사이버 전쟁 대비 및 테러 수사

2023년 7월

경 찰 청
임 석 우

< 차 례 >

Ⅰ. 국외훈련 개요

Ⅱ. 훈련기관 개요

Ⅲ. 서론
1. 연구 배경
2. 연구의 필요성

Ⅳ. 본론
1. 대한민국의 사이버 보안 현황
2. 싱가포르 사이버 보안 전략
3. 싱가포르 사이버 보안 관련 법률
4. 싱가포르 주요 사이버 보안 사고
5. 싱가포르 사이버 보안청
6. 싱가포르 경찰청 현장연수

Ⅴ 결론

Ⅵ 수집자료 및 기타 참고문헌

Ⅰ. 국외훈련 개요

1. 훈련국 : 싱가포르

2. 훈련기관명 : 싱가포르 국립대학교 (National University of Singapore)

3. 훈련분야 : 수사

4. 훈련내용 : 싱가포르 국립대학교 컴퓨터 대학교(School of computing)에 있는 '국립 사이버보안 연구실 (National Cybersecurity research & development Lab)에서 싱가포르 사이버 보안 정책에 대하여 연구하였고, 싱가포르 경찰청 소속 사이버 범죄 사령부 (CyberCrime Command)에서 현장훈련을 하였으며, 싱가포르 사이버보안청, 인터폴 등을 방문하여 싱가포르 사이버 보안 전략에 대해 연구하였다.

4. 훈련기간 : 2022.12월 ~ 2023.6월

Ⅱ. 훈련기관 개요

1. 기관개요

○ 훈련국 : 싱가포르

○ 훈련기관 : 싱가포르 국립 대학교 (National University of Singapore) 컴퓨터 대학(School of computing) '국가 사이버보안 연구소 (National Cybersecurity research & development Lab)

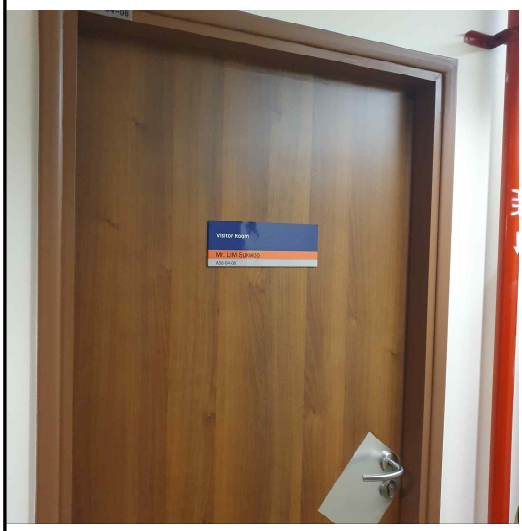
○ 인터넷 웹주소 : www.ncl.sg

○ 주소 : 21 Lower Kent Ridge Road, Singapore 119077

○ 전화번호 : +65 6516 6666

○ 연구실 주소 : AS6-04-06 (Art and science 빌딩 4층 6호

< NUS에서 제공한 연구실 사진 >



2. 기관소개

가. 싱가포르 국립 대학교(National University of Singapore)

○ 싱가포르 국립대학교(National University of Singapore, NUS)는 싱가포르에서 가장 오래된 대학이자 규모도 가장 큰 대학고, QS 세계 대학 랭킹에서 아시아 대학 종합 1위를 차지하고 있는 대학이다. 영국 식미지 시절인 1905년에 설립되었고 1980년 난양 공과대학교의 전신인 난양대학교(NAnyang University)가 싱가포르 대학과 합병되어 현재의 싱가포르 국립대학이 되었다.

나. 싱가포르 국립 대학교 컴퓨터 대학 (School of computing)

○ 싱가포르 국립대학교 컴퓨터 대학(School of computing)은 1988년에 설립되었고 컴퓨터 과학(computer science)와 정보 시스템(Information Systems and Analytics) 학과가 있다. 그리고 컴퓨터 대학에는 여러개의 연구소가 있는데 특히 사이버 보안과 관련된 연구소는 2개가 있다.

○ NUS-NCS Joint Laboratory for Cyber Security와 National Cybersecurity research & development Lab이다. 싱가포르 국립대학교(NUS)와 NCS Pte. Ltd. (NCS)는 2021년 6월 사이버 위협으로부터 개인, 기업 및 공공 기관을 보호하기 위한 능력과 혁신적인 디지털 솔루션을 개발하기 위해 NUS에 합동 연구소를 설립하였다. 주요 연구분야는 AI Security, Cyber-Physical System Security Data Security and Privacy이다.

다. 국가 사이버보안 연구소 (National Cybersecurity research & development Lab)

○ 지도교수 : Chang Ee-Chien, Associate Professor

○ 프로그램 디렉터 : Seah Choon Meng

○ 전화 : +65 6601 1056

○ 주소 : NCL COM3 - B1 - 09 Computing3, 11 Research Link Singapore 119391

○ 소개

국가사이버보안연구소(National Cybersecurity R&D Laboratory, NCL)는 2015년에 설립되었다. 연구소는 사이버보안 연구 및 개발을 위한 컴퓨팅 자원, 사이버 보안 실험 환경 및 응용 서비스를 지원하는 연구소이다.

연구소에는 다양한 보안 데이터 및 보안 서비스를 제공하는 300개의 노드로 구성된 클러스터가 포함되어 있고, 연구 결과의 공유와 검증을 통해 학계, 산업 및 정부 기관의 연구자들 간의 협력을 촉진하고 장려하는 플랫폼을 제공하기 위해 노력하고 있다.

연구소는 위와 같은 사이버 보안 장비를 이용하여 해킹 대회를 개최하기도 하고 다른 해킹 대회의 운영을 위한 서비스를 제공하고한다. 예를 들어 본 훈련생이 참가한 Catch The Flag, Gray Cat 등 해킹 대회를 직접 개최하기도 하였고, Nato 주관 에스토니아서 개최된 Locked Shield 대회에서 그린팀으로 참가하였다.

< NCL 홈페이지 본 훈련생 소개 >

NCL Technology Updates

Mr. Sukwoo Lin, a Visiting Researcher to National Cybersecurity R&D Lab (NCL)

March 08, 2023

National Cybersecurity R&D Lab (NCL) is very happy to host Mr. Sukwoo Lin as a Visiting Researcher, who have been selected for overseas training program sponsored by Korean Government. He is a Superintendent of the Korean National Police Agency (KNPA).

From left to right: Mr Seah Choon Meng (Program Director, NCL); Mr Sukwoo Lim (Visitor); Associate Professor Chang Ee-Chien (Principal Investigator, NCL)

Mr Sukwoo Lim has been working in Korean national police agency since 2016. Currently, he is working as a chief of criminal department at the Yeongdeungpo police station in Seoul, South Korea. Prior to joining the police, he worked as a lawyer for 3 years. He majored in Electrical Engineering. He has conducted investigations specializing in cyber terrorism and hacking investigations.

His research topics focus on the cybersecurity law of Singapore, the role of the Cyber Security Agency as well as the cooperative relationship between the Cyber Security Agency and the Singapore Police Force in cyber-terrorism investigations.

To leave a comment, click the button below to sign in with Google.

SIGN IN WITH GOOGLE

< NCL-CSA 모의 해킹대회 참가 모습>

NCL Technology Updates

NCL - CSA - Advanced Youth Cyber Exploration Programme (AYCEP) 2023

June 21, 2023

National Cybersecurity R&D Lab (NCL) would like to express our gratitude to the Cyber Security Agency of Singapore (CSA) for involving NCL as a co-partner for the Advanced Youth Cyber Exploration Programme (AYCEP) that was held on 06-07 June 2023. AYCEP showcased the immense potential and passion of Singapore's youth in the field of cybersecurity and provided a platform for collaboration, learning, and growth.

Together with Horangi, NCL provided technical training on Day 1 of AYCEP to prepare the participants for the CTF challenge. The final CTF round and table-top exercise scenarios was held in ASEAN-Singapore Cybersecurity Centre for Excellence on 07th June 2023. NCL was also part of the judging panel for the tabletop exercise. It was an incredible experience witnessing the dedication, problem-solving skills, and teamwork displayed by the participants as they tackled challenging questions and scenarios.

Congratulations to all the participants and winners of AYCEP! Your remarkable performances and commitment to cybersecurity excellence are truly inspiring. I applaud your dedication and enthusiasm to secure our digital future. Your passion and talent are the driving force behind a safer and more secure digital world.

We would also like to extend our sincere thanks to the Whitehat Society for their invaluable support in making the event a resounding success.

Ⅲ. 서론

1. 연구배경

○ 사이버 전쟁(cyber Warfare)[1)]

사이버 전쟁이란 국가/배후 조직이나 세력이 컴퓨터 바이러스나 DDos 등 수단을 사용하여 국가의 컴퓨터 시스템과 정보 네트워크에 운영상 중대한 위해를 가하는 것을 의미한다. 미국 사이버 보안 및 인프라 보안국(CISA)은 사이버 전쟁의 목적이 상대 국가의 약화 분열 혹은 파괴시키는 것이라고 정의 한다. 즉 사이버 전쟁이란 공격주체의 의도와 공격의 규모가 국가 시스템을 붕괴시키거나 위태롭게 만드는 효과를 노리는 것이라고 할 수 있다.

사이버 공격의 형태로는 랜섬웨어 디도스 공격 스파이웨어 공격뿐만 아니라 사이버 공간에서 허위정보를 흘려 상대방을 교란하는 등의 사이버 심리전도 포함한다. 현대전쟁은 물리적 타격과 사이버공격이 결합 된 하이브리드 전쟁이라고 표현할 수 있다. 국가주요시설 습격 및 미사일 피격, 주요 요인 암살과 같은 군사적 공격뿐만 아니라 눈에 보이지 않는 사이버공격을 통한 국가 통신망 마비, 가짜뉴스 유포, 정치공작 등 비군사적 공격으로 상대방에게 더 큰 타격을 입힐 수 있다.

○ 러시아-우크라이나 전쟁[2)]

2022년 러시아-우크라이나 전쟁 현대 전면전, 총력전에서 서이버 전

1) 2022 한화원, [사이버 전쟁 에 대한 법적 규율에 관한 연구]
2) 2022 사이버 보안 컨퍼런스 송태은 국립외교원 교수 발표

쟁이 실제로 어떻게 전개되는지 어떤 파괴력을 발휘하거나 한계를 갖는지 관찰할 수 있는 첫 번째 사례라고 할 수 있다. 그 동안 사이버 공격은 대부분 물리력을 동반하지 않는 사이버 공격이나 낮은 강도의 국지전에서의 사이버 공격이었다.

러시아는 2022. 2. 24. 우크라이나를 상대로 선전포고를 하고 전차와 전투를 이용한 공격을 개시하였다. 그러나 선전포고 이전에 군 통신, 인터넷, 라디오 및 국영방송, 핵발전소 에너지시설 등 국가기반시설에 대한 사이버공격을 시도한 것이 확인 되었고, 물리적 타격과 사이버 공격이 동시에 합동작전처럼 진행이 되기도 하였다.

○ 러시아-우크라이나 사이버 전쟁[3)]

러시아-우크라이나 전쟁에서 사이버 공격은 물리적 공격에 앞서 전세를 공격자에게 유리하게 만드는 전초전 기능을 수행하였다. 러시아 전쟁은 2월 24일에 발생하였으나 러시아는 그 이전부터 사이버 공격을 지속적으로 전개하였다. 러시아는 우크라이나의 주요 인프라 핵심 네트워크에 타격을 주어 정부 대중에 충격과 혼란에 빠트리게 하고 우크라이나의 반격을 지체시키는데 목적이 있었다. 즉 러시아는 전쟁의 전세를 유리하게 하고 신속한 물리공격과 침략을 신속히 진행할 목적이었다.

러시아는 2022. 1. 14. 우크라이나 외교부, 에너지부, 재무부 등 관련부터 약 70개의 홈페이지에 대해 사이버 공격을 하여 홈페이지를 마비시켰다. 그리고 2022. 1. 15. 우크라이나 정부 홈페이지에 ‘위스퍼게이트(Whispergate)’라고 불리는 해킹공격(Malware)을 하였다. 2022. 2. 15와 16.에는 우크라이나 국방부, 국무부 등의 홈페이지와 은행 시스템에 대하여 DDos 공격을 하였다. 특히 러시아는 우크라이나에 대

3) IFANS 주요국제문제분석 2022-19 러시아-우크라이나 전쟁의 사이버전: 평가와 함의 송태은

한 선전포고 전날 우크라이나 정부 기관과 민간 기업의 300여개 시스템에 대해 ‘헐메틱와이퍼(HermeticWiper)’로 불리는 대규모의 와이퍼 공격을 하여 국가 사회의 혼란을 야기하였다.

물리적 군사 공격과 사이버 공격이 합동작전 하듯이 발생한 사실도 있다. 사이버 공격은 전통적인 군사수단과 완전히 결합되어 조직적으로 전개된다. 예를 들어 3월 1일 키이우 TV 타워가 폭격을 받은 동시에 우크라이나 키이우시 미디어 회사를 해킹하여 데이터를 탈취한다던지 원전을 군사적으로 점령하면서 동시에 원전회사 네트워크를 마비시키거나 정부기관에 대해 사이버 공격을 하면서 공항과 정부건물을 폭격하는 일이 발생하였다.

러시아는 사이버 심리전도 활발히 진행 진행하였다. 러시아가 이미 키이우를 탈환하였다거나 우크라이나 대통령 젤란스키가 항복을 하였다는 등의 가짜뉴스를 퍼트렸고, 러시아 침략을 정당화 하는 내용의 글과 영상들이 급속히 공유되었다. 그러나 주요 소셜미디어의 운영주체가 페이스북 트위터 등이 미국 회사에 의해 운영되므로 가짜뉴스의 확산이 신속히 제한되어 우크라이나는 혼란에 하지지 않았다.

○ 우크라이나의 사이버 전쟁 대응[4)]

이번 전쟁에서 러시아는 다양하고 정교하며 파괴적인 사이버 공격을 하였으나, 우크라이나는 대체로 방어를 잘 해내었다.

러시아는 2014년 3월 크림반도 합병 과정에서 사이버 테러와 심리전 등 사이버 공격으로 정치적 경제적 전복활동을 전개하였고 우크라이나군과 직접 교전없이 우크라이나의 군사기지 의회 대법원 공항 등을 점령하고 크림반도를 합병할 수 있었다. 그러나 NATO는 2014년 러시

4) 2022 이용석, 정경두, [한국국방연구원] [러시아 대 우크라이나 사이버 전쟁의 교훈과 시사점]

아의 우크라이나 침공 및 크림반도 합병 이후 러시아의 사이버 전쟁을 포함한 하이브리드 위험에 적극적으로 준비를 해왔다.

NATO는 2014년 러시아의 우크라이나 침공 및 크림반도 합병 이후 러시아의 사이버 전쟁을 포함한 하이브리드 위험에 적극적으로 대응해 왔다. 러시아-우크라이나 전쟁은 사이버 전쟁 위협에 대한 대응태세 효과를 검증하는 중요한 시험대였다. NATO는 사이버 공격과 심리전 및 복합전에 대한 다양한 준비를 하였고 이러한 대응으로 러시아의 사이버 공격을 막아낼 수 있었다.

NATO는 2015년 3월 'East StartCom Task Force'를 조직하여 러시아의 사이버 테러 및 심리전에 취약한 동유럽 국가대르에 대한 지원을 하였고, 우크라이나 PSYOP팀은 2020년 1월 독일에서 진행되는 'Combined Resolve XIII' 군사훈련에 참여하였으며, 미국과 이라크-아프가니스탄 전쟁과 크림반도 전쟁 경험을 교환하는 등 사이버 공격과 심리전 등 복합 전쟁에 대한 다양한 준비를 하였다.

러시아는 2022. 2. 24. 전쟁을 시작하면서 가장 먼저 우크라이나의 인터넷 통신과 미디어 인프라에 대한 군사공격을 시작하였고, 우크라이나 군의 지휘 통제 통신 서비스인 미국 인터넷 회사 VISAT에 대해 사이버 공격을 하였다. 그러나 일론 머스크의 스페이스엑스 스타링크가 우크라이나에 신속하게 인터넷 서비스를 제공하여 우크라이나의 사이버 공간에 대한 접근이 정상화 되면서 군의 지회 통제가 확립되고 가짜뉴스 등에 대한 혼란이 발생하지 않았다. 결국 이러한 조치가 군과 민간이 러시아에 강력하게 항전할 수 있는데 큰 기여를 하였다.

러시아는 WIPER ATTACK으로 우크라이나 주요 기관 데이터를 삭제하는 공격을 하였으나 우크라이나는 데이터 정책을 변경하여 자국 주요 기관 데이터를 MICROSOFT 클라우드로 이동하여 데이터를 보존할

수 있었다.

2. 연구의 필요성

○ 북한의 사이버 공격 위협

북한에게 있어서 사이버 전력은 핵·생화학 무기와 함께 북한의 3대 비대칭 전력이다. 하버드 케네디 대학의 벨퍼센터가 제공하는 '사이버국력지수(NCPI)'를 통해 파악된 북한의 종합적인 사이버 역량은 2022년 세계 14위를 차지하고 있다. 북한의 사이버 공격은 지능적이고 정교해 지고 있으며, 국가핵심시설에 대한 은밀한 침투를 통해 국가안보와 직결되는 정보를 유출하고 있다. 그리고 최근 들어서는 가상화폐를 해킹하는 등 불법적인 금융활동을 통해 핵개발 등의 자금을 조달하고 있다.

○ 싱가포르의 사이버 안보 전략

싱가포르는 2017년 국제전기통신연합(ITU) 발표한 국제정보보호지수(Global Cybersecurity Index)에서 1등을 하였고 이후 계속하여 상위권을 유지하고 있다. 그리고 2014년 인터폴 제2청사(Interpol Global Complex for innovation, IGCI)를 유치하여 인터폴 사이버수사를 총괄하는 등 아시아의 사이버 보안의 대표 국가이다.

싱가포르 정부는 2015. 4. 1. 사이버보안 관련 모든 정부기관을 하나로 모아 사이버보안청(Cyber Security Agency, CSA)을 설립하고, 2017. 7. 사이버보안법이 제정하였으며, 국가사이버안보 전략을 발표

하는 등 사이버 안보관련 법과 제도를 정비하였다.

○ 과제 연구의 필요성

우리나라는 인터넷 등 고도화된 정보통신기술을 갖추고 있으나, 북한의 사이버테러 공격으로 국가 전산망이 마비되거나 국가 핵심 방산 자료가 해킹되는 등 사이버 전쟁 위협에 노출되어 있다. 특히 최근 우크라이나-러시아 전쟁 관련 사이버 전쟁이 확대되고 있고, 러시아 경제제재 참여국 대상 사이버 보복 우려가 높아지고 있다. 따라서 북한의 사이버 전쟁과 러시아의 사이버 공격에 대한 대비가 필요하다.

윤석열 정부는 ‘국가사이버안보위’를 설치하고 사이버보안 법령을 제정하겠다고 공약하였다. 싱가포르 사이버보안 컨트롤 타워인 싱가포르 사이버 보안청과 사이버 보안법 등을 연구하여 윤석열 정부의 ‘국가사이버안보위’ 설치와 관련된 정책 수립과 국가사이버보안 기법법 제정 등의 법령제정에 활용할 필요가 있다.

결국 싱가포르와 대한민국의 사이버 보안 전략을 비교 연구하여 사이버 전쟁 대비 및 테러 수사에 대한 현실적이고 효율적인 사이버 안보 정책을 제안하고자 한다.

Ⅳ. 본론

1. 한국의 사이버 보안 현황

○ 북한의 사이버 공격[5)6)]

북한에게 있어서 사이버 전력은 핵·생화학 무기와 함께 북한의 3대 비대칭 전력이다. 하버드 케네디 대학의 벨퍼센터가 제공하는 '사이버국력지수(NCPI)'를 통해 파악된 북한의 종합적인 사이버 역량은 2022년 세계 14위를 차지하고 있으며 사이버 역량의 상당 부분이 사이버 공격 활동과 불법적인 금융 활동에 집중되어 있다.

북한 해커조직은 2022년 총 16억 5천만 달러(약 2조670억 원)의 가상자산를 탈취하였다고 알려졌다. 그리고 북한은 금융사 전산망 공격(2013. 3. 20), DDoS 공격(2011. 3. 4., 2009. 7. 7.), 한수원 원전 해킹 사건(2014. 12.) 등 국가핵심시설에 대한 사이버 공격을 하였다. 2021년에는 한국항공우주산업(KAI)과 원자력연구원-대우조선해양이 해킹되어, 국산 전투기 설계 도면과 원자력 추진 핵잠수함 자료가 유출되었다. 그러나 해킹의 증거 확보와 피의자 추적에 어려움을 겪고 있으며 국가안보와 관련된 핵심 방산기밀이 북한으로 유출되고 있다.

○ 한국의 사이버 보안 현황

국회는 2016. 3. 2. 테러방지법을 제정하였으나, 후속 입법으로 추진

5) IFANS FOCUS 2022-28K(송태은) 북한의 사이버 공격과 우리의 대응
6) 2121 유동열 [(사)한국전략문제연구소] [북한의 사이버 위협 실태와 대응]

되던 사이버테러방지법이 시민·사회단체의 반대로 제정되지 못하였다. 정부는 국가안보실에 사이버안보비서관을 설치하였으나 폐지되었고, 현재 경찰 국정원 등 여러 기관에 나누어져 사이버보안 컨트롤타워가 부재한 상황이다.

정부는 2003년 이후 수차례 사이버안보정책을 수립하고 그때 마다 사이버안보 컨트롤타워를 지정하고 운영해 왔다. 이 과정에서 사이버 안보 조직의 역할과 기능이 성장하였지만, 일관성 없는 사이버 안보 정책과 투명하지 않은 정책 활동으로 여러 차례 지적을 받아왔다.

○ 청와대 국가안보실 「국가 사이버 안보전략」[7)]

정부는 2019년 4월 사이버 안보 정책 방향을 담은 국가 사이버 안보 전략을 발간하였다. 정부는 자유롭고 안전한 사이버공간을 구현해 국가 안보와 경제 발전을 뒷받침하고 국제 평화에 기여한다는 것을 국가 사이버안보 비전으로 제시했다. 3대 목표는 국가 주요기능의 안정적 수행, 사이버공격에 빈틈없는 대응, 튼튼한 사이버안보 기반 구축이다. 3대 기본원칙은 국민 기본권과 사이버안보의 조화, 법치주의 기반 안보활동 전개, 참여와 협력의 수행체계 구축이다.

국가사이버안보 전략과제는 ①국가 핵심 인프라 안전성 제고, ②사이버공격 대응역량 고도화 ③신뢰와 협력 기반 거버넌스 정립 ④사이버보안 산업 성장기반 구축 ⑤사이버보안 문화 정착 ⑥사이버안보 국제협력 선도 6가지다. 정부는 전략을 구체화하고 성실히 실행하기 위해 「국가 사이버안보기본계획」과 「국가 사이버안보 시행계획」

7) 2019년 청와대 안보실 발간 '국가사이버안보전략'

을 수립하여 추진한다고 하였다. 2019년 9월 국가사이버안보 기본계획과 시행계획을 발표하였다. 그리고 2019년 6월 국가 사이버안보 기본계획을 발표하고 사이버안보 6대 전략과제를 뒷받침하기 위해 기관별 실행계획을 18개 중점과제, 100개의 세부과제로 종합해 2022년까지 단계적으로 추진하겠다고 발표하였다.

그 이후 뉴스 프리존이라는 언론은 사이버안보정책 관련 정보공개 청구를 하여 분석한 결과 국가사이버안보 관련 정부의 후속 대책은 지지부진하다고 평가하였다.[8]. 국가사이버안보 전략이 정권과 관계없이 지속적으로, 그리고 제대로 추진되려면 반드시 법적・제도적 뒷받침이 필수적으로 선행되어야 하지만 2006년 노무현 정부 시절부터 사이버 위기 대응을 위한 범국가 차원의 기본법을 마련하기 시작했지만, 17년이 지난 지금까지도 제정되지 못하고 있다.[9]

○ 윤석열 정부의 사이버안보 전략[10]

윤석열 정부는 국가 사이버안보 대응역량을 강화하겠다고 발표하였다. 대통령 직속 국가사이버안보위를 설치하여 컨트롤 타워 운영체계 기관별 역할 등을 규정한 법령제정을 추진하여 국가 기관 간 협력을 활성화 하는 등 체계를 정비한다고 발표하였다.

민관 합동 사이버 협력체계 강화를 통해 핵심기술 보유기업 방산업체 국가기반시설에 대상 해킹 보호에 총력을 경주하여 경제안보에 기여할 것이고, 産·學·硏·官 협력아래 AI·양자통신 등 신기술 위협 대

8) 2022. 3. 11. 이기종 [뉴스프리존] [사이버안보정책2] 이대로 좋은가 입만 살아있는 사이버 안보 컨트롤'
9) 2020. 4. 6. 이기종 [뉴스프리존] [정부,'국가사이버안보전략' 수립 이후 1년간 성과와 향후과제는?]
10) 2023. 6. 7. 국가안보실 [윤석열 정부의 국가안보전략]

응 기술개발 및 국제공조 활성화, 사이버 위협에 대한 억지역량 배가하고, 신기술 연구 개발을 적극 지원, 해킹 탐지 차단 추적 시스템 고도화 국제사회의 사이버규범 수립에 적극 참여하고, 글로벌 협력 네트워크를 확충하며, 대학·특성화 교육 확대, 지역별 교육센터 설치 등 '10만 인재 양성' 프로그램을 가동하고, '사이버 예비군' 운영 등 사이버전 인력확보 하겠다고 발표하였다.

정부는 2022년 12월 '북한 IT 인력에 대한 정부 합동주의보'를 발표하고, 국정원의 국가사이버안보센터와 군의 사이버작전사령부는 2023년 5월 1일 업무협약(MOU)를 체결하는 등 부처 간 공조를 강화하였다. 그리고 국정원 산하 국가사이버안보센터는 2022년 11월 판교에 '국가사이버안보협력센터'를 개소하여 정부와 기업 간 사이버 안보 위협에 공조를 증가시키기 위해 노력하고 있다.

한국의 사이버작전사령부는 2022년 10월 미국사이버사령부가 주최하는 다국적군 사이버 군사훈련인 '사이버플래그'에 참가하였고, 2023년 2월 한미는 '북한의 중요 기반시설에 대한 랜섬웨어 공격 및 스파이 활동' 제하의 '한미 합동 사이버보안 권고문'을 발표하여 북한의 사이버 위협에 대해 대내외적으로 경고하는 조치하는 등 미국과의 사이버 분야 한미 동맹을 강화 하였다[11].

11) 2023. 6. 2. 대한민국정책브리핑 [한미 사이버보안 공동지침 마련]

2. 싱가포르 사이버 보안 전략

가. 개요[12)]

전 세계적으로 랜섬웨어, 사이버 사기, 해킹, 인터넷 서비스 중단 등 사이버 테러가 빈번하게 발생하자, 싱가포르는 2005년 최초로 infocomm 보안 마스터플랜을 발표하면서 사이버 보안 기능을 강화하기 시작하였다. 2009년 SITSA (Singapore Information Technology Security Authority)를 설립하여 대규모 사이버 공격 특히 중요 정보 인프라에 대한 국가적 차원의 대응을 개발하였다.

2015년 사이버 보안청(Cyber Security Agency)을 설립하여 국가 사이버 보안의 모든 기능을 감독하고 조정 하도록 하였고, 사이버 보안 규정, 정책 및 관행을 개발하고 시행하는 권한을 부여하였다. 그리고 2016년과 2021년 싱가포르 사이버 보안 전략을 발표하여 주요 목표를 설정하고 이를 실행해 나감으로써 사이버 보안 강국으로 성장하고 있다.

나. 주요 연혁

1) 2005년 Infocomm Security Masterplan (ISMP)

정보통신개발청(IDA)는 싱가포르 최초의 정보통신 보안 마스터 플랜을 설계하고 정부의 사이버 보안 제도를 구축하였다. 주요 내용은 사이버 위협을 완화하고 대응하기 위해 공공부문의 기본 역량을 강화

12) 2016~22 [Government of Singapore] [Singapore Cyber Landscape 2016~2022]

하는 것이었다.

2) 2008년 Infocomm Security Masterplan

두 번째 마스터 플랜은 싱가포르를 안전하고 신뢰할 수 있는 사이버 허브로 만든다는 비전과 함께 싱가포르의 CII(Critical Information Infrastructure)에 대한 보안을 강화하는 것이었다.

3) 2009년 Singapore Infocomm Technology Security Authority (SITSA)

SITSA는 사이버 공격과 사이버 스파이로부터 싱가포르를 보호하는 것을 목적으로 내무부 산하에 설립되었다.

4) 2013년 National Cyber Security Masterplan (NCSM2018)

세 번째 마스터 플랜은 CII에 대한 보안 뿐만 아니라 기업과 개인을 포함하여 보다 광범위한 정보통신 생태계를 구축하여 싱가포르를 신뢰할 수 있는 강력한 정보통신 허브'로 만드는 목표를 담고 있다.

5) 2013년 National Cybersecurity R&D (NCR) Programme

사이버 보안에 대한 R&D 전문성과 역량을 개발하기 위해 설립되었다. 사이버 보안성 신뢰성 안전성 유용성을 강조하여 사이버 인프라의 안전성을 향상시키는 것을 목표로 한다.

6) 2014년 National Cyber Security Centre (NCSC)

NCSC는 SITSA의 일부로 구성되어 사이버 상황 인식을 유지하고 부문 간 사이버 보안 이벤트를 연결시기며 각 주요기관과 협업하여 대규모 사이버 사고에 대한 국가적 수준의 대응을 제공한다.

7) 2015년 Cyber Security Agency of Singapore (CSA)

CSA는 총리 직속으로 설립되었고, 행정적으로 정보통신부(MCI)에서 관리한다. 싱가포르 컴퓨터 비상 대응팀(SingCERT), IDA 및 SITSA의 국가 사이버 보안 계획 및 개발기능과 같은 사이버 보안 모든 기관은 CSA로 통합되었다.

CSA는 사이버 보안 개발, CII 및 필수 서비스 보호, 대규모 사이버 테러에 대한 국가적 대응을 담당하고 있다. CSA는 사이버 보안 규정 정책 관행을 개발하고 시행할 권한을 보유하고 있다. 이러한 권한을 바탕으로 정부와 산업 학계 기업 및 인력과 국제협력 등 사이버 보안 관련 모든 부분에 대한 대응할 예정이다.

8) 2016년 CyberCrime Command (CCC)

사이버범죄사령부는 싱가포르 경찰의 범죄 수사국 내 부서로 사이버 범죄를 수사하기 위하여 설립되었다. 사이버범죄사령부는 국제적인 사이버 범죄를 수사하기 위해 인터폴 글로벌 혁신단지(IGCI)를 포함하여 법 집행기관 및 기업드로가 긴밀히 협력하고 있다.

9) 2016년 National Cybercrime Action Plan (NCAP)

NCAP는 2016년 7월 내무부에서 출범하였다. 사이버 범죄 대응하기 위하여 ①사이버 공간에서 안전을 유지하기 위한 공교육의 필요성, ②사이버 범죄에 대처할 수 있는 능력 개발, ③사이버범죄법의 강화, ④지역 및 국제 파트너십 구축을 목표로 하였다.

10) 2016년 Singapore Cyber Security Strategy

사이버 보안에 대한 국가적 차원의 전략을 발표하였다. 우선 국가핵심시설에 대한 사이버 보안 강화, 기업과 사회 전반에 대한 사이버 능력 강화, 안전한 사이버 공간 구축 그리고 국제적인 사이버 협력을 목표로 하였다.

11) 2021년 Singapore Cyber Security Strategy

2016년 처음 시행된 싱가포르 사이버 보안 전략을 보완하고 업데이트 하였다.

다. 2016 싱가포르 사이버 보안 전략 ('Strategy 2016')[13)]

1) 개요

리센룽(Lee Hsien Loong) 총리는 2016년 10월 10일 싱가포르 사이버 보안 전략을 발표하고 주요 4가지 목표를 제시하였다. 사이버 보안

13) 2016 [Government of Singapore] [Singapore Cybersecurity Strategy]

전략은 사이버 보안에 대한 싱가포르의 비전, 목표 및 우선순위를 제시하고, 안전하고 신뢰할 수 있는 사이버 환경을 위한 조정된 조치를 생성하며 국제 파트너십을 촉진을 목표로 한다.

2) 주요 내용

사이버 기술은 비즈니스와 사회를 활성화하고 강화할 수 있지만 안전하고 신뢰할 수 있는 경우에만 가능하다. 그러나 사이버 공격은 점점 더 빈번해지고 정교해지며 영향력이 커지고 있다. 전 세계적으로 발전소 및 은행과 같은 필수 서비스에 대한 사이버 범죄 및 사이버 공격이 급증하고 있다.

사이버 공격은 최악의 경우 경제와 사회에 심각한 혼란을 초래할 수 있다. 싱가포르에 대한 사이버 공격의 영향은 우리 해안을 넘어 파급 효과가 있다. 싱가포르는 개방 경제이며 나머지 세계와 연결되어 있다. 무역, 금융 및 물류의 주요 국제 중심지이다. 싱가포르에 대한 사이버 공격은 잠재적으로 더 넓은 지역 및 세계 경제에 영향을 미칠 수 있다.

사이버 위협은 경계가 없다. 사이버 보안에 대한 강력한 국제 협력은 우리의 공동 글로벌 보안을 위해 필요하고, 보다 안전한 사이버 공간을 위해서는 정부, 기업, 개인 및 지역 사회의 공동 행동이 필요하다.

싱가포르 정부는 주요 목표로 ① 국가핵심시설(Critical Information Infrastructure.)에 대한 안정성 강화, ② 기업과 개인의 역량강화를 통하여 사이버 위협에 대응하고 사이버 범죄를 예방하며 데이터를

보호하여 안전한 사이버 공간 구축, ③ 숙련된 인력 공급과 최신 기술 회사 그리고 강력한 연구협력 활기찬 사이버 보안 생태계 구축, ④ 국가 경계를 뛰어넘는 사이버 위협에 대응하기 위한 강력한 구제 파트너쉽 구축하겠다고 발표 하였다.

라. 2021 싱가포르 사이버 보안 전략 ('Strategy 2021')[14)]

1) 개요

싱가포르 정부는 2021년 빠르게 진화하는 기술 환경에 대응하기 위하여 '2021 싱가포르 사이버 보안 전략'을 발표하고 업데이트 된 3가지 목표와 2가지 지원방식을 제시하였다.

양자 컴퓨터 인공지능과 같은 새로운 신기술이 등장하여 새로운 위협이 되고 있다. 해커들의 공격은 더욱 정교해 지고 있으며 유비쿼터스 연결을 활용하여 더 많은 사이버 공격을 시도하고 있다. 이에 따라 싱가포르는 2016년 처음 시작된 사이버 보안 전략을 검토하고 갱신하였다.

2) 사이버 운영 환경의 주요 변화

○ 새로운 기술의 등장

양자 컴퓨터, 5G, 클라우드 컴퓨팅, 에지 컴퓨팅, 인공지능과 같은 새

14) 2021 [Government of Singapore] [Singapore Cybersecurity Strategy]

로운 기술은 우리의 네트워크 환경을 근본적으로 변화시킬 것이다. 어떤 기술은 우리의 네트워크를 위협할 수 있고 반면에 어떤 기술은 우리의 자산을 보호하는 새로운 방법을 제시할 수 있다.

○ 사이버 위험의 증가

우리는 디지털 영역과 물리적 영역이 융합되는 시대에 살고 있다. 사이버 공격으로 인한 결과로 인하여 물리적인 사고가 발생할 수 있다. 예를 들어 통신, 도로, 철도, 방송, 공항, 병원 등과 같은 국가 핵심시설에 대한 사이버 공격은 시설의 붕괴와 오작동 등으로 인한 물리적 사고와 파괴가 발생할 수 있다. 그리고 스마트 기기와 인터넷이 빠르게 보급되면서 사이버 위협은 우리의 일상생활에도 스며들고 있다.

○ **유비쿼터스 디지털 연결**

코로나19 팬데믹으로 인해 디지털화가 가속화 되고 있다. 기업과 사회는 디지털 인프라와 서비스에 더욱 더 의존하고 있다. 해커는 디지털화 된 유비쿼터스 시스템을 이용하여 사이버 공격을 할 수 있다. 이러한 사이버 공격은 규모만 증가하는 것이 아니며, 또한 더욱 정교하게 성장하고 있다. 따라서 정부는 기업 및 사회 개인과 협력할 필요가 있다.

○ **사이버 자원의 경쟁**

디지털 기술은 점점 국제 사회에서 권력 분배의 핵심 결정요인으로 인식되고 있다. 예를 들어 주요 디지털 기술에 대한 기술 표준 설정

은 점차 국제적 관심을 받고 있다. 이러한 사이버 자원을 적극적으로 확보하여 싱가포르가 더욱 개방적이고 안전하며 안정적이고 평화로운 사이버 공간을 만들 수 있다.

3) 전략 목표

○ **정보 인프라에 대한 보안 강화**

2016년 사이버보안 전략에서 정부는 국가핵심시설(Critical Inofrmation Infrastructure, CII)에 대한 사이버 보안 역량강화에 중점을 두었다. 그러나 전략 2016에는 CII를 넘어 보호 범위를 확장하였다. 그리고 사이버 공격에 대한 효율성, 속도 및 민첩성을 강화하기 위해 기술역량과 조정역할을 강화하는 것을 포함하였다.

CII (Critical Inofrmation Infrastructure) 정의

- 국가핵심시설이란 국가에서 필수적으로 필요한 서비스를 제공하는 시설의 운영을 지원하는 디지털 시스템을 의미한다.
- 국가핵심시설은 항공, 은행 및 금융, 에너지, 정부, 의료, inforcomm, 육상 운송, 해양, 미디어, 보안 및 항공, 물 등 11개 주요 부문으로 분류한다.
- CSA는 위 국가핵심시설의 디지털 시스템을 모니터링하고 규제한다. 동시에 국가핵심시설 사이버 보안 역량 강화를 위한 프로그램도 진행한다.

○ **안전한 사이버 공간의 구현**

전략 2016은 사이버 보안에 대한 인식을 높이고자 노력을 하였다. 그러나 높은 수준의 인식에도 불구하고 기업과 사회에서는 아직도 기존의 관행을 되풀이 하고 있다. 따라서 정부가 직접 사이버 보안을 제공하여 국민을 보호한다. 그리고 최종 사용자를 위한 사이버 보안의 사용 환경을 단순화 하여 누구나 쉽고 편리하게 사용할 수 있도록 할 것이다.

정부는 2020 싱가포르 사이버 보안 마스터 플랜을 발표하였다. 마스터 플랜[15]은 인터넷 사용자들의 사이버 보안에 대한 인식개선 뿐만 아니라 악성 사이버 활동에 대한 국가적 탐지 분석과 관련 프로그램 개발하여 대중에게 배포하고 기업 등에게 일정 수준의 사이버 보안 기준을 설정한다.

<SG Cyber Safe Trustmark>

경쟁 비즈니스 사회에서 디지털화는 어느 때 보다 빠르게 진행되고 있다. 이와 동시에 사이버 보안은 고객 인터넷으로 기업에 접속하여 서비스를 이용함에 있어 중요한 핵심요인이 된다. SG Cyber Safe Trustmark는 우수한 사이버 보안 조치를 취한 기업에게 부여하는 표시이다. 고객은 SG Cyber Safe Trustmark를 보고 서비스를 이용 여부를 판단할 수 있다.

15) 2020 Singapore CyberSecurity Master Plan

< cyber hygiene mark> 사이버 보안 마크

전담 IT 조직이 없는 소규모 기업에게는 별도의 마크를 부여한다. 이 마크는 기업이 일반적인 사이버 공격으로부터 더 잘 보호될 수 있도록 기본적인 사이버 보안에 중점을 두고 실용적이고 구현 가능 하도록 설계되었다.

○ **국제 사이버 협력 강화**

전략 2016에서는 국제 사이버 정책에 참여하는 것을 강화하였다. 그러나 싱가포르 인근 지역의 집단적 사이버 보안을 개선하기 위하여 동남아시아 국가(ASEAN) 측과 협력을 강화하고 다른 국제 파트너와의 강력한 보안 파트너쉽을 구축한다.

< 사이버보안 아세안 장관회의(AMCC) >

싱가포르는 연례 싱가포르 국제 사이버 위크(SICW)를 주최하여 사이버 보안에 대한 다중 이해관계자 대화를 촉진하고 사이버 보안에 관한 아세안 장관급 회의(AMCC)를 주최하여 사이버 보안 파트너 쉽을 강화하고 있다.

<ASEAN-싱가포르 사이버 보안센터(ASCCE)>

아세안 국가들의 사이버 역량을 강화하기 위한 프로그램으로 사이버 정책의 구축 운영 및 기술 역량 강화 등에 대하여 아세안 고위 관료 들을 대상으로 교육을 하고 있다.

4) 기초 활성화 목표

○ 활기찬 사이버 보안 생태계 개발

전략 2016은 기업의 로컬 사이버 보안 생태계를 위한 기반을 구축하고, Made in Singapore 솔루션 개발을 촉진하고, 개인과 기업의 비즈니스 설립과 성장을 목표로 하였다. 전략 2021은 국제적으로 인정받고 신뢰받을 수 있는 TIC(Testing, Inspection, and Certification) 허브로 자리매김하고자 한다. 즉 최신의 기술과 최고의 보안 서비스를 개발하여 세계전인 수준의 제품을 개발하는 것을 목표로 한다. 그리고 강력한 연구개발 지원을 통해 새로운 기술을 개발하고 해커보다 기술적으로 앞서도록 한다는 것이다.

○ 강력한 사이버 인력의 성장

사이버 보안 전략은 궁극적으로 사람과 재능에 달려있다. 정부 기업 및 사회에 대한 사이버보안 책임의 폭과 깊이는 계속 커질 것이다. 지금까지 논의한 목표를 달성하려면 새로운 인재를 양성하고 기존의 전문가의 기술을 향상시켜야 한다. 따라서 사이버 보안의 인재 파이프 라인을 확장하는 것이 중요하다. 강력한 교육시스템을 활용하여 숙련된 사이버 인력을 양성한다. 결국 전 세계적으로 사이버 보안 전문가가 부족한 상황에서 싱가포르의 경쟁우의를 확보할 수 있다.

< SG 사이버 유스(SG Cyber Youth) >

SG Cyber Youth는 학계, 지역 사회 및 업계의 지원을 받아 청소년의 사이버 보안 경력을 쌓을 수 있도록 돕는 프로그램이다. 사이버 보안 업계 멘토의 진로 지도를 제공하고, 학생자원봉사 인정해 주어 전반적인 관심을 넓힌다. 그리고 사이버 스파링, 심층 교육, SG Cyber Olympic 등의 프로그램을 통해 사이버 보안 재능을 가진 청소년을 선발한다.

<여성 사이버 보안 인력 양성(SG Cyber Women)>

SG Cyber Women은 더 많은 여성이 사이버 보안 분야에서 경력을 쌓도록 장려하는 프로그램이다. SG Cyber Women의 일부로서 Capture The-Flag for Girls 대회, Ladies in Cyber 멘토십 프로그램 및 기술 워크숍 등이 있다.

마. 싱가포르 인터폴 (Interpol Global Complex for Innovation, IGCI)[16)]

인터폴이라고 불리는 국제형사경찰기구(International Criminal Police Organization, ICPO)는 국제범죄 방지를 목적으로 사계 각국의 경찰기관에 의해 조직된 국제 기구이다. 프랑스 리옹에 사무총국이 있으나,

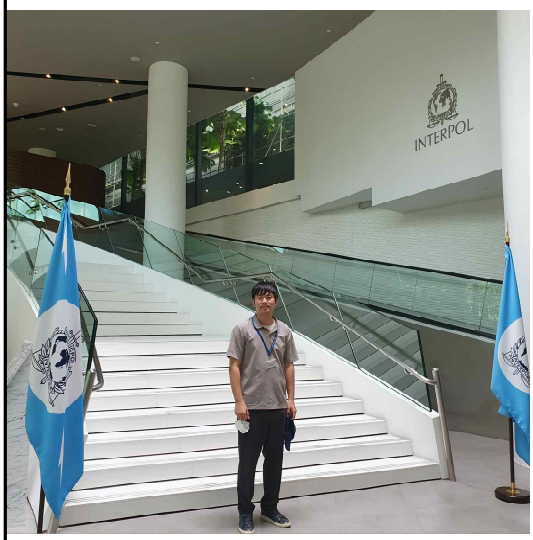
싱가포르는 인터폴 아시아 총국 제2청사를 유치하였다. 그리고 2015년에는 싱가포르 총국(Interpol Global Complex for Innovation, IGCI)이라는 이름으로 인터폴 제2청사를 개설하였다. IGCI는 아시아 권역의 범죄 정보 공유와 범죄수사 훈련 외에도 사이버 범죄 대책 업무도 실시하고 있다. IGCI에는 약 10여명의 한국 경찰이 파견되어 인

16) https://www.interpol.int/Who-we-are/Member-countries/Asia-South-Pacific/SINGAPORE

터폴 교육 부서와 사이버범죄 부서에 근무하고 있다.

IGCI의 인터폴 혁신센터(Interpol Innovation Center)에서는 다양한 배경을 가진 전문가들이 모여 치안 문제에 대한 현대적이고 창의적인 솔루션을 개발한다. 무인 항공 시스템, 선박 등을 포함한 새로운 포렌식 조사 운영을 연구하는 'Digital Forensics Lab'과 사이버 공간에서의 새로운 위협을 방지 예측 및 조사하기 위한 'Cyberspace and New Technologies Lab'이 있다.

< 인터폴 글로벌 혁신센터 방문 모습 >



바. 디지털 강국 싱가포르

본 훈련생이 싱가포르 국립 대학교, 사이버 보안청, 경찰청, 인터폴 등을 직접 방문하고 경험한 결과 우리나라 보다 월등히 디지털화 되어 있고 발전되었음을 확인할 수 있었다. 우리나라를 인터넷 강국이라고 불렀던 때가 있었다. 그러나 분명한 것은 지금은 인터넷 강국과는 매우 거리가 멀다는 것이다.

싱가포르에서 QR코드를 이용한 결제가 활성화 되어 있고 신용카드도 비접촉 결제가 가능하다. 식당 메뉴판도 QR코드 스캔하고 인터넷으로 주문한다. 인터넷 뱅킹 사용도 매우 편리하다. 상대방의 휴대전화, 주민번호 만으로도 송금이 가능하고 QR코드로 만으로도 모든 정보를 확인하고 이체 가능하다. 정부에 제출하는 신청서도 모두 인터넷으로 작성하고 서류는 스캔하여 제출한다. 신청결과도 Email로 받는다. 모든 행정이 디지털화 되어 있다.

싱가포르에서는 인터넷으로 고소장을 접수하거나 경찰서 로비에 비치된 키오스크를 통해 내용을 직접 입력하고 서류를 스캔하여 제출한다. 경찰 신고전화를 받아 Patrol이 출동하면 목격자에게 아이패드로 진술서를 작성하도록 한다. 진술서는 자동으로 경찰 시스템에 등록되고 한 부는 작성자에게 이메일 또는 휴대전화로 보내진다. 경찰 영상조사는 음성인식이 되어 서류를 작성할 필요가 없다. 경찰 단계부터 법원까지 모든 서류는 전자문서로 작성되고 증거서류도 스캔본만 제출된다. 모든 서류가 전자문서로 저장되다보니 제출시간 내용 등이 모두 디지털화 되어 분석도 편하고 정확성도 높다.

우리나라는 보안문제 그리고 노년 인구와 같은 인터넷 약자들 때문에 디지털화가 어렵다고 주장하는 사람들이 있다. 그러나 사이버 보

안청 주도로 주니어부터 시니어를 위한 사이버 교육이 잘 진행되어 와서 누구나 이메일이나 전자금융과 같은 인터넷을 쉽게 사용할 수 있다. 그리고 싱가포르 사이버 보안청은 사이버 보안을 위한 교육과 홍보뿐만 아니라 직접 보안프로그램을 제작하여 배포하여 사이버 보안을 강화한다. 싱가포르의 사이버 보안 전략 정책이 싱가포르 사이버 보안청을 통해 많은 것이 실현되어 있다는 것을 확인할 수 있었다.

3. 싱가포르 사이버 보안 관련 법률

가. 개요[17)]

싱가포르에는 사이버 보안과 관련하여 적용 가능한 여러 법률이 있다. 큰 틀에서 사이버 보안법(Cybersecurity Act)과 컴퓨터 오용법(Computer Misuse Act), 개인정보 보호법을 사이버 보안 관련 법률이라고 할 수 있다.

개인정보보호법(PDPA)은 개인 데이터와 관련하여 정부나 기업 등에 여러 데이터 보호 의무를 부과한다. 우선 PDPA는 정부와 기업에 개인정보 보호 책임자(DPO)를 지정하도록 하여 정부와 기업이 개인정보유출 등의 방지를 위한 합리적인 보안조치를 취하도록 한다. PDPA 의무 위반에 대하여 개인정보보호 위원회는 기관에 대한 조사를 할 수 있고, 벌금을 부과하거나 시정조치 등을 권고할 수 있다.

17) 2023 CSA [Cybersecurity Act] [https://www.csa.gov.sg/legislation/Cybersecurity-Act]

이 보고서에는 사이버 보안법 과 컴퓨터 오용 방지법에 대해서만 다루었다.

나. 사이버 보안법(Cybersecurity Act)[18)]

1) 주요내용

사이버 보안법(Cybersecurity Act)은 2018년 2월 5일 국회를 통과되었고, 2018년 3월 2일에 대통령의 승인을 받아 시행되었다. 사이버 보안법은 싱가포르의 사이버 보안 근거법률이다. 사이버 보안법의 주요 목표는 중요한 정보 인프라(Critical Inofrmation Infrastructure, CII)를 더 잘 보호하고, 싱가포르에 영향을 미치는 사이버 보안 사고에 대처하는 데 필요한 권한을 싱가포르 사이버 보안청(CSA)에 부여하는 것이다.

사이버 보안법은 CII 소유자에게 사이버 보안 사건을 보고할 의무를 부과하는 것을 포함하여 중요 정보 인프라(CII) 모니터링을 위한 프레임워크를 설정하고 싱가포르 사이버 보안청(CSA)장을 임명하여 CII 기관들의 사이버 보안 운영을 감독하도록 규정한다.

사이버 보안법은 CII 소유자에게 중요 정보 인프라(CII)와 관련하여 사이버 보안 사건을 보고하게 하는 등 다양한 법적의무를 부과한다. 그리고 사이버 법률을 위반하는 경우 S$100,000의 벌금 및/또는 2년의 징역형을 받을 수 있다.

18) 2021. 10. 28. [Lim Chong Kin, Drew & Napier LLC] [Singapore: Cybersecurity]

<CII 소유자들의 사이버 보안관련 의무>

- 특정 사이버 보안 및 데이터 사고에 대한 보고의무(report certain cybersecurity incidents and data breaches to the Cyber Security Agency of Singapore)
- 실행 및 성능 표준의 규정 준수(comply with codes of practice and performance standards)
- 사이버 보안 감사 및 위험 평가 수행(comply with codes of practice and performance standards)
- 사이버 보안 훈련에 참여 (participate in cybersecurity exercises.)

2) 주요 목표 및 내용

○ 사이버 공격에 대한 중요 정보 인프라(CII)의 보호를 강화

CII는 필수 서비스 제공에 직접 관여하는 국가핵심시설의 컴퓨터 시스템을 의미한다. CII에 대한 사이버 공격은 경제와 사회에 악영향을 미칠 수 있다. 사이버 보안법은 CII 지정을 위한 프레임워크를 제공하고 CII 소유자에게 사이버 공격으로부터 CII를 사전에 보호해야 하는 의무를 명확하게 하였다. 이러한 의무는 CII에 대한 사이버 보안 안전성을 높여 싱가포르 경제와 사회 시스템을 보호한다. CII는 11개 부문으로 나누어 지정 및 관리되고 있다.

CII (Critical Inofrmation Infrastructure) 지정요건

필수 서비스를 지속적으로 제공하는 데 필요한 컴퓨터 또는 컴퓨터 시스템으로, 이러한 서비스의 손실 또는 손상은 싱가포르에서 필수 서비스의 가용성을 약화시키는 영향을 미칩니다. 그리고 컴퓨터 또는 컴퓨터 시스템이 전체적으로 또는 부분적으로 싱가포르에 있습니다.
(it is a computer or a computer system necessary for the continuous delivery of an essential service, the loss or compromise of which will have a debilitating effect on the availability of the essential services in Singapore; and the computer or computer system is located wholly or partly in Singapore.)

○ CSA에 사이버 보안 위협 예방 및 대응 권한을 부여

사이버 보안법은 CSA에게 사이버 보안 위협 및 사건을 조사하여 그 영향을 파악하고 추가 피해 또는 사이버 보안 사건이 발생하지 않도록 방지할 수 있는 권한을 부여한다. 사이버 보안 위협 또는 사고의 심각성 및 필요한 대응에 따라 행사할 수 있는 권한이 나누어져 있다.

CSA의 사이버 보안 사고 예방 및대응 권한

○ 컴퓨터 또는 컴퓨터 시스템이 CII의 사이버 보안 기준 또는 수준을 충족하는지 확인하기 위한 정보를 얻을 수 있는 권한(the power to obtain information to ascertain if a computer or computer system fulfils the criteria or the level of cybersecurity of CIIs)

○ CII의 사이버 보안 또는 사이버 보안법의 효과적인 관리를 보장하기 위

해 CII 소유자 또는 소유자 등급에 서면 지시를 내릴 수 있는 권한 (the power to issue written directions to the CII owner or class of owners to ensure the cybersecurity of the CII or the effective administration of the Cybersecurity Act)

○ CII가 아닌 사람들과 관련된 것을 포함하여 사이버 보안 위협 또는 사건을 조사할 수 있는 권한. 커미셔너는 위협이나 사건의 심각성에 따라 다양한 수준의 침해로 권한을 행사할 수 있습니다. (the power to investigate cybersecurity threats or incidents, including those involving non-CII. The Commissioner may exercise powers with varying levels of intrusiveness, depending on the severity of the threat or incident)

○ 사이버 보안법에 따라 범죄와 관련하여 조사를 수행할 수 있는 권한을 경찰관에게 부여할 수 있습니다. (the power to authorise an officer to conduct investigations in relation to any offence under the Cybersecurity Act)

○ 사이버 보안 정보 공유를 위한 프레임 워크를 구축

사이버 보안법은 사이버 보안 관련 정보의 공유를 용이하게 한다. 사이버 보안 관련 정보의 공유는 정부나 기업이 사이버 보안 사고를 보다 효과적으로 예방하는데 도움이 되기 때문에 매우 중요하다. 이 법은 CII 소유자에게 중요 정보 인프라(CII)와 관련한 사이버 보안 이슈에 대해 CSA에 보고해야 하는 법적 의무를 부여한다. 그리고 CSA는 사이버 보안 관련 정보를 요청하고 이러한 정보를 공유할 수 있다.

CSA의 사이버 보안 사고 예방 및대응 권한

- 사이버 보안법 섹션 14(1)에 따라 CII 소유자는 사이버 보안 청장에게 다음 중 하나의 발생을 알려야 한다
  1. 중요 정보 인프라와 관련하여 규정된 사이버 보안 사고
  1. 중요 정보 인프라와 상호 연결되거나 통신하는 소유자의 제어 하에 있는 컴퓨터 또는 컴퓨터 시스템과 관련하여 규정된 사이버 보안 사고 및/또는
  1. 커미셔너가 소유자에게 서면 지시를 통해 지정한 중요한 정보 인프라와 관련된 기타 모든 유형의 사이버 보안 사고.

- 특히 사이버 보안(중요 정보 인프라 규정) 2018의 규정 5에 따라 CII 소유자는 사이버 보안 사고 후 2시간 이내에 다음 사항을 사이버 보안 국장에게 알려야 한다
  1. 영향을 받는 중요 정보 인프라
  1. 중요 정보 인프라 소유자의 이름과 연락처
  1. 중요한 정보 인프라 또는 상호 연결된 컴퓨터 또는 컴퓨터 시스템과 관련된 사이버 보안 사고의 성격, 발생 시기 및 방법
  1. 중요한 정보 인프라 또는 상호 연결된 컴퓨터 또는 컴퓨터 시스템이 영향을 받은 방식을 포함하여 관찰된 결과 효과 그리고
  1. 신고서를 제출하는 개인의 이름, 직위, 조직 및 연락처.

- 그러면 CII 소유자는 CSA 웹사이트를 통해 14일 이내에 다음과 같은 추가 정보를 제공해야 한다
  1. 사이버 보안 사고의 원인
  1. 중요한 정보 인프라 또는 상호 연결된 컴퓨터나 컴퓨터 시스템에 미치는 영향 그리고
  1. 어떤 개선 조치를 취했는지

○ 사이버 보안 서비스 공급자를 위한 자격증 부여

CSA는 2가지 종류의 사이버 보안 서비스 업체를 대상으로 라이선스(자격증)을 부여하고 있다. 관리형 보안 운영센터 모니터링 서비스와 침투 테스트 서비스이다. 관리형 보안운영센터 모니터링 서비스는 기업의 사이버 보안 시스템의 설치와 관리 운영을 의미한다. 침투 서비스는 기업의 의뢰를 받아서 사이버 보안 관련 취약점이 있는지 직접 해킹(침투)하는 것을 말한다. 일부 언론에서는 화이트해커 자격증이라고도 번역을 하였다. 그러나 기업의 허락을 받지 않고 시스템에 접속하는 것은 허용되지 않고, 이를 위반하는 경우 형사처벌 대상이 된다.

다. 컴퓨터 오용법(Computer Misuse Act 1993, CMA)[19)]

1) 개요

컴퓨터 오용법(The Computer Misuse Act 1993, CMA)은 1993년 컴퓨터 자료에 대한 무단 접근이나 수정, 기타 컴퓨터 범죄를 처벌하기 위해 제정되었다. 컴퓨터 오용법은 새로운 기술의 개발 및 다양한 종류의 사이버 범죄가 등장하면서 이러한 변화에 맞추어 1994년과 2012년 두 차례 걸쳐 개정 되었다. CMA 섹션 3에는 컴퓨터 시스템에 대한 무단 액세스 권한을 얻기 위해 컴퓨터 취약성을 악용하는

19) 2022. 11. 14. Lim Chong Kin, David Alfred, Albert pichlmaier (Drew&Napier LLC), [Cybersecurity Laws and Regulations Singapore]

것과 같은 범죄를 포함하여 다양한 사이버 범죄를 규정하였다.

2) 주요 사이버 범죄 종류

컴퓨터 오용법 제3조부터 제10조까지 사이버 범죄 행위를 규정하였다. 제11조 는 특정 컴퓨터나 시스템에 대한 범죄에 대해 가중처벌 조항이다. 여기서 특정 컴퓨터는 주로 국가핵심시설(CII)을 의미한다. 즉 국가핵심시설 컴퓨터 시스템에 대한 공격은 가중 처벌된다. 제12조는 교사 및 미수에 대한 내용을 규정하였다. 그리고 제19조는 모든 경찰관은 이 법에 따라 범죄를 저질렀다고 합리적으로 의심되는 사람을 영장 없이 체포할 수 있다고 규정하고 있다. 참고로 싱가포르는 중요 범죄에 대해서 경찰관은 영장 없이 피의자를 체포하거나 압수 수색을 할 수 있다. 제18조에는 경찰관뿐만 아니라 다른 법률에서 권한을 부여받은 사람도 컴퓨터 오용법에 관련된 범죄를 수사할 수 있다.

< CMA SECTION 11, 12, 18, 19 >

Section 11. Enhanced punishment for offences involving protected computers

Section 12. Abetments and attempts punishable as offences

Saving for investigations by police and law enforcement officers
Section 18. Nothing in this Act prohibits a police officer, an authorised person within the meaning of section 39 of the Criminal Procedure Code 2010 or any other duly authorised law enforcement officer from lawfully conducting investigations pursuant to the powers conferred on him or her under any written law.

Arrest by police without warrant
Section 19. Any police officer may arrest without warrant any person reasonably suspected of committing an offence under this Act.

○ 컴퓨터 자료에 대한 무단 액세스 (Section3: Unauthorised access to computer material)

컴퓨터에 저장된 프로그램이나 데이터에 대한 권한 없이 액세스를 확보할 목적으로 고의로 컴퓨터가 기능을 수행하도록 하는 사람은 $5,000 이하의 벌금 또는 2년 이하의 징역 또는 둘 모두에 처해질 수 있다. 그리고 두 번째 또는 후속 유죄 판결의 경우 $10,000 이하의 벌금 또는 3년 이하의 징역 또는 둘 다에 처해질 수 있다. Section3 위반의 결과로 피해가 발생하는 경우 가중처벌 되어 $50,000 이하의 벌금 또는 7년 이하의 징역 또는 둘 모두에 처해질 수 있다.

예를 들면 서버에 있는 다른 사람의 인터넷 은행계좌의 프로그램, 데이터 등에 접속하는 행위를 말한다.

○ 범죄를 저지르거나 범죄를 조장하려는 의도로 접근 (Section4: Access with intent to commit or facilitate commission of offence)

컴퓨터에 저장된 프로그램이나 데이터에 대한 액세스를 확보할 목적

으로 컴퓨터가 기능을 수행하도록 하는 사람은 $50,000 이하의 벌금 또는 10년 이하의 징역 또는 두 가지 모두에 처해질 수 있다. Section4은 재산, 사기, 부정직과 관련된 범죄 또는 신체적 상해를 유발하는 경우 가중처벌 되어 2년 이상의 징역형에 처할 수 있다.

예를 들면 사람들을 속이기 위해 회사 시스템에 접속하여 자료를 변경 삭제 복사 등을 하는 경우에 해당한다.

○ 컴퓨터 자료의 무단 수정 (Section5: Unauthorised modification of computer material

컴퓨터를 오용하여 컴퓨터 내용을 무단으로 수정하는 행위를 하는 사람은 유죄 판결을 받고 $10,000 이하의 벌금 또는 3년 이하의 징역 또는 두 가지 모두에 처해질 수 있다. 두 번째 또는 후속 유죄 판결의 경우 $20,000 이하의 벌금 또는 5년 이하의 징역 또는 두 가지 모두에 처해진다. Section5에 따른 위반의 결과로 피해가 발생하는 경우 위반으로 유죄 판결을 받은 사람은 $50,000 이하의 벌금 또는 7년 이하의 징역 또는 둘 모두에 처해질 수 있다.

예를 들어 데이터 삭제 변경, 웹사이트 해킹, 바이러스 트로이목마 랜섬웨어 등이 해당한다.

○ 컴퓨터 서비스의 무단 사용 또는 방해 (Section6: Unauthorised use or interception of computer service

전자기기, 음향, 기계 또는 기타 장치를 통해 컴퓨터의 기능을 직간접적으로 권한 없이 가로채거나 가로채도록 유발하는 행위 또는 컴퓨터 서비스를 직간접적으로 획득할 목적으로 컴퓨터에 대한 권한 없이 접속하여 사용하는 경우 적용된다.

예를 들면 와이파이 불법사용 키로깅 등이 해당한다.

○ 컴퓨터의 무단 사용 방해 (Section7: Unauthorised obstruction of use of computer

컴퓨터의 합법적인 사용을 방해하거나 중단하거나 방해 또는 컴퓨터에 저장된 프로그램이나 데이터에 대한 액세스를 방해 또는 방지하거나 유용성 또는 효율성을 손상시키는 사람은 $10,000 이하의 벌금 또는 3년 이하의 징역 또는 두 가지 모두에 처해지며, 두 번째 또는 후속 유죄 판결의 경우 $20,000 이하의 벌금 또는 5년 이하의 징역 또는 두 가지 모두에 처해질 수 있다.

예를 들어 디도스와 같이 시스템의 운영을 방해하는 공격을 하는 경우 적용된다.

○ 액세스 코드의 무단 공개 (Section8: Unauthorised disclosure of access code

부당한 이익, 불법적인 목적 등으로 컴퓨터에 저장된 프로그램이나 데이터에 액세스할 수 있는 암호, 액세스 코드 또는 기타 수단을 고

의로 무단으로 공개한 사람은 $10,000 이하의 벌금 또는 3년 이하의 징역 또는 두 가지 모두에 처해질 수 있고, 두 번째 또는 후속 유죄 판결의 경우 $20,000 이하의 벌금 또는 5년 이하의 징역 또는 둘 다에 처해질 수 있다.

예를 들어 허가받지 않고 다른 사람의 비밀번호를 공유하는 경우 적용된다.

○ 일정한 규정을 위반하여 취득한 개인정보의 제공 등 (Section9: Supplying, etc., personal information obtained in contravention of certain provisions)

다른 사람에 대한 개인정보가 제3조 제4조 제5조 제6조를 위반하여 얻어진 것을 알거나 알 수 있었음에도 불구하고 해당 개인정보를 취득하거나 보유 제공 판매하는 경우 적용된다.

예를 들어 도난된 신용카드의 사용 판매 양도를 하는 경우 등에 적용된다.

○ 특정 범죄에 사용하기 위한 물품의 취득 등 (Section10: Obtaining, etc., items for use in certain offences)

이 조항은 물품이나 서비스에 적용된다. 주로 주로 3, 4, 5, 6 또는 7조에 따른 범죄를 저지르기 위해 설계되거나 적합하게 조정된 또는 사용 가능한 장치(컴퓨터 프로그램을 포함)를 취득 사용 판매 배포하는 행위에 대해 처벌한다.

예를 들어 해킹을 위한 시스템을 판매 양도 취득하는 경우 성립한다.

4. 싱가포르 주요 사이버 보안 사고

가. 2018년 SingHealth 데이터 유출 사건 (SingHealth data breach)[20)]

1) 개요

Sing Health는 싱가포르에서 가장 큰 공공의료 기관 그룹으로, 2000년에 설립되었으며 4개의 공립 병원, 3개의 지역 병원, 5개의 국립 전문 센터 및 8개의 지역병원으로 구성되어 있다.

2018년 6월 27일부터 7월 4일 사이에 발생한 사이버 공격으로 150만 명의 SingHealth 환자의 개인 정보와 외래 환자에게 투여된 의약품 기록 등이 유출되었다. SingHealth에 가입한 환자의 이름과 주민번호(FIN Number), 생년월일, 카드번호, 주소가 외부로 유출되었으며 해커는 리센룽(Lee Hsien Loong) 싱가포르 총리의 건강정보를 목표로 한 것으로 알려졌다.

2) 주요내용

CSA의 조사에 따르면 해커들은 먼저 프런트 엔드 워크스테이션을 통해 SingHealth의 IT 시스템에 침입했으며 나중에 데이터베이스를

20) https://en.wikipedia.org/wiki/2018_SingHealth_data_breach

접속을 위한 위해 로그인 정보를 획득한 것으로 확인되었다. 해커에게 악용된 서버는 랜섬웨어 공격으로 인해 2017년 5월 이후 1년 넘게 보안 업데이트를 받지 못한 것이었다. 해커들은 6월 27일부터 7월 4일까지 1주일 동안 SingHealth의 IT 시스템에 접속하여 데이터를 유출하였다. 정보통신부 장관은 해커들이 SingHealth의 바이러스 백신 및 보안 도구를 우회하기 위해 맞춤형 멀웨어를 제작하는 등 정교한 맞춤형 사이버 공격(Advanced Persistent Threat, APT)라고 발표하였다.

3) 정부대응 및 조치

7월 4일 데이터베이스 관리자는 SingHealth의 IT 데이터베이스 중 하나에서 비정상적인 활동을 처음으로 감지하였다. 그리고 침입에 대한 대응조치를 하였고 네트워크에 대한 모니터링을 시작하였다.

7월 10일 사이버 공격으로 데이터 유출을 확인하고, 정보통신부 CSA 등 관련기관에 통보하였고 컴퓨터와 서버에 대한 포렌식을 진행하였다.

7월 20일 정보통신부 장관은 사이버 공격과 데이터 유출에 대한 내용의 성명을 발표하였다. 그리고 데이터가 유출된 환자들에게 유출사실을 문자 메시지로 전송하였다.

7월 24일 국회에 사고조사위원회가 소집되었다. 사이버 공격의 원인에 대해서 조사하고 유사한 공격을 방지하기 위한 조치를 취하였다. 그리고 3차례 비공개 청문회 및 공청회를 열러 사건에 대해 조사하

였다.

2019년 1월 10일 조사위원회는 SingHealth 사이버 공격에 대한 보고서를 발표하였다. 보고서는 직원들이 사이버 보안에 대한 지식이 부족하여 사이버 공격에 즉각 대응을 하지 못 하였고, SingHealth 네트워크 시스템에 여러 가지 취약점이 있었으며 보안 프로그램 등이 제때 패치되지 아니하여 데이터가 유출된 것이라고 하였다.

나. 2016년 StarHub DDoS 공격 사건 (StarHub DDoS Attacks)

2016년에는 싱가포르에서 스타허브(StarHub)라는 통신 사업자가 DDoS(분산 서비스 거부) 공격의 대상이 되었습니다. 이 공격은 광범위한 인터넷 서비스 장애를 초래하였으며, 싱가포르에서 사회적 및 경제적으로 큰 영향을 미쳤다.

2016년 10월 22일과 24일 2차례 걸쳐 StarHub는 시스템이 마비되어 고객들의 인터넷 서비스가 중단되었다. 해커는 좀비컴퓨터를 통해 StarHub의 DNS에 반복적으로 쿼리를 보내는 방식으로 DDos공격을 하였다. StarHub는 트래픽을 수동으로 필토링하고 DNS 용량을 늘려 인터넷 서비스를 복구하였다. 고객정보 등은 유출되지 않은 것으로 확인되었다.

다. 2017년 국방부/국군 데이터 유출 사건 (MINDEF/SAF Data Breach)

싱가포르 국방부와 싱가포르 국군은 2017년 2월 약 850명의 국가복

무요원과 직원들의 개인 데이터가 사이버 공격으로 유출되었다고 발표하였다. MINDEF/SAF 데이터 유출은 2019년 초에 발견되었으나, 무단 접근은 수개월에 걸쳐 이루어졌다. 해커들은 MINDEF/SAF의 I-net 시스템에 접근하여 군인들의 개인 정보(이름, 신분증 번호, 연락처 등)를 포함한 데이터를 유출하였다.

정부는 해킹사실을 확인한 직후 I-net과 연결된 모든 인터넷 접속을 차단하고 포렌식 등 조사를 진행하였다. 그리고 네트워크 보안 강화, 다중 인증 요소 도입, 직원의 인식과 교육 프로그램 강화 등 보안강화조치를 하였다. 군사정보 유출은 국방력과 국가안전에 대한 잠재적인 위협을 야기할 수 기 때문에 국가 안보와 관련된 심각한 우려를 불러일으켰다.

5. 싱가포르 사이버 보안청 (Cyber Security Agency of Singapore, CSA)[21]

가. 개요

싱가포르 사이버 보안청(Cyber Security Agency of Singapore, CSA)은 싱가포르의 사이버 보안 전략, 운영, 교육, 보급 및 생태계 개발을 담당하는 국가 기관이다. 사이버 보안청은 관리 체계상으로는 정보통신부 관할 하부기관이나, 실제로는 싱가포르의 모든 국가 사이버 보

21) www.csa.gov.sg

안 기능을 총괄하고 있으며 사이버 보안 사고 발생 시 총리에게 직접 보고하는 기관이다.

싱가포르 사이버 보안청은 싱가포르 정보통신기술보안청의 조직을 흡수하여 2015년에 설립되었다. 그리고 싱가포르의 사이버 보안 관련 모든 조직을 하나로 통합하고 기업 및 전문가 등 다양한 이해당사자들과 공조하여 사이버 보안 강화 및 전략 개발을 담당하고 있다.

사이버 보안청의 주요 프로그램에는 싱가포르 컴퓨터 긴급 대응팀(SingCERT) 운영 통한 국가 사이버 사건 대응, 사이버 보안 산업 개발 지원 그리고 사이버 보안 프로그램 보급 및 교육 캠페인 등 사이버 보안 의식 확산 연합(Cybersecurity Awareness Alliance), 국제 참여를 통한 글로벌 사이버 보안 협력 강화 등이 있다.

<싱가포르 사이버 보안청 방문 모습>

나. 미션 및 목표

1) 미션

CSA의 주요 미션은 싱가포르의 중요한 정보 기반 시설, 핵심 서비스 및 시민들을 위한 견고하고 안전한 사이버 공간을 보장하는 것이다.

2) 목표

국가 사이버 보안 강화 : CSA는 견고한 사이버 보안 조치의 구현, 인식 제고 및 안전한 디지털 생태계 조성을 통해 싱가포르의 사이버 위협에 대한 저항력을 강화한다.

사이버 보안 능력 개발 : CSA는 교육, 훈련, 연구 및 개발 그리고 인재 육성 이니셔티브를 지원하여 싱가포르에 숙련된 사이버 보안 인력을 육성하는 데 초점을 맞추고 있다.

국제적인 협력 구축 : CSA는 국제적인 동료 기관, 산업 이해관계자 및 학계와 협력하여 전 세계적인 사이버 보안 생태계를 발전시키고 사이버 위협을 공동으로 대응한다.

3) 역할

정책 및 법규: CSA는 신뢰할 수 있는 안전한 디지털 환경을 보장하기 위해 사이버 보안 정책, 규정 및 표준을 수립하고 이를 실행한다 다른 정부 기관 및 산업 파트너와 협력하여 종합적인 사이버 보안 전략을 개발한다.

사고 대응 및 관리: CSA는 주요한 사이버 사고에 대한 대응을 조정하고, 사이버 사고 발생 시 조직에 지원 및 지침을 제공하며, 위협 정보 공유를 원활하게 진행한다.

중요한 정보 기반 시설 보호: CSA는 싱가포르의 중요한 정보 기반 시설 보호를 감독하기 위해 가이드라인을 수립하고 위험 평가를 수행하여 사이버 위협에 대한 견고한 대비 조치를 취한다.

다. 주요 프로그램

○ 사이버 보안 인식 캠페인

CSA는 개인, 기업 및 교육 기관을 대상으로 사이버 보안 위협, 최선의 방법 및 온라인 안전의 중요성에 대해 인식을 높이기 위한 공개 홍보 캠페인을 진행한다. 싱가포르 국제사이버주간(Singapore International Cyber Week), Singapore Cyber Landscape 등과 같은 사이버 보안 캠페인을 통해 정보를 공유하고 사이버 안전의 중요성에 대한 인식을 높이고 있다.

○ 사이버 보안 인재 개발

CSA는 교육 기관, 산업 파트너 및 전문 기관과 협력하여 사이버 보안 훈련 프로그램, 인증 및 장학금을 개발한다 이러한 이니셔티브는 싱가포르의 강력한 사이버 보안 인력을 육성하는 것을 목표로한다. SG Cyber Youth Program 등의 프로그램을 통해 전문인력을 육성한다.

○ 위협 정보 공유

CSA는 정부 기관, 핵심 기반 시설 운영자 및 기타 이해관계자 간에 적시에 관련성 있는 사이버 위협 정보를 공유할 수 있도록 지원한다. 최근 ASEAN 등 인근지역 국가들과의 사이버 보안 협력뿐만 아니라 대한민국 등 다양한 국가들과의 사이버 보안협력을 통해 정보를 공유하여 방어능력을 향상시키고 있다.

○ 안전한 보안 프로그램 개발

CSA는 소프트웨어 개발자와 기관에 대한 리소스, 가이드라인 및 교육을 제공하여 안전한 코딩 관행을 촉진한다 이 프로그램은 소프트웨어 응용 프로그램과 시스템의 보안을 향상시키는 것을 목표로 한다 예를 들어 SG Cyber Safe 프로그램을 통해 사이버 보안 툴킷을 제공하고 동시에 사이버 보안 인증 제도도 운영하고 있다.

○ 싱가포르 컴퓨터 긴급 대응팀 (Sing CERT)

SingCERT는 사이버 보안 공격, 사이버 사건 및 취약점 등에 대한 모니터링 및 대응을 조정하고, 관련 조직 및 부문에 사이버 보안 사건에 대한 인지 및 대응 능력을 제공한다.

SingCERT는 싱가포르의 중요 부문 및 조직에 대한 사이버 보안 사건 대응을 담당한다 SingCERT는 사이버 공격, 데이터 유출, 시스템 침입 등과 같은 사이버 보안 사건에 신속하게 대응하여 피해를 최소화하고 조사를 수행한다. SingCERT는 싱가포르에 대한 신속한 위협

분석 및 사이버 보안 경보를 제공한다. 이를 통해 싱가포르의 중요 부문과 조직은 최신 사이버 위협에 대해 경고를 받고 필요한 조치를 취할 수 있다.

SingCERT는 싱가포르 기업과 기관에 대한 사이버 보안 관련 정보를 제공한다. 이는 최신 사이버 보안 위협, 취약점, 해킹 기술 및 방어 전략에 대한 정보를 제공하여 싱가포르의 조직이 보안 수준을 높이는 데 도움을 준다.

6. 싱가포르 경찰청 현장연수

가. 개요

싱가포르 경찰청 수사과에서 2주 동안 현장 연수을 받았다. 처음 연수기관을 알아보고자 연락을 하였고 사이버 수사 분야에 관하여 2주 동안 실습이 가능하다는 답변을 받았다. 싱가포르 사이버 범죄 사령부에서 실습을 하였으며 사령부 내 사이버테러수사팀 포렌식팀 경찰서 사이버범죄수사팀 안티스캠사령부 그리고 경찰 훈련기관 등 싱가포르 경찰 전반의 업무에 대해 실습을 할 수 었다.

<SPF 사이버범죄사령관 및 직원과 만남>

<SPF로부터 받은 현장연수 공문>

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

Criminal Investigation Department
Police Cantonment Complex
391 New Bridge Road
Singapore 088762
Tel +65 6435 0000
www.police.gov.sg

4 January 2023

Mr. Sukwoo Lim
Korean National Police Agency
Field of Study: Cybercrime Investigation
Fellowship Period: 29 December 2022 to 28 June 2023
Status: Visiting Researcher

Dear Mr. Sukwoo Lim,

ATTACHMENT TO THE SINGAPORE POLICE FORCE

I refer to your letter of request dated 27 September 2022.

2 I am pleased to inform you that your request for attachment to the Singapore Police Force has been confirmed and will take place from 13 to 24 February 2023.

3 Details of the attachment will be provided to you closer to the attachment date. Should you have any queries prior to the attachment, you may contact ASP Augustus Tang at HP: +65 – 9115 4867 or augustus_tang@spf.gov.sg. I look forward to meeting you in February.

Yours Sincerely,

SUPT Randy Chua
Head, Technology Crime Policy Branch
Technology Crime Division
Criminal Investigation Department
Singapore Police Force

<SPF 현장연수 스케줄>

Attachment Programme for Mr Lim Suk-Woo (13 Feb 2023 – 24 Feb 2023)

Week 1: 13 Feb 2023 – 17 Feb 2023

13 Feb:

Meeting with CyberCrime Command (CCC) Management

- Admin arrangement and orientation around Police Cantonment Complex

Technology Crime Policy Branch (TCPB)

- Briefing on SPF, CID and CCC structure, roles and responsibilities

14 Feb: Technology Crime Investigation Branch (TCIB)

- Briefing on TCIB's roles and responsibilities
- Briefing on TCIB's collaboration efforts with external partners and usage of tools/systems in cybercrime investigation

15 Feb: Cybercrime Investigation Training

16 Feb: Technology Crime Forensic Branch (TCFB)

- Briefing on TCFB's roles and responsibilities
  - Search and seizure of different type of exhibits
- Visit to TCFB Labs
- Briefing on TCFB's collaboration efforts with external partners and usage of tools/systems in cybercrime forensic

17 Feb: Technology Crime Policy Branch (TCPB)

- Sharing by Supt Lim Suk-Woo on his area of work during CCC monthly In-service training

Week 2: 20 Feb 2023 - 24 Feb 2023

20 Feb:

Anti-Scam Command / SPF

- Visit to Anti-Scam Command

Cyber Security Agency

- Visit to Cyber Security Agency

21 Feb: INTERPOL Global Complex for Innovation

- Visit to INTERPOL Global Complex for Innovation

22 Feb:

Home Team School of Criminal Investigation

- Visit to Home Team School of Criminal Investigation

23 Feb: Cybercrime Response Team (CCRT) 'E'

- Visit to E Div CCRT
- Briefing on CCRT E's roles and responsibilities

24 Feb: Cybercrime Response Team (CCRT) 'L'

- Visit to L Div CCRT
- Briefing on CCRT L's roles and responsibilities

End of Attachment

나. 싱가포르 경찰청 소개[22)]

1) 개요

싱가포르 경찰청은 1820년에 설립되었으며, 동남아시아에서 가장 오래된 경찰기관 중 하나이다. 싱가포르 경찰청(Singapore Police Force, SPF)은 싱가포르 내 내무부의 관할 하에 있는 제복 조직이다. SPF의 임무는 싱가포르의 안전과 보안을 위해 범죄를 예방, 방지, 및 탐지하는 것이다.

2) 미션 및 비전

SPF 미션은 "범죄를 예방, 방지, 탐지(To prevent, deter and detect crime)"이고, 비전은 “세계에서 가장 안전한 싱가포르를 만들도록 하는 국가를 위한 경찰력(A Force for the Nation – To Make Singapore the Safest Place in the World)이다. SPF의 업무는 ①현장 경찰활동, ②대응 및 전자 서비스, ③수사, ④지역사회 참여, ⑤공공 안전 및 질서 다섯 가지 주요 영역에 초점을 두고 수행된다.

3) 조직구조 등

SPF는 현재 16개의 스태프 부서, 4개의 전문 스태프 부서, 18개의 전문 및 라인 부대, 7개의 육상 사단으로 구성되어 있다. 본부는 노베나(Novena) 지구의 뉴 피닉스 파크(New Phoenix Park) 건물[23)]에 위

22) http://www.spf.gov.sg/

치해 있다. 2020년 기준으로 SPF는 약 10,706명의 인력으로 구성되어 있으며, 그 중 9,571명은 신분이 있는 경찰관이고, 1,135명은 민간 직원이다.

<SPF 조직도>

다. 싱가포르 경찰청 수사국(Criminal Investigation Department, CID)

23) 28 Irrawaddy Road, New Phoenix Park, Singapore 329560

1) 소개

수사국(Criminal Investigation Department, CID)은 싱가포르 경찰(Police Force) 내 범죄 수사에 관한 최고의 수사 기관이다. CID는 Outram Park MRT 근처에 있는 Police Cantonment Complex (PCC)에 위치해 있다.

CID는 살인, 강간, 폭탄 폭발 사건, 조직 범죄, 카지노 범죄, 사이버 범죄 등 심각하고 민감한 사건을 수사하는 업무를 담당한다. 이외에도 조직폭력, 무면허 도박, 지적 재산권 침해 등에 대한 범죄 억제 및 단속과 수사도 맡고 있다. CID는 수사와 단속 기능 외에도 수사 정책과 관련된 권한도 가지고 있다. 정부기관 수사 부서에 정책 지침을 제공하고 수사의 질을 향상시키기 위한 능력을 개발하는 역할도 수행한다.

<SPF CID건물 및 로비에서의 모습>

2) 미션

수사의 탁월함을 통해 범죄를 예방, 억제 및 탐지하는 것 (To prevent, deter and detect crime through excellence in investigation.)

3) 역할/기능

○ 주요 범죄 수사과(Major Crime Division)

주요 범죄 수사과는 살인, 납치, 화기 관련, 강간 및 성폭력, 폭탄 및 폭발 관련 등 심각하고 민감한 사건을 수사한다.

○ 특수 범죄 수사과 (Specialised Crime Division)

특수 범죄 수사과는 조직폭력, 불법 도박, 인신 매매, 무면허 도박, 지적 재산권 침해, 카지노 범죄 사례에 대한 수사 및 단속을 수행한다. 그리고 재정수사과에서는 은닉한 범죄수익을 찾아 몰수하는 업무를 하고 있다.

○ 기술 범죄 수사과(Technology Division)

기술 범죄 수사과는 기술 범죄 정책국, 기술 범죄 수사과, 기술 범죄

법의학국으로 구성된다. 이 부서는 컴퓨터 오용법에 따른 사이버 범죄에 초점을 맞추어 수사를 한다.

○ 법의학과(Forensics Division)

CID에서 수사하는 사건에 대한 지문, 문서감정, 증거물 분석 등을 포함한 범죄 현장의 법의학 지원을 제공한다.

○ 범죄정보과(Intelligence Division)

정보 국은 유용한 범죄 정보의 수집, 처리, 분석 및 전파를 통해 CID 부서를 지원하는 역할을 한다.

○ 수사 서비스 및 지원 과(Investigation Services and Support Division)

수사 서비스 및 지원 국은 범죄기록을 보관하고 관련 수사관련 시스템과 물품 등을 수사 지원을 한다.

○ 작전, 수사 정책 및 훈련 과 (Operation, Investigation Policy and Training Division)

CID와 모든 지역 부서 및 전문 부서에 대한 수사 정책을 개발하고 주요 사건의 저정 지휘 통제를 한다. 그리고 경찰관들의 교육과 관련된 업무도 담당한다.

○ 연구, 기획 및 조직 발전 과(Research, Planning and Organisational

Development Division)

연구, 기획 및 조직 발전 국은 CID의 전략 및 운영 기획, 정책 개발 및 법률 검토, 역량 개발 및 정보 관리 업무를 담당한다.

4) 수사 전문가 트렉 (Investigation Expert Career Track, IECT)

싱가포르 경찰은 전문가 트렉(Expert Career Track)을 운영한다. 전문 수사관은 3단계의 전문가로 트렉(Senior Specialist, Principal Specialist, Expert) 으로 이루어져 있다. 전문가는 6년 이상의 수사경력을 보유하여야 하고 여러 인터뷰와 시험 등을 거쳐 선발한다. 전문가 트랙은 전체 수사 인원의 3~4% 정도이다. 그리고 전문가로 선발되면 일정 수당을 추가로 받지만 민감하고 중요한 사건을 처리하여야 하고 자문과 교육 등 추가적인 업무도 주어진다. 그리고 매년 평가를 통해 자격을 박탈하기도 한다.

라. 기술 범죄 수사과(Technology Division)

1) 개요

기술 범죄 수사과는 기술범죄 정책, 수사, 포렌식 3개의 브렌치(Branch)로 이루어져 있다. 기술범죄 수사과는 사이버범죄사령부(CyberCrime Command)라고도 한다. 싱가포르 사이버 보안 전략 2016에 보면 2015년 폭증하는 사이버범죄에 대응하기 위해 사이버사

령부를 설치한 것을 확인할 수 있다. 사이버사령부는 컴퓨터 오용법(Computer Misuse Act)에 규정된 범죄만을 수사한다.

2) 사이버 범죄 분류

○ Cyber-dependent Crime

컴퓨터 남용법(Computer Misuse Act, CMA)에 따른 컴퓨터가 표적인 범죄로, 해킹, 웹사이트 변조, 랜섬웨어 등과 같은 범죄행위를 위미한다.

○ Cyber-enabled Crime

컴퓨터를 통해 범죄행위를 용이하게 하는 범죄들이다. 즉 온라인 사기, 온라인 괴롭힘과 사이버 협박 등 사이버를 활용한 범죄를 의미한다.

○ 사이버범죄사령부에서는 Cyber-dependent Crime를 수사한다. Cyber-enabled Crime은 안티스캠센터 등 다른 수사부서에서 담당한다.

2) 기술범죄 정책계 (Technology Crime Policy Branch, TCPB)

TCPB는 정책, 사이버범죄예방, 교육, 교류협력, 연구개발 5개의 팀 약 15명으로 구성되어 있다. 정책팀은 사이버범죄사령부 구성과 운영에 관한 사항 및 수사절차 배당 등에 관한 업무를 한다. 사이버범죄예방팀은 온라인 오프라인 범죄예방을 위한 홍보 활동을 주로 한다.

교육팀은 사이버범죄 수사관의 커리어 개발을 위한 교육프로그램을 진행하고 매월 사이버범죄 중요사건에 대한 사례발표를 진행한다. 마침 교육 중인 2월 17일에 사례발표 화상회의가 있어 한국 경찰에 대한 소개와 IP카메라 사건에 대한 사례를 발표하였다. 교류협력은 정부 민간기관 간 또는 국외 법집행기관과의 업무협력을 담당하며 연구개발 부서는 장비 구매 서비스 개발 등의 업무를 한다.

3) 기술범죄 수사계 (Technology Crime Investigation Branch, TCFB)

TCFB는 즉시대응팀, 추적팀, 로그분석팀, 악성코드 수사팀으로 이루어져 있다. 수사계장이 있고 그 밑에 같은 계급의 보조계장이 있다. 그리고 8개의 팀으로 구성되어 있으며 한 팀에 팀장을 포함하여 5명 정도로 구성되어 있다. 당직팀이 있어 24시간 사건을 받고 매일 아침 9시에 전날 접수한 사건들에 대한 panal 회의를 진행하며 사건처리 방향에 대해 논의한다. 그리고 중요한 사건이 접수되는 경우 계장을 비롯한 모든 팀원이 모여 회의를 진행한다. 연수기간 중에 정부기관 공무원이 허가 없이 부하 직원의 의료정보를 조회한 사건이 접수되어 모든 팀원이 모여 회의를 진행하였다.

팀별로 전문분야가 나누어져 있으나 당직 날에 배당받은 사건을 처리하며 대형사건이 발생하였을 때 업무를 나눈다고 하였다. 사건을 배당받은 경찰관은 5일 이내에 첫 번째 보고서를 작성하여 팀장에게 보고하여야 한다. 팀장은 보고서를 확인한 후에 20~30일 이내에 필요한 수사를 진행한 후에 다시 보고하도록 지시한다.

수사서류는 모두 디지털로 작성된다. 피해자는 보통 고소장(Police

report)을 온라인으로 제출하며 경찰서에 방문해서도 키오스크를 통해 직접 고소장을 작성하고 증거서류를 스캔하여 제출한다. 지역경찰(Patrol)이 사건을 접수하는 경우 진정인 등에게 아이패드로 진술서를 작성토록 하고 완성된 진술서는 경찰시스템에 자동으로 등록되고 동시에 진정인의 이메일이나 휴대전화로 전송된다. 모든 증거서류는 스캔하여 파일로 업로드 하고 검찰과 법원에도 모두 디지털 파일의 사건 기록만 제출된다.

4) 포렌식계 (Technology Crime Forensic Branch)

우선 포렌식계에 있는 공무원은 모두 민간인이다. 그리고 각 경찰서마다 3~4명의 포렌식 수사관이 배치되어 대부분의 포렌식 업무를 수행한다. 다만 증거물이 훼손되어 복구가 필요하거나 비밀번호나 안티포렌식으로 증거물이 지워지는 등 고급 기술이나 장비가 필요한 경우에는 또는 Police Cantonment Complex (PCC)에 위치한 포렌식 본부에서 진행한다.

<SPF 포렌식 키오스크 모습>

- 장기적으로 경찰관이 스스로 포렌식을 할 수 있는 형태의 키오스크 기계를 개발 중에 있다.
- 모니터와 자판 마우스 그리고 증거품들과 연결할 수 있는 케이플로 구성되어 있다.
- 휴대전화, USB, 컴퓨터 외장하드를 포렌식할 수 있다.

5) 경찰서 사이버범죄 대응팀 (CyberCrime Response Team)

싱가포르는 랜드 디비전(Land Division)이라는 이름으로 7개의 경찰서(Ang Mo Kio Division, Bedok Division, Central Division, Clementi Division, Jurong Division, Tanglin Division, Woodlands Division)가 존재한다.

경찰서에는 1명의 수사과장((Head Investigator)가 있고 그 아래 여러 개의 수사팀이 존재한다. 사이버범죄 대응팀은 팀장을 포함하여 4~5명으로 구성되어 있다. 팀 구성은 보조수사관(Assistant Investigation Officer), 수사관(Investigation Officer), 선임수사관(Senior Investigation Officer)으로 이루어져 있다. 배당은 사건의 난이도에 따라서 간단한 사건은 보조수사관이 민감한 사건은 선임수사관이 담당한다. 그리고 사이버범죄 대응팀은 컴퓨터 오용법과 관련된 사건만

처리를 한다.

<Tanglin Division, Woodlands Division CyberCrime Response Team방문 사진>

마. 안티 스캠사령부 (Anti-Scam Command, ASCom)

싱가포르 경찰은 2022년 3월 22일 사기 조사, 사고 대응, 개입, 단속 및 감지 기능을 통합하여 안티스캠 사령부를 창설하였다. 안티스캠 사령부는 사기방지센터와 3개의 수사팀 그리고 7개 경찰서에 있는 스캠 대응팀으로 이루어져 있다.

사기방지센터에는 7개의 시중은행으로부터 직원을 파견받아 합동 근무를 하고 있고, 스캠신고를 받으면 은행직원의 도움을 받아 즉시 계좌를 동결하여 피해를 예방하고 있다.

<안티스캠사령부 방문 사진>

Ⅴ 결론

청와대 국가안보실은 2019년 국가 사이버 안보 전략을 발표하고 실행계획 까지 마련하였으나 이후 정부기관의 사이버 안보 정책 실행은 지지부진 하다는 평가를 받고 있다. 지난 정권마다 각자의 사이버 안보 전략을 세우고 사이버 안보 컨트롤 타워를 마련하였으나 정권이 바뀌면 내용이 변경되고 컨트롤 타워의 역할이 바뀌는 등 일관성 없이 진행되었다.

국가사이버안보 전략이 정권과 관계없이 지속적으로, 그리고 제대로

추진되려면 반드시 법적·제도적 뒷받침이 필수적으로 선행되어야 한다. 노무현 정부 시절인 2006년 사이버 위기 대응을 위한 범국가 차원의 기본법을 논의하기 시작하였으나, 17년이 지난 지금에도 사이버 보안 관련 법률이 제정되지 못하고 있다.

현재 국정원은 북한의 위협에 대비해 사이버 안보 분야에 집중하고 있다. 그러나 정보기관이라는 특성상 국가 사이버안보 컨트롤 타워로 역할을 하기 어렵고 민간 기업과의 연계도 부족하다. 대통령 국가안보실은 인력과 자원의 한계가 있어 사이버 안보 정책을 직접 실행할 수 없고, 한국인터넷정보원(KISA)은 민간 기업들과 활발한 교류가 있으나, 정부기관에 대한 조사 감독 등의 권한이 없어 국가 사이버안보 컨트롤 타워 역할을 할 수가 없다. 경찰은 사이버 안보 관련 뛰어난 인력과 장비가 있으나 수사기관이라는 한계 때문에 국가 사이버 안보 관련 업무를 맡는 것이 적절하지 않다.

싱가포르 사이버 보안청은 싱가포르 정보통신기술부의 조직을 흡수하여 2015년 설립되었다. 그리고 2018년 사이버 보안법이 통과되면서 사이버 보안청의 역할에 대한 법적 근거가 마련되었다. 싱가포르 정부는 총리 주재로 사이버 보안 전략(CyberSecurity Strategy)을 수립하여 발표하였고 사이버 보안청을 중심으로 보안 전략을 구체적으로 실행해 나갔다. 싱가포르 사이버 보안청은 매년 'Cyber Landscape'을 발표하여 사이버 동향을 검토하고 2020년에는 'CyberSecurity Masterplan 2020'을 수립하여 싱가포르 정부가 수립한 사이버 보안 전략 실행을 구체화 하였다. 그리고 진화하는 기술의 발달과 새로운 범죄 환경에 대응하기 위해 2021년 사이버 보안 전략을 업데이트 하였다.

싱가포르 사이버 보안청은 정부기관을 포함한 국가핵심시설(CII)에 대한 사이버 보안을 강화하고, 사이버 보안 산업의 진흥 그리고 사이버 보안 교육까지 사이버 보안 관련 정책 업무를 총괄하여 수행하고 있다. 그리고 이러한 정책의 일관성으로 인해 싱가포르는 2017년 국제전기통신연합(ITU) 발표한 국제정보보호지수(Global Cybersecurity Index)에서 1등을 하였고 이후 계속하여 상위권을 유지하고 있다. 그리고 2014년 인터폴 제2청사(Interpol Global Complex for innovation, IGCI)를 유치하는 성과도 있었다.

우크라이나는 2014년 러시아의 크림반도 병합에 속수무책으로 당하였다. 러시아의 물리적 진격 이전에 사이버 공격으로 정부 시스템이 마비되었고 가짜뉴스와 선동전과 같은 사이버 심리전에도 밀리면서 제대로 된 대응도 하지 못한 채 크림반도를 빼앗겼다. 그 이후 우크라이나는 NATO 등 서방국가들의 도움으로 사이버 보안을 강화 하였고, 2022년 러시아-우크라이나 전쟁에서 러시아의 사이버 공격을 막아내고 사이버 심리전에도 우위를 점할 수 있었다.

싱가포르도 2018년 발생한 사이버 공격으로 150만 명의 SingHealth 환자 정보가 유출되었다. 특히 해커들은 리센룽 싱가포르 총리의 건강정보를 목저으로 했다고 알려졌다. 이러한 사이버 공격 이후 싱가포르는 사이버 보안법을 개정하여 사이버 보안청의 사이버 공격 조사에 대한 법적근거를 마련하고 컴퓨터 오용법에 국가핵심시설에 대한 공격은 가중처벌 하는 규정을 신설하였다. 그리고 사이버 보안청을 중심으로 국가 핵심시설의 사이버 보안을 강화하고 싱가포르 국립대학 등과 협력하여 사이버 보안 인력을 양성하고 있다.

우선 여러 기관으로 흩어져 있는 국가 사이버 안보 관련 기능을 하나로 합쳐야 한다. 싱가포르의 사이버 보안청(CSA)와 같이 정부와 민간을 아우를 수 있는 기관의 설립이 필요하다. 이러한 기관이 국가 사이버 안보의 전략을 직접 수행하는 기관이 되고 국가 안보실이 위 기관을 지휘 감독하는 형태가 되어야 한다. 그리고 사이버 테러 방지법 또는 국가 사이버 안보법 등 여러 가지 명칭으로 불리고 있는 사이버 안보 관련 법률을 제정하여야 한다. 싱가포르 사이버 보안청은 싱가포르 정보통신기술부의 조직을 흡수하여 2015년 설립되고 2018년 사이버 보안법이 통과되면서 사이버 보안청의 역할에 대한 법적 근거가 마련되었다. 그리고 싱가포르 총리를 중심으로 국가 사이버 안보 전략을 설계하고 사이버 보안청이 정책을 실현해 나가고 있다. 우리나라도 사이버 보안 전담조직의 신설, 국가 사이버 보안 법률의 제정, 대통령실의 사이버 안보전략 설계하는 방법으로 강한 사이버 안보 체계를 마련하여 북한의 사이버 전쟁과 테러로부터 안전한 사이버 공간을 만들어야 할 것이다.

Ⅵ 수집자료 및 기타 참고문헌

2022 한화원, [사이버 전쟁 에 대한 법적 규율에 관한 연구]

2022 사이버 보안 컨퍼런스 송태은 국립외교원 교수 발표

IFANS 주요국제문제분석 2022-19 러시아-우크라이나 전쟁의 사이버전: 평가와 함의 송태은

2022 이용석, 정경두, [한국국방연구원] [러시아 대 우크라이나 사이버 전쟁의 교훈과 시사점]

IFANS FOCUS 2022-28K(송태은) 북한의 사이버 공격과 우리의 대응

2012. 유동열 [(사)한국전략문제연구소] [북한의 사이버 위협 실태와 대응]

2019. 청와대 안보실 발간 '국가사이버안보전략'

2022. 3. 11. 이기종 [뉴스프리존] [사이버안보정책2] 이대로 좋은가 입만 살아있는 사이버 안보 컨트롤'

2020. 4. 6. 이기종 [뉴스프리존] [정부,'국가사이버안보전략' 수립 이후 1년간 성과와 향후과제는?]

2023. 6. 7. 국가안보실 [윤석열 정부의 국가안보전략]

2023. 6. 2. 대한민국정책브리핑 [한미 사이버보안 공동지침 마련]

2016~22 [Government of Singapore] [Singapore Cyber Landscape 2016~2022]

2016 [Government of Singapore] [Singapore Cybersecurity Strategy]

2021 [Government of Singapore] [Singapore Cybersecurity Strategy]

2020 Singapore CyberSecurity Master Plan

2023 CSA [Cybersecurity Act]

[https://www.csa.gov.sg/legislation/Cybersecurity-Act]

2021. 10. 28. [Lim Chong Kin, Drew & Napier LLC] [Singapore: Cybersecurity]

2022. 11. 14. Lim Chong Kin, David Alfred, Albert pichlmaier (Drew&Napier LLC), [Cybersecurity Laws and Regulations Singapore]

2023. 6. 30. https://www.interpol.int/ Who-we-are/Member-countries/ Asia-South-Pacific/ SINGAPORE

2023. 6. 30. https://en.wikipedia.org/wiki/2018_SingHealth_data_breach

2023. 6. 30. www.csa.gov.sg