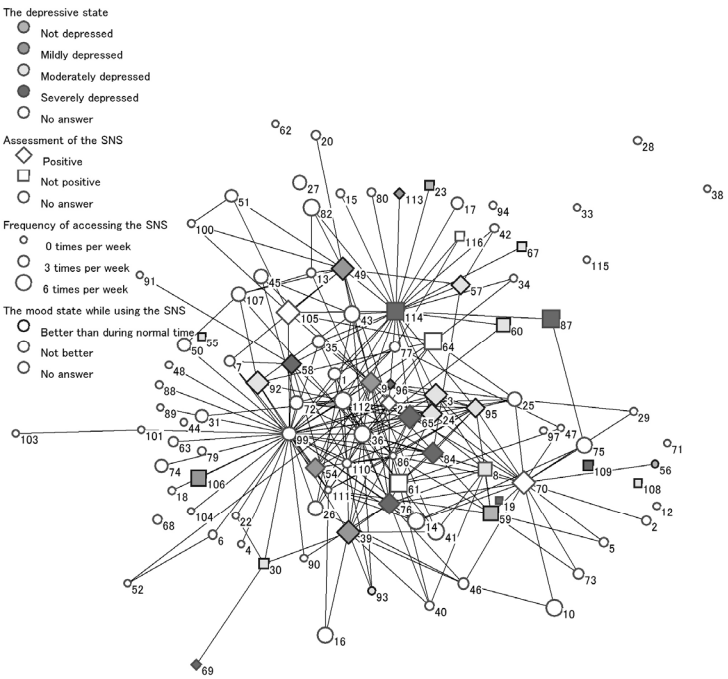
1.5 국방정보보호를 위한 OSINT 활용방안

그렇다면 이러한 OSINT를 국방정보보호를 위해서 어떻게 사용가능한가? 다양한 공개정보 소스로부터 수집한 공개정보들은 정형화 과정과 일련의 데이터 정제과정을 거쳐서 분석과정에 이른다. 이로써 공개정보는 유의미한 중요 정보로 바뀌게 되는 것이다. 이러한 점에서 OSINT는 투명한 정보를 검색 및 수집하고 각 정보나 객체들간의 숨겨진 관계를 찾아내는 것이 하나의 큰 목표로서 최근의 이슈였던 빅데이터 분석과도 연관이 있다. 이러한 공개정보 분석을 통해서 우리기 얻을 수 있는 주요 국방정보보호 기술은 크게 두가지를 둘 수 있다.

1.5.1 악성코드 개발자 프로파일링

예를 들어, 공개 정보 내에 존재하는 객체들 간의 연결 관계는 노드(node)와 엣지(Edge)들로 해당 내용을 정리할 수 있다. 아래 그림과 같이 각각의 노드들은 크기나 모양으로 각 노드의 특징들이나 정도를 나타낼 수 있으며 엣지들은 각 노드들 간의 종속성이나 원인과 결과 또는 상호 연관성을 나타낸다.

SNS상에서 각 노드들의 연결을 보여주는 Social Network



우리가 주목해야 하는 부분은 바로 관계를 뽑아내는 그 노드들이 바로 각각의 악성코드일 수도 있고 또는 악성코드를 개발한 개발자가 될 수 있다. 이러한 방식으로 접근함으로서 악성코드 개발자들을 기계학습 기술인 분류법(Classification)과 그룹핑(Clustering) 기법을 이용하여 프로파일링할 수 있다. 이러한 프로파일링 기술은 기존에 해킹흔적을 보고 침입한 해커들의 프로파일링을 구축했던 사이버 게놈 프로젝트(Cyber Genome Project)와 상당한 부분에서 일치한다. 즉, 해커들이 남긴 흔적뿐만 아니라, 악성코드 자체를 역공학을 이용하여 숨겨진 개발자이 코드패턴이나 스타일을 찾아낼수 있고 또한 난독화 스타일을 통해 개발자들의 프로파일링이 가능해진다.

1.5.2 OSINT를 이용한 세계 정세 파악 및 사건 사고 예측

실시간으로 얻어지는 공개정보는 전세계에서 어떤 사건이 일어나는지 그리고 해당 국가나 지역의 현재 정세와 가까운 미래를 엿볼 수 있다. 예를 들어, 트위터 정보를 통해서 현재 각국의 움직임이나 시시각각 변하는 정치적 안정 및 대외비밀로 여겨져야 할 고급정보가 공개소스에 노출됨으로서 가까운 미래에 일어날 사건사고들을 예측이 가능해진다. 이러한 주변국에 대한 사건사고 파악 및 예측은 국가간 정보우위를 선점할 수 있기 그 가치가 높다고

말할수 있다. 반대로, 이러한 OSINT기술을 이용하여 내부적으로는 국내에서 발생할수 있는 비공개 사건사고에 대한 노출을 미연에 방지할수 있고 사건사고 발생시 보고체계에 의한 연락망보다 보다 신속정확하게 대처가 가능해진다. 또한 국내 정세 및 국가적 위협신호를 OSINT로부터 얻어낸다면 국가안보차원에서 의미가 있다. 아래의 그림은 Twitter와 같은 SNS상의 공개정보들을 수집하여 중국, 미국, 러시아, 일본, 대한민국에서 실시간으로 어떤 정보가 오가는지를 실시간으로 관제할 수 있는 시스템을 보여주고 있다. 각 분야 별로 특이점을 찾아냄으로서 시시각각 변화하는 국방관련 세계정세를 신속하게 파악할 수 있게 된다. 그러므로 이러한 관제 시스템 구축을 위해서 국가적으로 지원이 필요하다.

공개정보를 이용한 세계정세 파악 시스템 (출처: 고려대학교 정보보호대학원)

참 고 문 헌

[1] 조남훈, “과학기술 진보와 미래전 양상”, 電子工學會誌 第37卷 第11號, 2010.11, 16-26

[2] 유진철, 이원우, 임원택, 신규용, “한국군에 적합한 네트워크 작전 수행방안 연구”, 국방연구, 제 55권 제 2호, 2012, 6, 47-75

[3] 시만텍, “지능형 지속 위협 (APT): 시만텍의 관점”, http://www.s-online.co.kr/symantec_Library/FTP/PDF/WP/WP_APT_KR.pdf

[4] BBC news, “China military unit ‘behind prolific hacking”, 19, February, 2013, http://www.bbc.com/news/world-asia-china-21502088

[5] CNN news, “Hackers stole data on Pentagon's newest fighter jet”, 21, April, 2009, http://edition.cnn.com/2009/US/04/21/pentagon.hacked/

[6] 한국인터넷진흥원 (KISA), “KISA 보호나라 & KrCERT”, 2016, https://www.krcert.or.kr/ransomware

[7] 장영준, “사회 공학 기법과 악성코드 집중 분석”, 안철수연구소 전문가칼럼, 24. April, 2007

[8] 보안뉴스, “[긴급] 신종 랜섬웨어 ‘록키’ 국내 금융기관 유입”, 22, Febrary, 2016, http://www.boannews.com/media/view.asp?idx=49684

[9] 안철수연구소, “랜섬웨어, ‘이것’이 궁금하다!”, 29, June, 2016. http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=25176

[10] 김종현, 김현주, 김익균, “악성코드 대응을 위한 사이버게놈 기술동향”, 30권, 5호, 2015. 10. 01. 118-128

[11] 엄정호, “사이버공간에서 정보우세를 위한 사이버 방위전략”, 보안공학연구논문지, 제 9권 제 5호, 2012년 10월, 377-386

[12] 염흥렬, “사이버 테러 및 대응 사례 [2015 국가위기관리 종합보고서] 북한의 사이버 위협과 우리의 대응”, 블루투데이 2016.03.14

[13] Stuart Russell and Peter Norvig, “Artificial Intelligence: A modern approach”, The third edition, Pearson Publisher, 2010

[14] Kalyan Veeramachaneni, Ignacio Arnaldo and Vamsi Korrapati, “AI2: Training a big data machine to defend”, IEEE 2nd International Conference on Big Data Security on Cloud, 2016, 49-54

[15] Y. Benglo, “Learning deep architecture for AI”, Foundations and Trends in Machine Learning, Vol. 2, No. 1, 1-127, 2009

[16] J. Markoff, “How many computers to identify a car?”, The New York Times, June 25, 2012