JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 22, No. 12, pp. 2005-2017, Dec. 2021

Check for updates

COVID-19 시대의 민·관·군 통합 사이버 재난본부 구성 방안

백 인 정[1] · 손 태 식[2*]
[1]아주대 정보통신대학원 정보통신공학과 석사과정
[2*]아주대 정보통신대학 사이버보안학과 교수 손태식

An Integrated Civil,Private,Military Cyber Disaster Headquarters in the COVID-19 Era

In-Jeong Baek[1] · Tea-Sik Shon[2*]

[1]Master's Course, Graduate School of Information and Communication Technology, Ajou University, Suwon-si, Gyeonggi-do, Republic of Korea
[2*]Professor, Department of Cyber Security, Ajou University, Suwon-si, Gyeonggi-do, Republic of Korea

[요 약]

COVID-19로 IT 활용이 급증하면서 사이버위협이 더욱 위협적으로 다가오고 있다. COVID-19 시대에 사이버 공격은 민·관·군을 포함해서 사회의 주요 조직과 시설을 대상으로 하고 있다. 이러한 상황을 기반으로 한국에서 사이버 공격에 대한 대응 태세에 대한 분석이 진행 중이며 미래에는 사이버 공격이 재난 상황으로 이어질 수 있어 이에 대비하고 있다. 현재 COVID-19로 비대면 회의, 온라인수업을 많이 진행하고 사이버 공간에서의 상호작용이 증가하면서 사이버 공격으로 인한 국가적 대형 참사가 발생할 가능성을 가지고 있다. 이러한 위협에 대응하기 위해 국가는 사이버 공격에 국가안보가 위협을 받아 심각한 사회 경제적 손실을 받을 수 있음을 인식하고, 사이버 공간 속에서 안심하고 인터넷을 활용할 수 있도록 민·관·군 통합 사이버 재난본부 구성을 고민해야 한다. 정부 기관의 보안 및 정보화 부서들의 변화가 필요하며 민·관·군 통합 사이버 재난본부 기능을 결집하여 사이버 재난 상황에 능동적으로 대응 할 수 있는 기구와 방안을 본 논문에서 제안하고 시나리오 기반으로 검증한다.

[Abstract]

Cyber threats have become more prevalent and threatening as IT utilization increased rapidly due to COVID-19. Cyber attacks have targeted major organizations, public utilities, governments, military defenses, and the general public. Cyber attacks can lead to major crisis situations and this has prompted an analysis of Korea's response posture to such attacks and what preparations have been made against them. With COVID-19, activities in cyberspace have increased and so have the possibility of a national crisis caused by cyber attacks. To address cyber attacks, the state should recognize that national security can be threatened by cyber attacks and consider forming an integrated public-private cyber disaster headquarters. Changes in the security and informatization departments of government agencies are needed. Measures to actively respond to cyber disaster situations by integrating the functions of the public and private sectors and the military in a cyber disaster headquarters are proposed in this paper covering a wide range of scenarios.

색인어 : 사이버공격, 사이버재난, 민·관·군 통합, 사이버안보, COVID-19
Keyword : CyberAttack, CyberDisaster, Civil·Private·Military Integration, CyberSecurity, COVID-19

http://dx.doi.org/10.9728/dcs.2021.22.12.2005

Received 23 October 2021; **Revised** 17 November 2021
Accepted 17 December 2021

***Corresponding Author; Tea-Sik Shon**

Tel: +82-31-219-3321
E-mail: tsshon@ajou.ac.kr

Ⅰ. 서 론

앞으로 우리는 다양한 안보 위기에 처해 있다. 많은 사건 중에서 사이버테러의 행위의 다양성과 대상의 불특정을 띄며 흔히 자살폭탄테러와 같은 물리적인 폭력으로 규정될 수 있으나, 최근 생화학 테러나 사이버 공격과 같은 새로운 디지털 유형의 형태로 범위가 확대되어 왔다. 이처럼 다양한 디지털 유형의 위험 속에서 '사이버 국가안보의 위험'은 고도로 역동적이며 미래적으로도 파급효과가 막대한 영역이다. 사이버 국가안보 체제를 구축하기 위해 상당한 수준의 IT 및 네트워크 전문기술과 이해가 필요하며, 개인 및 해당 조직, 국가 등 사용범위의 다양성에 따라 사이버 국가안보를 해결하기 위한 시스템이 개선 및 발전되어야 한다.

사이버 공간에서 네트워크 위협 혹은 범죄행위는 자살폭탄테러, 현상 범죄 등과 비교하였을 때 현실적인 문제가 세계적으로 즉각 미치는 피해로 문제화되지 않아 "실제 사이버 공격의 위협은 정말 존재는 하는 걸까?"에 대한 논의가 진행되기도 하였다. 하지만 국가 공공기관에 사이버 공격이 2015년~2020년간 국회 정보위원회에 보고한 자료에 11,727건의 피해사례와 제1, 2금융권에서의 현금인출기 해킹, 국가 중요기반시설의 정보시스템 혹은 컴퓨터 네트워크 및 전산망에 대한 일시적 또는 중·장기적 위협과 동시에 네트워크 장애 혹은 파괴를 유발하는 행위는 실제로 발생하고 있으며 이에 대한 학제적인 연구 방향과 정책적 대응이 요구되기에 이르렀다.[1] 한국은 사이버 국가안보에 대한 논의와 대응이 초기 단계에 처해 있으며, 이에 대한 개념의 이해와 정립이 함께 정책적으로 대응 영역 및 사이버 재난관리 모델에 관한 연구가 진행되어야 한다. 사이버위협 및 사이버 범죄의 특성상 행위에 대한 초기에 컴퓨터 네트워크 시스템의 붕괴나 정보의 유출에서 시작하여 나아가 공격행위를 동반한 테러의 준비단계에서 혹은 테러 집단 소통 채널로 사용될 수 있으며, 대상에 따라 위기의 확산이 폭발적일 수 있다는 이차적 특징을 동반 할 수 있다. 따라서 본 논문에서는 현재 국내 사이버 공격에 관해 관심을 갖고 민·관·군의 주요 기관에서 사이버 공격에 따른 재난 통제 및 사이버 공격에 대한 대응 방안 준비에 현황을 분석하였다. 사이버보안의 위협은 악성코드로부터의 위협, 아이디 도용의 피해와 위협 등으로 다양하며 한국에서 2009년에 사이버 공격 발생 이후 대규모로 사이버 테러가 이어져 주요 기관 홈페이지 마비, 금융권 서버 다운 등 문제가 발생해 왔다. 이에 대한 근원적 차원의 사이버 공격 및 위협에 따른 재난에 대비한 중앙통제 시스템의 모델이 필요하고 나아가 위험유형별 대응 전략 모델을 구체화하였다. 따라서 사이버 공격이라 구분할 수 있는 범주를 규정하고 앞으로 우리가COVID-19 시대에 적합한 민·관·군 통합 사이버 재난본부 구성방안에 중요성을 인식하고 준비하기 위한 연구라 할 수 있다.

Post COVID-19로 삶의 환경이 변화되면서 화상회의, 비대면 수업 등 사이버공간 및 기술에 대한 의존도가 더욱 높아지고 있음을 말하고 이에 반하여 사이버 위협이 증가하였음을 통해 향후에는 사이버 재난에 대한 대응 체계에 대한 고찰의 필요성을 대두시켰다.

5G 시대를 사는 지금 네트워크 및 인공지능, IT 최신 기술의 급속한 성장과 발전으로 생활 속에 인터넷이 급속하게 보급되어 국가 정보화의 기반인프라가 다른 국가에 비해 매우 잘 되어 있는 반면에 주변 강대국들의 사이버위협 속에서 우리가 직접적으로 원격교육이라는 시스템을 도입하고 일부 기업체들에서도 재택근무 등을 인터넷을 통해 관련 업무들을 진행하고 있다. 환경이 변하게 되면 이에 따른 위협도 반드시 존재하게 된다. 지식 정보화 사회에 대한 사이버 공격이 산업과 경제 활동은 물론 국가안보를 근본적으로 위협하는 요인이 된다. COVID-19가 전 세계적으로 대유행하면서 사이버 범죄자들은 교묘하게 악용한 피싱공격, 랜섬웨어 등 사이버 위협이 증가하고 있다.

COVID-19가 확산하면서, 각국 보건당국은COVID-19의 위험을 알리고 간단한 대처 방법 등을 지속해서 전파하고 있으며, 악의적 행위자들은 위기상황을 이용하여 피싱 메일이나 랜섬웨어를 통해 이용자들을 위협하고 있다. 이미 해외 주요 국가들은 한 번의 사이버 공격으로 국가 안보에 구멍이 뚫려 사회적 경제 손실을 일으킬 수 있음을 인식하고, 사이버 가상공간 속에서 자국민이 안심하고 인터넷을 활용할 수 있도록 안정성을 최대한 보장하기 위해서 국가적인 정책을 마련하여 추진 중이다.

앞으로도COVID-19를 이용한 사이버위협도 기승을 부릴 것으로 예상되며 한국에서도 사이버 공격 및 위협으로부터 사전 예방과 사후 복구를 위한 체계적인 관리가 필요하다. 이를 위해 본 논문에서는 사이버 재난 발생 시 존재하는 위협요소를 분석하여 한국형 민·관·군 사이버 통합 재난본부 구성방안을 제안한다. 본 논문에서는 Ⅱ장에서 사이버 재난본부 관련하여 주요 내용 고찰을 시행한다. 본 장에서는 재난관리에 대한 중요성을 인지시킴과 동시에 사이버 재난 본부 개념을 정리하고, 이를 토대로 Ⅲ장에서는COVID-19 전, 후의 사이버 본부사례 비교연구를 통해 Ⅳ장에서 민·관·군 통합 사이버 재난본부 장단점을 비교 및 분석하여 한국에서의 통합 사이버 재난본부 합리적인 방안을 도출하여 Ⅴ장에서는 사이버 통합 재난본부 구성 시나리오를 통해 대응 체계구조를 살펴보고 Ⅵ장에서 결론을 맺는다.

재난은 예방하는 것이 우선이지만 계속 변화하는 환경 속에서 재난은 발생하고 있기 때문에 이에 대한 피해의 최소화가 필요하며 재난은 위험과 불확실성을 내재적 속성을 가지고 있다. 재난관리 과정을 1. 재난의 완화와 예방 및 준비단계, 2. 재난의 대비와 계획, 3. 재난의 대응, 4. 재난의 복구의 4단계로 나눌 수가 있다.[2] 일반적인 재난 발생 시 국가 또는 해당 지역방위 책임관으로 지휘를 받기 때문에 대응하는 부분부터 이질성, 지휘체계의 혼선과 정보공유 및 기관의 협조가 미흡한 것이 현실이다.

Ⅱ. 관련연구

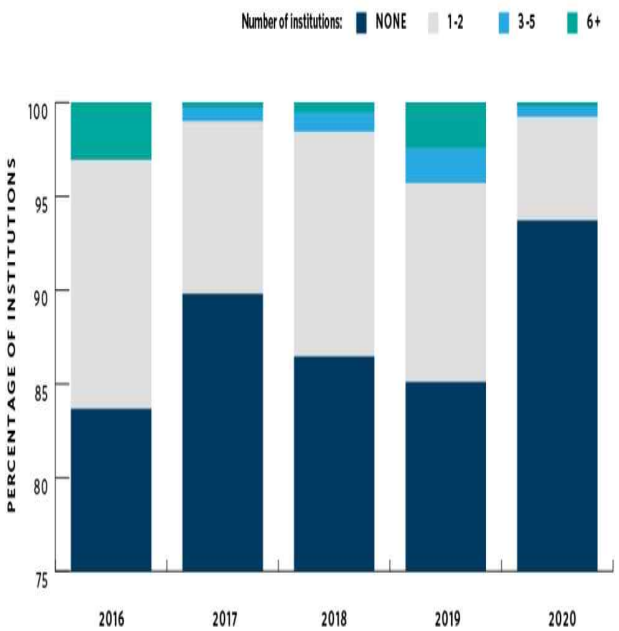

그림 1. 한국 사이버공격 피해현황[1]
Fig. 1. Cyber Attacks That Caused Damage in the Korean Public Sector

현재COVID-19로 인해 IT를 활용하게 되는 요즘 사이버 공격으로 국가 재난 상황이 발생한다면 "우리는 현재 시스템으로 대응이 가능한가?"라는 의문과 함께 현재COVID-19 시대 비대면, 디지털전환 가속화에 따라 그림1처럼 사이버 공격은 더욱 증가하고 어디에서는 지금도 피해 보고 있다. 그렇기 때문에 사이버 공격에 대한 대응 체계를 고도화해야 한다.

하나의 관리체제 속에서 각각의 고유 기능들을 하나로 통합 관리할 때 효과적인 사이버 재난관리의 총체성으로 인해 사이버 공격에 대응하는 각 기관과 정부의 조정과 통제 등 필요한 활동체제를 갖추는 노력 또한, 사이버 재난관리에 필수적인 요소이다. 사이버안전(국가·공공)분야 위기 대응 매뉴얼에서 국가정보원은 '국가 위기관리 기본지침(대통령훈령 제229호)' 및 사이버안전분야 위기관리 표준 매뉴얼'을 근거로 '사이버안전 국가·공공분야' 위기상황 발생 시 국가정보원이 적용할 세부 대응 절차 및 제반 조치사항 등을 표 1.와 같이 만들어 각 공공기관에 비치하고 있다. 국가정보원은 재난 위기 징후를 포착하거나 재난 위기 발생이 예상되는 경우, 그 위협 또는 위험의 수준을 평가하기 위한 자체 위기평가 회의를 구성하고 회의를 통해 도출된 평가 및 판단 결과에 따라 위기 경보를 발령한다. 위기 평가 회의는 국가사이버안전센터장을 의장으로 하고 국방·행안부·방통위 등 6개 부처 파견관 및 의장이 지명하는 사이버안전 센터 3급 공무원을 위원으로 구성한다. 국가정보원은 위기 경보 발령 시 국가위기상황센터 및 유관기관에 신속하게 통보하고, 범정부 차원의 평가와 조치가 요구되는 수준의 경보를 발령하는 경우에는 국가위기상황센터에 통보한다. 중앙행정기관은 정보 수집 시 산하기관과 소속기관 및 지방자치단체에 경보 발령 사실을 신속히 전파한다. 위기 대응 매뉴얼은 사이버 공격에 대해서 신속하게 대응하고 피해를 최소화하기 위한 것으로 사이버 재난위기경보 발령 및 사이버 공격에 따른 대응 요령을 전파하고, 사이버 공격에피해 원인을 파악하여 대응책을 수립한다. 신속한 복구 지원을 하고, 피해확산 방지를 위해 사이버 공격진원지와 경유지를 네트워크상에서 차단하고, 국내외 사이버안전 관련 유관기관 및 업체와 공조하며 사고 재발 방지대책을 수립하고 이행한다. 심각 단계의 경우 범정부 차원의 합동 조사본부를 구성하여 운영하게 되어 있다. 아울러 복구지원본부를 구성하여 국가안보와 관련된 기관, 핵심기반시설 운용기관, 대국민 행정서비스 제공기관 등의 순으로 피해복구를 지원한다.[3]

실질적으로 한 기관에는 이러한 시스템이 있지만, 현실적으로 통합상황을 이루고 있는 곳 그리고 훈련들은 찾아볼 수가 없으며 사이버 재난 발생 시 효율적 대응 수행이 어렵다. 그래서 우리는 민·관·군 통합 사이버 재난 본부 구성을 통해 중앙통제가 원활하게 이루어지는 부분이 필요하다고 생각하는 요즘에 조금 더 통합적이면서 간단한 조직 구성도가 정부 정책적으로 검토가 되어 국가적인 사업과 제도가 통과되어 진행될 수 있도록 서로가 힘을 통합 해야 한다.

표 1. 사이버위기관리 표준 매뉴얼[4]
Table 1. Cyber Safety Crisis Management Manual

Stage	Cyber incident response
Routine	· Perform routine health checks on the servers, network, security equipment, security policy, etc. · Monitor vulnerabilities and released security patches for deployment (i.e., security updates to the operating system, application software, middleware, etc.) · Update the antivirus signatures and definitions. · Monitor and review alerts from the intrusion detection and prevention systems. · Monitor traffic on service ports. · Identify trends in threats and vulnerabilities.
Attention	· Notify internal stakeholders and customers of a cyber threat requiring "Attention". · Verify that antivirus signatures and definitions are up-to-date · Deploy critical operating system security patches · Recommend blocking of unused ports that are not required for corporate internal services. · Review of the emergency response network by the Incident Response Team. · Routine operations are performed as usual.
Caution	· "Caution" notification is sent to internal stakeholders and customers regarding a potential cyber threat that might affect the company. · Verify that antivirus signatures and definitions are up-to-date · Deploy critical operating system security patches · Recommend blocking of unused ports that are not required for corporate internal services. · Check for abnormalities in all systems and IT infrastructure. · Perform tasks under the "Attention" stage.

Warning	· Send a “Warning” message to internal stakeholders and customers regarding an active cyber threat on the company. · Monitor news and media coverage on the cyber threat. · Continuous inspection of all systems and IT infrastructure. · Recommend minimizing PC use in companies. · Review of the emergency response network by the Incident Response Team. · Perform tasks under the “Caution” stage.
Critical	· Send a “Critical” notification to internal stakeholders and customers regarding an active cyber attack on the company. · Monitor news and media coverage on the cyber attack. ·Monitor the entire network ontinuously (24/7) and block corresponding ports and services used in the cyber attack. · Disconnect the infected systems and infrastructure from the internal network. · Mobilize the emergency response network. · Perform tasks under the “Warning” stage.

Ⅲ. COVID-19 전·후의 국외 사이버 본부 사례 비교연구

사이버 본부사례를 통해 국내의 통합 사이버 재난본부의 장단점을 비교 및 분석하며 향후 발전할 방안들이 어떤 구조적인 요소들이 포함되어 있는지 비교 분석해 보고 해외국가들의 사례들을 통해 국내 민·관·군 통합 사이버 재난 본부 구성안 발전 및 향후 사이버보안 법안에 포함되어야 할 선진국 대상으로 비교분석 하였다. 더욱 효율적인 방안들을 강구 할 수 있도록 내용을 분석하고 해외 국가에 대한 사이버 본부 구성을 비교한다.

3-1 해외사례 비교분석

표 2. 2020년 해외 사이버보안 지수 국가별 비교[5]
Table 2. Global Cybersecurity Index 2020: Country profiles

Country	Global Rank	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
U.S.A	1	20	20	20	20	20
U.K	2	20	19.54	20	20	20
Korea	4	20	19.54	18.98	20	20
Japan	7	20	19.08	18.74	20	20
France	9	20	19.21	18.98	19.48	19.41
India	10	20	19.08	18.41	20	20
Germany	13	20	19.54	18.98	19.48	19.41
China	33	20	17.94	16.63	19.04	18.91

The following table sets out the score and rank for each country that took part in the questionnaire of the International Telecommunication Union (ITU). This measures the commitment of each country to cybersecurity.
※ A maximum of 20 points can be awarded for each of the five pillars.

지금도 표적을 두고 랜섬웨어의 공격은 우리가 잠을 자는 시간에도 끊임없이 진행되고 있다. 2020년의 랜섬웨어는 COVID-19 대유행에 따른 위장형 공격과 원격근무 시스템을 노린 이메일, 원격접속 등에 대한 공격이 유행하였다. 공격자는 더 많은 금전적 자산 이득을 위해 랜섬웨어의 변화를 시도하고 있으며 공격 양상이 변화하고 있다. 2021년 랜섬웨어 표적형 공격대상의 범위가 확대되고 감염될 경우 피해 역시 증가할 것이다. 표 2.와 그림 2.를 참고로 미국부터 살펴보면 미국의 사이버 보안 대응 체계는 모든 기관의 역량을 하나로 통합하고 단일화한다. 국가 사이버보안 업무의 중앙통제 역할을 수행하는 부처가 있고 정책을 자문하는 곳, 네트워크 보호와 국방 부문의 주요 기반시설 관리와 미연방 네트워크 주요기반시설 보호와 각종 국가 사이버 위협에 대응하는 기관들이 자리 잡고 있다.

영국의 경우 내무부와 통신정보 수집과 제공을 담당하고 있는 부처들과 국가 산업발전을 위해 정보보호 정책을 담당하는 곳이 있으며 외부로부터의 사이버테러 공격에 대처하고, 정부의 정보보호와 관련된 활동들을 조정한다. 특히 사이버 범죄 및 테러에 대응하는 역량과 네트워크 복원력을 강조하는 기조를 유지하고 있다.

일본은 사이버보안 기본법에 따라 사이버보안 감사를 수행하고 정부뿐만 아니라 통합된 행정기관과 특수기업 및 증인 된 기업에서 적절한 조언을 제공한다.

중국은 국가안전부가 국내적 차원에서 사이버 안보 업무를 전체적으로 총괄하는 한편, 산하 기술정찰국을 통해 사이버 보안 정책을 수립한다. 공안부는 국가 기밀 보호를 위한 역할을 수행하고, 인터넷 경찰은 사이버 범죄, 반체제 운동에 대한 감시 활동을 통해 국제협력 전략의 지향성이 미국처럼 개인정보보호나 자유의 보장이라는 가치를 추구하기보다는 국내의 회의 통제와 외국기업에 대한 규제 등을 목적으로 한다.

인도의 경우 비대면 환경이 필수가 되면서 새로운 업무 문화가 생겨나고, 산업 분야에서 디지털화를 가속화 하다 보니 모든 산업 분야에서 디지털화를 가속화하고 있다. 재택근무자를 대상으로 악성 첨부파일을 포함한 이메일을 발송하거나 악성 웹사이트 접속을 유도하여 악성코드에 감염시키는 공격이 나타나고 있다.

독일의 경우는 사이버보안위원회에서 정보보안 관련 전략 수립과 정책의 자문을 담당하며, 연방 정보기술위원소속 기관이다. 사이버보안 관련 업무를 전담토록 하고 있다. DFN-CERT는 정보통신 기반 사고 대응을 위한 사이버사고 처리, 사건 처리에 필요한 기술적 지원, 관련 정보 수집, 제공 분석 등의 업무를 수행한다. 사이버 연방군은 사이버 군부대로 사이버보안, 군사작전 등을 담당하면서 현재는 자국의 사이버 보호를 제3국 보안기업의 제품들에 의존하고 있어 핵심기술을 확장해나가기 위해 노력하고 있다.

마지막으로 프랑스의 경우 민간영역과 공공의 영역 전체에 대해 가해지는 사이버 공격 및 위협에 대한 대응책을 규율하고 있다. 중국이나 러시아와 같은 국가 행위자로부터 위협

보다는 중동지역 이슬람 세력을 더 심각한 위협으로 인식하고 대응하는 과정에서 형성되어 있다. 프랑스가 국방 차원에서 구축한 사이버 방위의 시스템은 전통적인 군사 안보의 시각에서 본 대응이라기보다는 국가업무 전반을 강조하는 사이버 안보의 관점으로 판단된다. 국가별 특성에 따라 다양한 사이버 재난 구조로 반영하고 있지만 여기서 공통점은 모든 국가가 이사이버 공격 및 위협에 대한 문제를 국가안보의 시각에서 인식하고, 이에 대한 대비책을 한층 강화하고 있다는 사실이다. 아래 그림 2.에서처럼 국가별 사이버 공격 및 위협에 대해 우선순위를 높이고 인적·물적인 사항과 법 제도 정비에 중점을 갖고 통합 사이버 재난본부를 수행하는 부처와 통합지휘본부에 대한 기능을 사후적 반응이 아닌 전반적 정비를 통해 대응 개념의 도입을 본 논문에서 제안한다.

그림 2. 해외 사이버 보안지수[6]

Fig. 2. GCI(Global Cybersecurity Index) results: Score and rankings

그림 2.에서는 해외 국가들의 사이버 보안 지수들을 비교하였다. 확실하게 선진국들의 사이버보안 지수는 높고 그만큼 사이버 공격으로부터 국가적 관점이 반영되었다고 평가 할 수 있다.

3-2 선진국(미국, 영국, 일본)의 세부적인 사례 비교분석

표 3. 미국 사이버보안과 관련 부처의 역할 [7]-[14]

Table 3. The role of US cybersecurity agencies and related federal departments

Agency/ Department	Role
Cybersecurity and Infrastructure Agency (CISA)	· Builds the national capacity to defend against cyber-attacks and works with the federal government to provide cybersecurity tools, incident response services and assessment capabilities to safeguard the federal civilian executive branch networks that support the essential operations of partner departments and agencies.
National Security Agency (NSA)	· Through their Cyber Security Collaboration Center, the NSA prevents and eradictes threats to U.S.
Cyber Threat Intelligence Integration Center (CTIIC)	· Produces coordinated IC analysis of foreign cyber threats to US national interests, ensure the information is shared among the federal cyber community, and support the work of operators, analysts, and policymakers with timely intelligence about significant cyber threats and threat actors.
Office of the Director of National Intelligence (ODNI)	·Responsible for leading the Intelligence Community in intelligence integration through synchronizing collection, analysis, and counterintelligence.
Department of Homeland Security (DHS)	·Responsible for safeguarding the American people, their homeland, and their values. Their scope includes securing cyberspace and critical infrastructure.
Department of Defense (DoD)	· Established United States Cyber Command in 2010 to unify the direction of cyberspace operations, strengthen DoD cyberspace capabilities, and bolster DoD cyber expertise.
Department of Justice (DoJ)	· Enforces the law and defends the interests of the United States according to the law. · The FBI operates under the jurisdiction of the DoJ. It is the lead federal agency for investigating cyber-attacks and intrusions.
Department of Commerce (DoC)	· The National Institute of Standards and Technology operates under the DoC. This agency is responsible for the standardization of cybersecurity practices through the NIST Cybersecurity Framework.
NSC (National Security Council)	· The US President's principal forum for considering national security and foreign policy matters with senior advisors and cabinet officials.
Office of Management and Budget (OMB)	· the OMB was assigned cybersecurity-related tasks including, but not limited to, reviewing agency-specific cybersecurity requirements and taking the appropriate steps to ensure to the greatest extent possible that service providers share data with agencies, CISA, and the FBI as may be necessary for the Federal Government to respond to cyber threats, incidents, and risks.

선진국의 사례를 세부적으로 살펴보면 현재 사이버 미국의 사이버보안 대응 체계는 사이버 국가보안과 사이버테러를 동일한 개념으로 인식하고 국가 모든 기관의 역량을 통합하고 단일화한다. 표 3.에서의 세부적인 기능을 살펴보면 국가안보위원회에서 국가 사이버보안 업무의 중앙통제 역할 이행하고 사이버보안국에서 대통령의 사이버보안 정책을 자문하며 활동하고 있다.

국방부에서 군사 네트워크 방어 및 보호와 국방 부문의 국가 주요 기반 시설들을 관리하며, 국토안보부는 미연방 네트워크와 국가 주요기반시설 보호, 각종 사이버 공격 및 위협에 대응하고 산하 기관인 국가 사이버보안 통신 통합센터에서 각급 기관과 민간의 사이버 공격에 대한 정보를 취합하여 분석하는 기술들을 지원한다.

법무부의 연방수사국은 사이버 범죄 활동 수사를 담당하며, 상무부의 국립표준기술연구소에서 사이버 보안 및 네트워크 관련 기술개발과 표준 업무를 담당한다. 국가정보국의 사이버위협정보통합센터는 사이버위협, 사고의 종합적 분석, 그리고 유관 및 민간기관과 네트워크 정보를 공유하는 역할을 한다. 예산관리국은 전자정부 정보기술, 연방 기관의 사이버보안 감독 등의 연방정부의 네트워크 정보시스템 보호 역할을 하고 있다.

미국의 사이버보안과 관련된 정부 조직의 주요 부처와 역할은 최대한 유관기관 및 민간기관의 종합적 네트워크 정보 분석을 통해 정보공유를 하고 있다는 부분은 다른 국가에서도 벤치마킹해야 한다. 범정부의 국가 정보시스템 지위와 역할이 균형적으로 잘 나타났다. 독단적인 작전을 수행하거나 의사결정을 하는데 최대한 많은 의견이 반영된다면 사이버 공격 시에 빠른 대응을 하기에 제한된다. 하지만 제한사항들이 발생 할 수 있다는 범위안에서 기능이 다른 기관들과 조율하면서 모든 기관을 통합하며 사이버 재난을 중앙통제 시스템에서는 사이버 재난발생 시에 각 기관에서 통제하는 것이 아닌 국가안보실에서 총괄적으로 민, 관, 군을 통해 대응하려는 부분을 다음과 같은 형태로 수정하면 좋을 것이다. 한국의 중앙통제시스템은 역량이 분산되어 있다. 이것을 통합시켜야 한다. 정보통신기술의 발달과 사이버 공격의 다양성에 효과적으로 대응하기 위해서는 관련 법안들의 정비가 필요하다. 사이버보안 정책 추진을 위해 국가 및 공공기관의 사이버안보 의식 강화를 위해 대국민 대상으로 홍보 활동을 통해 사회 전반적인 사이버보안 의식을 향상해야 한다. 사이버보안 의식 확산과 다양한 교육 및 홍보 프로그램 개발을 통해 정부 및 공공기관, 국민, 민간기업 등을 대상으로 사이버보안 실천 활동을 강화한다. 이를 통해 민·관·군 사이버훈련 정례화 및 체계화를 추진하여 사이버보안 방위 훈련을 강화 할 수가 있다. 사이버보안 개념에 대한 인식이 국민들에게 공유가 된다면 유기적 협력 체계로까지 발전할 수 있다. 국가 사이버 안보 강화를 위해 정보보안 인재 양성과 프로그램 개발을 통해 화이트해커 사이버 예비군에 집중적으로 지원을 할 수가 있다.

표 4. 영국 사이버보안과 관련 부처의 역할 [15]-[18]
Table 4. The role of the United Kingdom cybersecurity and related ministries

Agency/ Department	Role
National Cyber Security Centre (NCSC)	·Launched in 2016, this agency supports the most critical organizations in the UK, the wider public sector, industry, SMEs as well as the general public. They provide effective incident response to minimise harm to the UK, help with recover, and learn lessosn for the future.
Government Communications Headquarters (GCHQ)	·GCHQ is a world-leading intelligence, cyber and security agency with a mission to keep the UK safe. ·It is responsible for information collection, decryption, interpretation/translation, information decryption of digital communications.
Communications-Electronics Security Group (CESG)	·Originally a department under GCHQ, in charge of information assurance.This agency is now part of the National Cyber Security Centre. ·It provides information assurance policies and related services to the government and major consumers for the purpose of protecting important UK secrets as well as providing advice on the security of communications and electronic data. ·It supports the establishment of national information security-related policies and guidelines, and provides technical advice and solutions necessary for the implementation of information protection policies of each ministry (Jongha Ahn, 2014).
Centre for the Protection of National Infrastructure (CPNI)	·CPNI is the government authority for protective security advice to the UK national infrastructure. Its role is to protect national security by helping reduce the vulnerability of the national infrastructure to terrorism and other threats. It is accountable to the Director General of the MI5. ·NSAC is in charge of personnel and facility security, and through the newly launched CPNI, converges physical and cyber security (Yeonsu Lee, 2009)

영국 주요 기반시설 보호는 내무부와 통신정보 수집과 제공을 담당하고 있는 외무부가 있으며, 국가 산업발전을 위해 정보보호 정책을 담당하는 기업혁신기술부 등이 영국의 사이버보안을 담당하고 있는 대표적인 정부 부처다. 표 5.에서 살펴보면 정보통신본부는 외무부 산하 통신 정보기관으로 전자기파, 음향, 기타 설비 장비로부터 나오는 방사물, 암호화와 같이 정보자료와 관계되거나 이로부터 생산되는 정보를 획득, 처리하고 있다. 내각부 산하기관으로 정보보증 중앙 기구는 외부로부터 사이버테러 공격에 대처하고, 정부의 정보보호와 관련된 활동을 조정한다. 통신 전자 보안 단은 통신과 전자 데이터 보안을 위한 자문, 영국의 중요한 기밀 보호, 그리고 정부와 소비자에게 정보보증 정책과 관련된 서비스를 제공한다. 응용 보안기술부는 영국의 국가 중요 기반시설을 보호하고 새로운 네트워크 기술을 소개하는 영역까지 업무를 확장하고 있다. 영국의 국가 사이버보안과 연관된 정부조직의 주요 역할은 표 4.를 참고하면 된다. 특별하게 중심을 잡고 통제하는 부처가 없으며, 부처별 역할에 대한 특성이 강하게 보이지만 국가적인 사이버 재난 발생 시 통합적으로 조직이 움직이는 방식으로 구성되어 있지 않아 중요한 결심을 하는 상황에서 혼란을 가중하고 그에 따른 상황에 피해를 볼 것으로 예상된다.

표 5. 일본 사이버보안 부처의 역할[19]-[21]
Table 5. The role of Japan cybersecurity agencies and related ministries

Agency/ Department	Role
Cyber Security Strategy Headquarters	This Cybersecurity Strategic Headquarters was established under the Cabinet in 2014 to effectively and comprehensively promote cybersecurity policies. It is headed by the Chief Cabinet Secretary, with the Minister of Cybersecurity as deputy. The Cybersecurity Strategic Headquarters decides and revises the Common Standards, formulates basic policies of audits and publishes audit results, and decides the direction of the policies. It also develops and implements a cybersecurity strategy plan and prepares guidelines related to the plan implementation of each department and province. It is comprised of the Critical Infrastructure Expert Panel, Technological Strategy Expert Panel, Human Resources Expert Panel for Dissemination and Enlightenment, and the Cybersecurity Measures Promotion Committee
IT Integration Strategic Headquarters	· This agency oversees policies and strategies for the IT sector and deliberates and adjusts information and communication strategies. It also coordinates ICT R&D support policies.
Information Processing Promotion Organization	· It is responsible for improving the reliability of IT systems and strengthening industrial cybersecurity capabilities, including nurturing IT talent (Kwon Heonyeong, 2016). ·This organization also supports the establishment of national information security-related policies and guidelines, and provides technical advice and solutions necessary for the implementation of information protection policies of each ministry (Ahn Jong-ha, 2014)
National Center of Incident Readiness and Strategy for Cybersecurity (NISC)	The NISC was established in 2015. It works together with public and private sectors on a variety of activities to create a "free, fair, and secure cyberspace." It plays a leading role as a focal point in coordinating intra-government collaboration and promoting partnerships between industry, academia, and public and private sectors. It coordinates cybersecurity policy by formulating: · Cybersecurity strategy · Cybersecurity policy for Critical Infrastructure Protection · Common Standard on Information Security Measures of Government Entities · Cybersecurity Human Resource Development Plan · Cybersecurity Research and Development Strategy · The NISC also takes on the role of a government CERT and together with the JPCERT/CC, work as a national CERT.
Other government departments with cybersecurity-related responsibilities	· National Police Agency: responds to and investigates cyber crimes · Ministry of Internal Affairs and Communications: formulates policies on network communications · Ministry of Economy, Trade and Industry: formulates policies on the IT industry Ministry of Defense: responsible for cyber security as part of national security

일본에서는 사이버보안 기본법에 따르면 표 5.에 사이버보안 전략본부가 전략추진 사령탑 역할을 수행하고, 내각관방 산하의 정보보호센터는 사무국으로서 전략에서 근거한 정책을 추진한다. NISC는 국가 사이버보안 감사를 시행하고 정부뿐만 아니라 통합된 행정기관과 민간 특수기업 및 승인된 업체들에 적절한 사이버 보안에 관한 조언을 제공한다. 민간통신사업자, 방송사, 보안업체 등으로 구성된 네트워크 기술정보 공유 분석센터는 사이버 공격에 대한 지식을 공유하고 조치를 하고 있다. 또한 NISC는 국가 사이버보안 전략본부 및 관련 실무 그룹의 홍보와 인적 자원 개발에 관해 연구위원회에서 학계, 산업계 및 정부 전문가와 사이버보안 인적 자원 개발의 정책 및 프로그램에 대해 논의한다. 내각관방 산하기관인 일본 정보보호센터는 국가 사이버보안 정책을 담당하며, 일본 정부의 네트워크 보안 정책을 추진 및 평가하고 전략 방향을 제시한다. 일본의 사이버보안과 관련된 정부조직의 주요 부처와 역할은 표 5. 와 같다. 일본도 마찬가지로 미국처럼 통합적으로 민·관 전체를 통제하는 중앙통제 시스템이 있지만, 전문인력 육성을 위한 교육 훈련 프로그램이 세부적으로 갖춰있지는 않은 것 같다. 사이버 재난 관리를 위한 사전교육 프로그램은 재난 발생 가능성을 줄이고 발생 시 복구 시간을 최소화하기 위한 방향으로 기본적인 교육과 훈련으로 피해의 효과를 최소화 할 수 있다. 이렇게 미국, 영국, 일본의 세부적인 사례를 비교하였다.

Ⅳ. 제안하는 국내 민·관·군 통합 사이버 재난 본부 구성 강점

표 6. 에서 나타나는 것처럼 민·관·군 통합 사이버 재난 본구 구성 시 강점과 약점을 알 수 있다. 이것을 바탕으로 현재COVID-19시대에 사이버 재난본부 구성안을 세부적으로 제안하려고 한다.

먼저, 사이버 재난 예방하기 위해서 사이버안전 대책을 강화하는 기본적인 매뉴얼 항목들이 절실하게 필요하다. 다른 국가와 비교하였을 때 우리나라에서는 국가 차원에서 사이버 재난 상황에 대한 방안을 체계적으로 관리할 수 있는 절차가 정립되어 있지 않아 위 사항을 조기 특성화고등학교 설립을 통해

향후 미래지향적인 차세대 정보통신 산업군으로 직업과 연계될 수 있는 국가적인 관심 사항으로 발전시켜야 한다고 제안 한다.

두 번째로 사이버 공격은 공간 및 시간에 제약이 없다. 세계적인 문제가 발생할 수도 있고, 지금 어디에서 계속해서 사이버 공격을 시도하고 있을지 모른다. 이에 따라 UN 동맹국 들로부터 사이버 공격에 대한 자료가 실시간으로 공유 되어 공유된 정보를 축적하여 모의훈련으로 상황을 재구성하여 사이버 공격 및 위협으로부터 예방 및 방어 할 수 있는 훈련체계 방안을 만들어야 한다고 제안한다.

표 6. 민·관·군 통합 사이버 재난본부 강점과 약점[22]
Table 6. Strengths and weaknesses of the integrated cyber disaster headquarters of the public, public, and military.

Strengths	Weakness
· Threat intelligence analysis dissemination: Due to the integration of the public, private, and military sectors, threat intelligence gathering can be centralized, with the analysis disseminated quickly among them. This allows for a quicker response time to incidents as all affected sectors are informed of the cyber threat in a timely manner.	· Choice of the appropriate operating model for the integrated cyber disaster headquarters: There are several operating models that can be selected for operating the cyber disaster headquarters. However, the challenge is to determine the parties responsible and accountable for the critical infrastructures being protected as well as the overall party in charge of the cyber disaster headquarters. Currently, there is an overlap of responsibilities between the public and private sector over the management of critical infrastructure. Another matter to consider is the fundamental difference in the operating approach of the public and private sectors and the military forces. It is known that governments have longer processes and slower response whilst the private sector prioritizes efficient operations.
· Integration of operations and improved knowledge and skill-sharing: An integrated cyber disaster headquarters facilitates operations that combine the resources of the public sector, the private sector, and the military forces. This allows for easier coordination of resources required to respond to cyber incidents across all sectors and industries. Moreover, the public and private sectors and the military forces can pool their knowledge and expertise and learn from each other on how to strengthen their cyber defense mechanisms.	· Professional manpower required for integrated cyber disaster headquarters: Attackers target a wide range of continuously changing IT landscape, creating the challenge of hiring security experts for each piece of technology requiring protection. Moreover, the challenge does not only lie on hiring the required professional manpower but also providing regular training for them on the evolving technologies they must protect and the constantly changing techniques used by attackers.
· Defined communication lines: Not one organization has a big picture view of the state of cybersecurity or of the full extent of the cyber threats they are facing. Thus, having defined communication lines between the public, private, and military sectors allows them to have a clearer picture of their cyber landscape, to mobilize resources efficiently, and to provide the right information to the right people for decision-making.	· Time and resources required for setup and stabilization of operations: A cyber disaster headquarters requires substantial resources, not just in manpower, but also in technological and financial resources. Moreover, there may be legal and regulatory requirements, such as those on data privacy, that need to be considered. Integrated operations between the various sectors involved require a significant amount of time from the preparation stage until operations have stabilized. For the integrated cyber disaster headquarters, careful long-term planning and execution is important for it to be effective. As such, a cyber disaster headquarters cannot be quick solution to the immediate need of responding to increasing cyber threats and attacks.
· Simplified decision-making: With the integration of the public, private, and military sectors, simplified escalation and decision-making procedures can be defined and implemented. With te key decision-makers for the various types of cyber-attacks already identified, response times will be quicker, limiting the impact of the attack.	· Amount of information sharing of each involved sector: For the integrated cyber disaster headquarters to be effective, trust is essential amongst the sectors involved. This is especially true for information sharing. However, the private sector has always feared government interference and has thus limited the information they shared. On the other hand, the government, through the public sector and the military, may not be willing to share information on matters of national security and defence. There has also been an increasing concern from the people on their data privacy that must be considered. It is necessary for all parties involved to identify the level of information sharing and trust needed for their cyber operations to be effective.

현재 시점에서 사이버에 관한 국내, 국제법이 명확하지 않기 때문에 이런 사항들이 시급하게 보완이 필요하다고 제안한다.

세 번째는 전문인 양성을 위한 국가적인 지원 그리고 처우 개선이 시급하다고 제안한다. 다른 국가에서는 수많은 돈을 투자하여 인력양성을 하는 사례가 있다. 정부가 중심을 잡고 인재 발견 및 사이버 전문인력 양성을 하는 사례가 많이 있으며

지금도 다른 국가에서는 인력을 양성하기 위해 심혈을 기울이고 있을 것이다. 한국에서도 중앙정부가 중심을 잡고 인재 발견 및 양성을 통해 적극적인 정부 정책이 필요하다고 제안한다.

한국의 현실적인 사이버 안보 상황을 살펴보면 국민 비율 대비 인터넷 사용과 네트워크 구축에 따른 인프라 강국이라고 하면서도 사이버보안은 취약국이라는 것이 차질없이 드러난다. 북한발 사이버 공격과 중국과 러시아의 사이버 공격 마저 위협도 는 세계적으로 유래까지 없을 정도로 높아지는데 이런 취약한 상황들을 민간, 공공대상으로 저액이 통합된다면 침해 대응 역량이 강화될 수 있는 부분과 사이버 중앙통제에 예방, 대응 중심 기능이 집중되면서 기술 개발과 인력 양성, 산업이 집중될 수 있다. 보다 통합관제, 사이버 사고 조사 등 권한이 분산하지 않고 집중해서 충분한 사이버 통합 재난본부를 운영 할 수 있다고 판단한다. 정보공유와 기반시설 관리 강화와 기관별로 분산된 사이버보안 대응 영역을 한곳으로 집중한다면 사전에 피해에 대한 대응을 충분히 할 수 있다. 제안하는 사이버 통합 재난본부를 민·관·군 구성방안으로 단일화보다는 통합하는 방안으로 사이버통합 재난본부를 구성해야 한다.

첫째, 주요 국가들의 사이버 통합 재난 본부 구성을 볼 수 있었고 우리나라도 그에 따른 조직들은 갖춰져 있다. 하지만 여기서 더 보완해야 할 사항을 제시한다면 먼저, 전반의 디지털 의존도가 높아진 시대 흐름에 관련법 체계개선 및 법적 기반 확보가 필요하다. 앞에서 2006년 법안 마련에 노력하였지만, 물거품이 되었다. 21대 국회에서 조태용 의원이 국가 사이버 안보 정책 조정 회의를 설치하고 사이버 안보 기본법안을 발휘한 지 1년 넘게 위원회 심사 단계에 계류 중이다. 범국가적 사이버보안 문제를 해결하기 위해 사이버보안 정책을 국가적 차원에서 설정하고 이를 관련 법률에 적용하는 것이 절대적으로 필요하다. 현재 상황에서는 개인정보보호와는 달리 사이버보안을 규율하는 기본법이 존재하지 않기 때문에 부문별 법률에 나누어 해당 부분의 원칙만 정할 수밖에 없다. 정책 수립 관련 규정의 실효성 부족을 보완하기 위해서 관련 내용을 정립하는 것이 필요하다. 한국은 아직 국가 차원에서 사이버 공격으로부터 체계적으로 관리할 수 있는 제도와 정치적 의견이 구체적인 방법 및 절차가 정립되어 있지 않아 사이버 공격 및 위협으로 가상현실에서 위기 발생 시 국가안보와 국익에 중대한 위협과 손해를 끼칠 우려가 있다. 그렇기 때문에 국가 사이버보안 기본계획 및 시행계획, 정보공유 민관 협력체계 강화, 주요정보통신기반시설 관리강화, 침해사고 대응을 위한 대책본부 구성, 민관으로 나뉘어 있는 경보체계 통합 등이 전반적인 사이버보안 기본법 정비가 필요로 하다. 국가 사이버안보실현을 위한 부분, 국가 사이버통신 통합을 법제화 하는부분, 사이버 인력관리 수행을 위한 관리 감독직 채용방식 및 처우 개선, 사이버 인력개발 및 교육과 공공기관과 민간의 장벽을 낮추는 방안들이다.

둘째, 동맹국의 전산통합 체계를 마련해야 한다. 사이버 공격 및 위협은 특성상 24시간 공간과 시간에 제약 없이 한 국가만의 문제가 아닌 세계적인 문제로 대두할 수 있다. 사이버 공격 및 위협에 신속하게 대응하기 위해서는 국가적 공조가 필수적으로 이루어져야 한다. 아직 국내법과 상충한다는 이유로 한국은 가입되어 있지 않은 상황이다. 최근 정부에서도 가입의 필요성을 인식하고 동맹국 가입을 위한 준비 작업이 진행 중이다. 이 부분을 지혜롭게 제도개선에 발판이 된다면 효과적인 사이버전에 대응하고 새로운 공격 방법을 연구하여 위기로부터 초기에 바로 잡을 수 있다.

셋째, 사이버안보 전문인력을 양성하는 방안이다. 사이버 의존도가 높아짐에도 불구하고 한국에서는 사이버 전문인력 양성과 처우가 미흡하고 지금 주변을 보아도 쉽게 공감할 수 있다. 또한, 국가적인 전문인력 프로그램이 많이 있다고 하지만 실질적으로 사회에서 활용하는 것은 많이 없다고 본다. 사이버 전문인력을 양성하기 위해서 선진국에서는 다양한 정책을 마련하고 교육하고 있다. 한국에서도 국가적 차원에서 교육 체계를 확립하고 전문인력을 양성해야 수준을 높일 수가 있다. 국방영역에 사이버 공격 훈련 시스템을 도입하고, 정부에서 역량 있는 사이버 전문 인재 발견 및 양성 등에 적극적인 국가정책을 마련해야 하고 노력해야 한다.

넷째, 사이버 공격 및 위협에 대한 대응 체계를 보완해야 한다. 사이버테러에 관련하여 책임기관이 필요하다는 많은 연구에도 불구하고 여전히 한국에서는 중앙통제 시스템이 통일된 기관이 존재하지 않고 있다. 국내 기관 중 역량, 경험, 자원 등을 고려했을 때 핵심기관이 국가정보원이 적절하다고 판단하지만, 국가정보원에 신뢰와 권한 통제가 전제되어야 할 것이다. 한국은 5G를 넘어 6G 개발도 통신사에서 실험중이다. 현재 과학기술이 확장되어서 우리는 앞으로 더 다양해질 사이버 공격 및 테러 위협의 심각성을 인식하고 보다 신속하고, 효율적인 사이버 공격에 대한 대응 체계를 구축해 나아가야 한다.

한국의 사이버 공격 및 위협에 대응하는 기관은 국가정보원, 검찰청, 경찰청, 한국인터넷진흥원, 방송통신위원회, 국방부, 국가보안기술연구소 등으로 구성되어 있지만, 수행기관 측면의 대응 현황에서는 국가정보원 내 국가사이버안전센터는 국가 및 공공기관, 국가안보 관련 시설 국가정보의 관련된 사이버 공격 및 위협에 따른 대응업무를 담당하는 기관으로, 국가정보보안업무 기획, 조정 및 계획, 보안정책을 수립하여 국가기관 보안 대책을 지원하며 네트워크 암호기술, 보안시스템 개발 보급, 정보보호 시스템의 인증업무 등을 수행하고 있지만, 정부에서 계속 관심 두고 정보를 공유하며 국가 및 민간기관에 따른 취약사항들을 기관에서 분석하여 보완 및 발전시킬 수 있는 사항으로 변화 해야 한다.

민간, 공공대상으로 정책이 통합된다면 침해 대응 역량이 강화될 수 있는 부분과 사이버 중앙통제 예방, 대응 중심 기능이 집중되면서 기술개발과 인력양성, 산업육성이 집중되어 통합관제, 사이버 사고 조사 등 권한이 분산하지 않고 각 기능에 따른 역할에 집중하여 충분한 사이버 재난본부를 운영할 수 있을 것이라 제안한다. 정보공유와 기반시설 사이버 관리 강화와 기관별로 분산된 사이버보안 대응 영역을 한곳으로 끌어모을 수 있다면 사전에 피해에 대한

대응을 충분히 파악하고 위험에 따른 사이버 공격에 따른 예방을 충분히 할 수 있다. 제안하는 민·관·군 통합 사이버 재난본부 구성방안으로 단일화보다는 통합하는 방안으로 사이버 재난본부 구성 협력관계를 갖춰야 한다. 너무 많은 기관으로 얽혀서 사이버 재난본부를 구성한다면 중앙통제를 하는 처지에서 힘들고 때로는 원활한 통제가 불가하여 대응하기가 힘들 수가 있다. 그래서 조직을 함축하여 더욱 효율적인 중앙통제가 가능하도록 구성을 하며, 민·관·군 협력관계와 사이버 공격위협 시 동맹국들로부터 공조를 받아 사이버 공격에 대응하는 방안을 그림 3.처럼 제시하였다. 최종적인 통합 NSC(국가안보실)에서 국가 정부 공공부문에 걸쳐 사이버 공격에 대한 실제적인 노력을 이끌어가고, 국가 사이버 보안 기술 정책을 적극적으로 민간에서 적용 확대가 되어 기술 및 관리 역량 향상을 지원받아 동등한 역량으로 사이버 공격에 대한 정보수집 하고 기술 발전한 융합으로 인한 시스템들을 민·관·군에 제공하여 통합 운용하는 역할들을 이어간다.

민간에서는 사이버보안, 정보보호 산업육성을 위해 삼성 청년 SW 아카데미교육 프로그램을 참고하여 통신사업자(KT, SKT, LGU+)에서 교육을 진행하여 고등과정(특수목적 고등포함) 또는 대학교에서도 사이버 관련 필수교양과목으로 선정하여 국가지원으로 교육을 반영하여 청년들에게 취업과 연계하여 더욱 미래지향적으로 접근하기 쉽게 반영하는 방안이 있다. 교육과 훈련은 사이버 재난 관리를 위한 사전 교육으로 재난 발생 시 가능성을 줄이고, 복구 시간을 최소화하기 위한 방향으로 더 나아가 공공기관 및 국방 분야 사이버 보안에 대한 특화된 훈련을 연계하여 지속해서 관련 학문이 멈추지 않도록 국가적인 관심과 교육 시행에 정보공유에 무게를 가진다면 민·관·군의 사이버보안 대응 체계의 장점을 살리면서, 사이버보안에 관련된 여러 부처 전문기관 담당 조직에 입장표명을 들어보고 좋은 안으로 설정하되 분명 기관마다 특성화된 인재양성 기준 차이가 있을 것이며 그에 따른 각 기관의 입장을 반영하여 부처 및 학계와 사회에서 연구하는 과정이 필요하다. 관계에서는 국가적인 차원으로 범국가 차원에서 정보보호 전문인력을 양성해 나가야 한다고 제안한다. 보통 관에서는 업체에 위탁을 바탕으로 하는 경우가 있는데 국가 공공기관의 사이버 테러리즘 대응 전문인력 양성을 위해서는 현행 보안업무에 의해 각 기관의 사이버 대응에 대한 업무를 주관하고 있는 담당관을 중심으로 영속적인 교육을 강화해 나가야 한다고 제안한다. 또한, 매년 개최되는 정보보호 및 암호 관련학술 세미나, 정보보호 심포지엄, 화이트해커대회 개최 등을 통해 대국민 인식 제고를 위해서 프로그램을 개발하여 시행하고 언론매체를 통한 적극적인 대외적인 홍보 활동이 필요하다. 그리고 해외 국가에 대한 정보자료 수집 및 제반 사항 등 필요 정보들을 공유 및 소통할 수 있는 외교부 사이버 정보보안팀에서 위와 같은 역할을 통해 조금 더 동맹국들로부터 업무협조를 받을 수 있다.

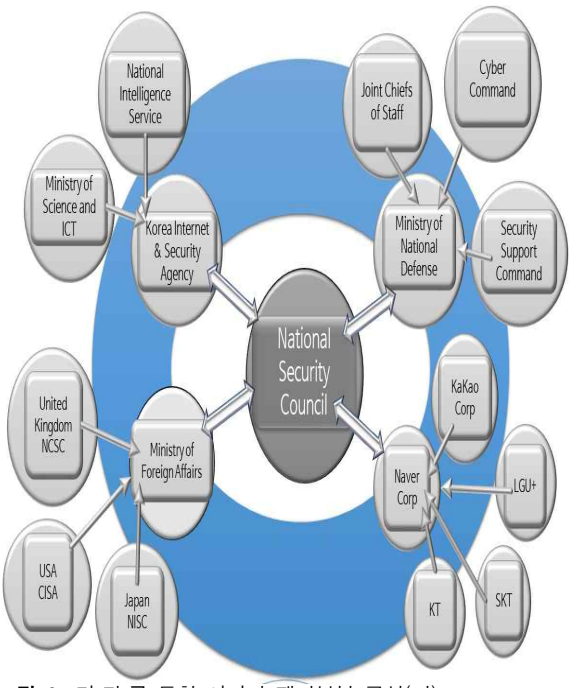

그림 3. 민·관·군 통합 사이버 재난본부 구성(안)
Fig. 3. Formation of the Civil/Public/Military Integrated Cyber Disaster Headquarters (Plan)

민·관·군 통합 사이버 재난본부가 필요한 이유는 먼저 강점으로 운영 통합 및 지식 및 기술 공유 개선 할 수가 있다. 통합 사이버 재난본부는 공공, 민간, 군부대의 자원을 통합한 운영을 촉진한다. 이를 통해 모든 부문과 산업에 걸쳐 사이버 사고에 대응하는 데 필요한 자원을 더욱 쉽게 조정할 수 있다. 나아가 민·관·군의 사이버 전문지식을 취합하여 사이버 방어 체계 강화 방안을 배울 수 있다.

다음으로 위협분석 공유이다. 민·관·군 통합으로 위협정보 수집이 중앙 집중화될 수 있고, 이들 사이에 분석 내용이 빠르게 전파된다. 따라서 영향을 받는 모든 부문이 사이버 위협에 대한 정보를 적시에 전달받음으로 사고에 대한 대응 시간이 단축되고 신속한 조치를 할 수 있게 된다. 어느 조직도 사이버 보안의 상태나 그들이 직면하고 있는 사이버 위협의 전체 범위에 대한 큰 그림을 가지고 있지 않다. 따라서 민·관·군 간 통신선을 정의하면 사이버 지형을 더욱 명확히 파악하고 자원을 효율적으로 동원하며 의사결정에 적합한 사람에게 올바른 정보를 제공할 수 있다.

다음으로 단순화된 의사 결정을 할 수 있다. 민·관·군이 통합되면서 간소화된 단계적 확대와 의사결정 절차를 정의하고 구현할 수 있게 됐다. 다양한 유형의 사이버 공격에 대한 주요 의사 결정권자가 이미 확인되었기 때문에 응답 시간이 빨라져 공격의 영향이 제한될 것이다. 반면에 통합 사이버 재난 본부에 필요한 전문인력이 부족하다. 공격자는 지속해서 변화하는 광범위한 IT 환경을 목표로 하므로 보호가 필요한 기술별로 보안 전문가를 고용해야 하는 과제를

안고 있다. 더욱이, 과제는 필요한 전문인력을 고용하는 것뿐만 아니라 그들이 보호해야 할 진화하는 기술과 공격자들이 사용하는 끊임없이 변화하는 기술에 대한 정기적인 교육을 제공하는 데 있다. 그리고 통합 사이버 재난본부의 적절한 운영모델 선정이 필요하다. 통합 사이버 재난본부 운영에 선택할 수 있는 운영모델은 여러 가지가 있다. 다만 통합 사이버 재난본부 전체 담당자는 물론 보호 대상인 중요 인프라에 대한 책임자를 정하는 것이 과제다. 현재 중요 인프라 관리를 놓고 공공과 민간이 책임져야 할 부분이 겹친다. 민·관·군의 작전 접근에 근본적인 차이가 있다는 점도 고려해야 할 문제다. 민간은 효율적인 운영을 우선시 하는 반면 정부는 프로세스가 길고 대응이 더딘 것으로 알려졌다.

마지막으로 운영의 설정 및 안정화에 필요한 시간 및 자원이 필요하다. 통합 사이버 재난본부는 인력뿐 아니라 기술력, 재원 등에서도 상당한 자원이 필요하다. 또한, 데이터 개인정보 보호와 같은 법적 및 규제 요건을 고려해야 할 수 있다. 관련된 다양한 부문 간의 통합적인 운영을 위해서는 준비 단계부터 운영이 안정화될 때까지 상당한 시간이 필요하다. 통합사이버 재난본부가 실효를 거두려면 세심한 장기계획과 실행이 중요하다. 그런 만큼 통합 사이버 재난본부가 늘어나는 사이버 위협과 공격에 당장 대응해야 할 필요성을 빠르게 해결할 수는 없다. 관련 부문별 정보 공유에 신뢰가 부족하다. 통합 사이버재난본부가 실효성을 가지려면 관련 분야 간 신뢰가 필수이다. 특히 정보 공유의 경우에는 더욱더 그렇다. 그러나 민간 부문은 항상 정부의 간섭을 두려워하여 그들이 공유하는 정보를 제한해 왔다. 반면, 정부는 공공 부문과 군을 통해 국가 안보와 국방 문제에 대한 정보를 공유하려 하지 않을 수 있다.

또한, 고려해야 할 데이터 프라이버시에 대한 국민들의 우려가 증가하고 있다. 모든 관련 당사자가 사이버 운영의 효과를 거두기 위해 필요한 정보 공유와 신뢰 수준을 파악할 필요가 있다.

군에서는 각 해외의 사이버 공격에 대한 정보공유가 필수적이며 국제간 사이버 공격에 관한 정보를 공유하기 위해서 국제해킹사고 대응기구 및 사이버 공격 대응 기관 등과 협력을 강화해 나가야 한다고 제안한다. 군이라는 폐쇄적인 기능을 무시할 수 없지만, 융통성을 가지고 민·관에 국외 해커들에 의한 전산시스템 경유지로 이용하는 사례가 계속 증가하고 있는 해커들을 국내 전산망에 침투하는 것을 차단하고 색출하기 위해서는 국제간의 정보들을 공유하며 더욱더 창의적이고 모의훈련 들을 통해 사이버 재난에 대한 경험적인 측면의 공조가 더욱 넓어져야 한다.

Ⅴ. COVID-19 시대의 제안하는 민·관·군 통합 사이버 재난본부 시나리오

앞서 해외사례 및 선진국의 사이버본부 분석을 바탕으로 그림 4.처럼 구현한 민·관·군 통합 사이버 재난본부 구성안을 가지고 시나리오를 통해 검증한다.

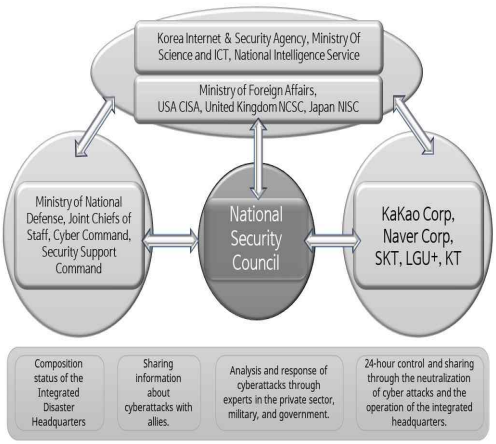

그림 4. 민·관·군 통합 사이버 재난본부 시나리오 체계
Fig. 4. The scenario system of the integrated cyber disaster headquarters between the public, private, and military sectors.

사이버 공격은 계속 급증하며, 공격기법의 양상은 지능화되어 가고 있다. 사이버 공격은 단순 해킹에서 금전적인 목적으로 진화하였으며, 정보통신망에 대한 사이버 공격은 최악의 경우 금융, 의료, 교통 등의 국가 전체를 마비시켜 위기를 초래할 수 있다. 이에 따른 대안으로는 그림 4.처럼 NSC (국가안보실)가 중심이 되어, 민·관·군 통합 사이버 재난본부 구성을 운영한다. 적절한 민간기업들과 함께 협조적·지속해서 협력하고 사이버위협으로부터 정보공유를 위해 기술 중립적으로 접근하며, 사이버 모의훈련이 잘되어 있는 군의 조직을 활용하여 사이버 공격에 대응한다.

전산장비의 부속품 제조 과정 중에 컴퓨터 마우스, 키보드 등의 장치 속에 아주 작은 칩 형태로 숨겨있다가 군부대 및 국가 공공기업 전력망 관제센터로 물건이 납품되었다. 이때 해커는 10Km 이상 떨어진 곳에서 원격으로 컴퓨터 부속품에 심어둔 백도어 칩을 이용하여 무선신호를 사용해서 침투를 시도한다.

군부대, 국가기관이나 금융기관의 전력망들이 마비가 되어버리고, 국가비상사태가 가동되어 인포콘 3단계 발령이 되어 민·관·군을 총체적으로 통제하는 국가안보실에서 민·관·군에 정보보호 대응태세를 격상한다. 24시간 공간과 시간에 제약 없이 동맹국과 현재 상황들을 외교부 측에서는 정보 공유를 하며, 비슷한 유형의 사이버 공격이 있었는지 확인하고 사이버 전문인력들을 양산한 민간기업에 공유하도록 한다.

민간기업에서도 격상한 상황에 따라 관련 전문담당자들을 위기조치반을 소집한다. 현황에 따른 업무를 총괄적으로 국가 중요기반시설 보호, 각종 사이버 공격 및 위협에 대응하고 민간 측면에서 각급 기관과 민간의 사이버 위협으로부터 정보를 통합하고 분석을 시도하고 있으며 그에 따른 영향을 국가안보실에 기술지원 및 상황보고를 한다.

국가정보국의 군에서는 사이버위협, 사고의 종합적분석, 그리고 유관 및 민간기관과 정보를 국가안보실에 공유하는 역할을 한다. 외교부 기관에서 해외 사이버 동맹국들의 전문 인력팀들과 지속적인 연락 반을 통해 일어난 상황에 대해 정보공유 및 조언을 지속해서 정보를 취합하며 전자정부 정보기술, 연방 기관의 사이버보안 감독 등의 연방 정부의 정보시스템 보호 역할을 국가안보실에 공유한다. 위 경우는 최대한 유관기관 및 민간기관의 종합적 네트워크 정보 분석을 통해 정보공유를 하며 국가안보실에서는 통합적으로 상황 보고를 받고 사이버 공격에 대한 분산적인 지휘를 통해 사이버 공격에 따른 대응을 한다.

Ⅵ. 결 론

국가 및 사회 전반의 디지털 의존도가 높아진 지금 국내 사이버 공격 및 위협으로 피해당한 금액이 2015년 기준으로 2021년 상반기까지 약 6조8천억 원에 달한다. 현재 COVID-19 이후 업무 패러다임 전환에 따른 네트워크 용량 증가와 장거리 회선통합으로 재정지출 효율화를 이루기 위해 기획재정부에서 안을 제시하여 국가 융합망 회선통합 사업이 진행되고 있다. 국가기관 통신망이 단일 통신사에 의존 및 이원화 구성 부족으로 통신사업자 재난 발생 시 국가기관 서비스 중단 우려로 인한 재난은 불확실하며, 복잡하고 익숙해지지 않기 때문에 이를 관리하는 것은 어려운 일이다. 또한, 기존 기관 간 통신회선 중복구간 통합(집선)으로 예산 감축을 위해 회선을 관리한다면 사이버보안에는 더욱 취약할 수밖에 없다. 현재 국가에서 사이버보안 대응 체계상으로 과학기술정보통신부, 국가정보원, 국방부 영역을 분담하고 협력을 지휘하는 명목상 중앙통제는 국가안보실이 있지만 충분한 전문 인력들이 있지 않다. 사이버 보안 분야의 전문성과 연구개발, 인재양성 기능, 사이버 공격에 대한 민간과 공동으로 훈련과 대응을 함으로써 우리는 사이버 재난관리를 하기 위해서는 정형화된 매뉴얼, 체계의 구축과 함께 상황 적응성 향상이 필요하다. 그러나 정형화된 매뉴얼 체계까지 포괄적으로 재난을 관리할 수 있을 때 상황 적응 향상 역시 이루어질 수 있다. 이에 국내 재난관리 체계의 올바른 방향을 제시하기 위해 필요한 정책적 제안들에 대한 연구는 물론 이 체계의 효율적인 운영을 위한 연구도 필요하다.

국가 사이버안보 수행체계 측면에서, 미국은 바이든 행정부 출범 이후 대통령 직속 국가 사이버실을 신설하여 국가안보 차원에서 사이버 공격 대응 태세를 갖추고 있다고 평가할 수 있다. 사이버 공격에 관하여 심각성과 중요성을 인식하고 국가전략 차원에서 대응 체계를 갖추기 위해 부단히 노력하고, 주요 선진국의 수준과 비슷한 대응 체계를 갖추려고 하는 목적이 필요하다. 사이버 공격에 대비한 공격적, 방어적 대응 체계는 다소 미흡하다. 사이버 공격이 국가안보의 위협으로 다가온 만큼 국가안전을 보장하기 위해 더욱 큰 틀의 국가전략을 구성할 필요가 있다. 미국의 사이버 테러 대응 임무 수행 체계는 비교적 업무 구분이 명확하고 담당 기관 별로 임무 영역이 명확하게 구분되어 있는지를 확인해서 부처들의 기능을 세분되어 통합해야 하는지를 검토해 볼 필요가 있다. 특히 대부분의 정부 부처와 기관의 보안부서와 정보화 부서가 분리되어 있는데 이를 통합운용하여 정책적으로 검토할 필요가 있으며 더는 제도적인 측면에서 늦어서도 안 될뿐더러 통합 사이버 재난본부 기능을 각 기관에 분산시키지 않고 하나로 결집해서 사이버 공격 및 위협에 대응하면서 사이버보안 기본법에 민·관·군 협력체계 강화, 주요정보통신기반 시설 관리강화와 사이버 공격에 따른 대응 대책본부 구성 부분이 최소한 법에 통과되어 향후 사이버안보 방위 훈련과 민·관·군 합동대응체계 공유를 통해 신속하고 효율적 대응을 위한 국제적 협력관계를 우리나라가 주도하며 글로벌 사이버안보 의사결정에 대한 영향력 강화로 국제적으로도 위상을 제고한다. 사이버 공격에 대한 중재자로서 국제협력을 확대하고, 사이버 공격 대응에 취약한 국가들에 대한 사이버 공격 개발원조를 시행한다. 사이버 공격에 대한 후발국들을 견인하고 사이버보안 국제규범화에도 기여할 수 있다. 사이버보안은 기술의 우위에 따라 많이 좌우된다는 특성이 있고 후발국에는 기술적, 물적 지원들이 필요하다. 네트워크로 연결된 상태에서 안보 수준이 취약한 국가들에 일정 수준 기술과 물적 수준들을 유지해주며, 정보통신기술 선도국가로 부응 할 수 있을 것이다.

앞으로 연구·개발 향상, 사이버 전문인력 개발 및 교육, 국민 인식 제고와 지속적인 사이버 공격에 대한 대내적인 홍보활동을 하며, 통과하지 못한 사이버보안 법제화 문제들이 통과되어 법으로부터 자율적인 민·관·군 협력으로부터 사이버 위협에 대응하도록 국가에서의 적극적인 개입이 필요하다.

민·관·군 통합 사이버 재난본부 구성은 사이버 공격으로부터 준비된 본부의 통합대응으로 인명과 피해를 방지하기 위함이다. 현장의 목소리와 선진적인 사이버 재난 본부 구성안을 마련하기 위한 대한민국 정부의 발 빠른 대처가 요구된다.

참고문헌

[1] In addition to the NIS, "Information Security White Paper 2021" (Korean), p. 218. 2021

[2] Petak, William J., "Emergency Management: A Challenge for Public Administraton," Public Administrative Review, vol.45, Special Issue, pp.3-5, Jan. 1985. https://doi.org/10.2307/3134992

[3] Chung, Min Kyung, Lim, Jong-in, and Kwon, Hun-Yeong, “A Study on North Korea’s Cyber Attacks and Countermeasures,” Journal of Information Technology

Services, vol. 15, no. 1, pp. 67–79, Mar. 2016.
doi: 10.9716/KITS.2016.15.1.067
[4] Shin Su-Jeong, Jung Hyunchul, Myungho, Hong Seokbeom, Choi Woohyung, Lee Hyun-woo, Lee Sanggyu., Park Young Gil, Private Cyber Safety Manual, pp. 33, Dec 2005. https://doi.org/10.9716/KITS.2016.15.1.067
[5] "Cyber Security(National, Public) Disaster Countermeasure Manual," NIS, 2009. (in Korean) https://scienceon.kisti.re.kr/commons/util/originalView.do?cn=JAKO201011949344297&oCn=JAKO201011949344297&dbt=JAKO&journal=NJOU00291533
[6] Global Cybersecurity Index 2020 [Internet]. Available: https://www.itu,int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
[7] CTIIC [Internet]. Available: https://www.dni.gov/index.php/ctiic-who-we-are
[8] CISA [Internet]. Available: https://www.cisa.gov/about-cisa
[9] NSA [Internet]. Available: https://www.nsa.gov/about/
[10] NSC [Internet]. Available: https://www.whitehouse.gov/nsc/
[11] DoJ [Internet]. Available: https://www.justice.gov/about
[12] DoC [Internet]. Available: https://www.commerce.gov/about
[13] NIST [Internet]. Available: https://www.nist.gov/cyberframework
[14] CISCP [Internet]. Available: https://www.cisa.gov/ciscp
[15] W. Baek, "A Study of Efficient Disaster Management System," A Master's Thesis, KangwonUniversity, pp.21-27, Feb. 2009. (in Korean)
[16] NCSC [Internet]. Available: https://www.ncsc.gov.uk/section/about-ncsc/what-we-do
[17] GCHQ [Internet]. Available: https://www.gchq.gov.uk/section/mission/overview
[18] CESG [Internet]. Available: https://www.gov.uk/government/organisations/cesg
[19] CPNI [Internet]. Available: https://www.cpni.gov.uk/about-cpni
[20] Cybersecurity Strategic Headquarters [Internet]. Available: https://www.nisc.go.jp/eng/index.html#sec1
[21] NISC [Internet]. Available: https://www.nisc.go.jp/eng/index.html#sec1
[22] Responsible researcher: Lee Changjoo, Co-researcher: Jang Geon-tae, Son Hee-seop, Report on the leakage of high-tech industrial secrets through cyberattacks and countermeasures, Korean Policy Society, pp. 45, Dec. 2019.https://intelligence.na.go.kr

손태식(Tae-Shik Shon)

2005년 : 고려대학교 박사
現) 아주대학교 교수
現) 국가정보원 정보보안 실태 평가위원, 한국전력 정보보안 자문위원, 디지털 포렌식 표준화 포럼 자문위원, 원전 사이버보안 워킹그룹 위원, CC인증위원회 위원, 스마트그리드 핵심 보안기술 자문위원, 한국정보보호학회 이사, 한국정보처리학회 이사, 한국디지털포렌식학회 이사 Associate Editor(Seurity and Communication Networks, Wiley) Associate Editor(J.of Parallel, Emergent and Distributed Systems,Taylor and Francis)
2005년~2011년: 삼성전자 통신연구소/DMC연구소 책임연구원
2004년~2005년: University of Minnesota Research Scholar
※관심분야 : Digital Forensics, Vehicle Security, ICS

백인정(In-Jeong Baek)

2007년~2011년: 육군3사관학교
2019년~현 재: 아주대 정보통신대학원 사이버보안과
2011년~2021년: 대한민국 육군 정보통신 장교
2021년~현 재: 행정안전부 국가정보자원관리원 국가융합망 구축실무추진단
※관심분야 : 정보보호(Personal Information), AI, 디지털포렌식, 유비쿼터스 컴퓨팅(AR)