정보기관의 사이버안보 역할 정립에 관한 연구
-사이버안보관련 법안 제·개정안을 중심으로-

윤오준*, 김소정**, 정준현***

요 약

제4차 산업혁명 시대가 진전되어 정보통신기술이 획기적으로 발전하면서 사이버위협은 점점 더 지능적이고 고도화될 것이다. 그렇기 때문에 그 위협에 대한 대비책을 마련하면서 사고가 발생할 경우에도 체계적이고 신속한 조치를 취하기 위해서는 정보기관의 역할이 중요하다고 할 것이다. 그러나 우리나라는 이와 관련된 '국가사이버안보법안' 제정이나 「국가정보원법」 개정에 대한 논의가 지지부진하여 사이버위협을 대응하는데 어려움이 있는 실정이다. 이에 본 논문에서는 현행 법 체계상 정보기관의 사이버안보 기능, 최근의 법 제·개정 논의 동향과 우리 실정에 맞는 정보기관의 역할에 대한 시사점을 살펴본 후 향후 사이버안보 수행체계 보강을 위한 정보기관의 역할 정립 방안으로 사이버안보에 관한 첩보수집·분석 집중, 사이버위협 예측·대응역량 제고, 법과 원칙 준수를 위한 법적 토대 구축 등을 제시하고자 한다.

A Study on establishing the Role of Intelligence Agency on Cybersecurity
- Focusing on Revision or Enactment of Cybersecurity related Bill -

Yoon Oh Jun*, Kim So Jeong**, Jeong Jun Hyeon***

ABSTRACT

As the era of the 4th Industrial Revolution has progressed and the information and communication technologies have developed dramatically, the cyber threats will gradually become more intelligent and sophisticated. Therefore, in order to take systematic and prompt action in case of an accident while preparing measures against the threat, the role of intelligence agency is important. However, Korea is having difficulty in responding to the threats due to the lack of support for the national cybersecurity bill or the amendment bill of the National Intelligence Service. In this paper, I examine the cybersecurity function of the intelligence agency, the recent debate trends, and implications for the role of intelligence agency in our current situation. And then I intend to suggest some measures such as concentration on information gathering and analysis, enhancement of cyber threat prediction and response capacity, and strengthening of legal basis as a way to establish the role of intelligence agency for reinforcement of cybersecurity performance system.

Key words : Cybersecurity, Cyber threat, Intelligence Agency, Cybersecurity Bill

접수일(2018년 9월 27일), 수정일(1차: 2018년 10월 23일), 게재확정일(2018년 10월 30일)

* 단국대학교 대학원 법학과
** 국가보안기술연구소
*** 단국대학교 법과대학 법학과

1. 서 론

사이버공간이 경제·사회·문화 등 국민들의 생활 영역으로 확산됨은 물론 정치·국방·행정 등 국가 모든 분야의 안보요소로 확대됨에 따라 대부분의 부처들이 사이버안보 수호를 주요 업무로 인식하고 소관분야 정책을 수립하여 시행하고 있고, 또한 해외 많은 나라의 정부기관들도 사이버안보를 중요 어젠더로 설정하고 향후 구비해야 할 필수적이고 핵심적인 역량으로 간주하여 대비해 나가고 있다. 무엇보다도 사이버안보 위협에 대해 능동적으로 대응하기 위해서는 국내외 사이버공간을 초월하여 발생하는 사이버위협의 특성상 그 위협 주체에 대한 해외 정보기관들과의 정보협력을 통한 첩보수집과 공동대응이 우선되어야 하며 이와 더불어 국내 공공 및 주요기관을 대상으로 하는 사이버공격에 대한 정보수집과 분석, 보안취약점 발굴·개선, 해킹사고 원인분석, 재발 방지를 위한 정책정보 생산·배포 등이 필요하다.

이러한 환경에서 정부 내 또는 국회의 여야당에서 관계부처들의 사이버안보 역할에 대한 논의가 진행되고 있다. 몇몇 시민단체에서는 정보기관의 역할에 대한 일부 부정적인 의견을 제시하는 등 정보기관이 주관하는 것에 대한 이견을 표출하고 있기도 하지만, 다른 한편으로는 정부부처 내부는 물론 여야 정치권 등 많은 기관과 인사들이 사이버안보에 대한 정보기관의 독보적인 역할을 인정하고 있으며, 일부는 그간의 주도적 기능을 시대 환경에 맞게 분산 또는 타 기관과 협업하여 공동으로 수행토록 해야 한다는 건설적인 의견을 개진하기도 한다.

앞으로 제4차 산업혁명 시대가 진전되어 정보통신기술이 획기적으로 발전하면서 사이버위협은 점점 더 지능적이고 고도화될 것이다. 그렇기 때문에 '국가사이버안보법안'이나 「국가정보원법」 개정안 등 사이버안보관련 법안의 정비를 통해 사이버위협에 대한 대비책을 마련하는 한편, 사고가 발생할 경우에도 체계적이고 신속한 대응조치를 취하기 위한 유관기관 간의 역할 정립이 중요하다 할 것이다.

이에 본 논문에서는 현행 법 체계상 정보기관에 대한 사이버안보 기능 및 수행업무, 최근 법 제·개정 논의 동향, 우리 실정에 맞는 정보기관의 역할에 대한 시사점을 살펴보고 향후 역할 정립 방안을 제시함으로써 글로벌 사이버위협으로부터 국가안보 수호, 국민안전 및 국익 보호를 위한 법적 토대를 구축하는데 일조하고자 한다.

2. 관련 연구

2.1 법령 체계상 정보기관의 기능

국가정보기구는 법에 근거하여 국가안보를 위하여 정보를 수집하고 이를 분석하여 필요한 정보를 생산하는 특별한 활동을 하는 정부조직을 말한다[1]. 우리나라는 「정부조직법」 제17조에서 대통령의 소속으로 국가정보원을 설치하도록 규정하고 있고, 「국가정보원법」은 제1조에서 국가정보원의 조직, 직무범위와 국가안보 업무의 효율적 수행을 위하여 필요한 사항을 규정하는 것이 법의 목적이라고 하고 있다.

국정원법 직무조항은 1960년대의 정보환경에서 규정된 이후 정보통신기술의 획기적 발전에도 불구하고 여야의 정치적 이해득실 계산으로 큰 틀의 개정 없이 유지되어 온 나머지 사이버공간이라는 새로운 안보환경에 부응하지 못하고 있는 실정이다. 이로 말미암아 실제 수행하고 있는 사이버안보와 관련된 정보에 대한 수집, 작성, 배포 기능과 국가 정보통신망에 대한 사이버보안 업무가 직무에 제대로 반영이 되지 않아 법치주의에 미흡하다는 지적이 많으며, 국가적인 측면에서도 국회 및 정부가 국가 최고의 정보기관을 순수한 안보수호 기관으로서 사이버안보 역량 강화를 위한 선진화와 전문화 노력에 소홀했다는 비판도 받아왔다. 미국 CIA 및 영국 GCHQ 등 세계 최고의 정보기관들이 중장기적인 미래업무를 준비하면서 사이버요소를 중요한 과제로 설정하고 있다는 것은 우리에게 시사하는 바가 크다 하겠다. 따라서, 우리나라의 정보기관도 본연의 순수한 안보기관으로서의 역할 강화를 위해서는 사이버안보를 직무범위에 명확하게 명시하여 규정할 필요가 있다고 할 것이다.

사이버안보와 관련한 법령으로는 「국가정보원법」, 「전자정부법」, 「정보통신기반보호법」 등이 있으며, 그 외 「국가사이버안전관리규정」, 「국가위기관리기본지침」 등 대통령훈령이 있다.

「국가정보원법」 제3조 직무조항에서 국외정보의 수집·작성 및 배포, 국가 기밀에 속하는 문서·자재·시설 및 지역에 대한 보안 업무, 정보 및 보안 업무의 기획·조정 업무를 수행토록 하고 있으며, 「전자정부법」 제56조(정보통신망 등의 보안대책 수립, 시행)제3항, 동법 시행령 제69조, 제70조 등에서는 국정원으로 하여금 행정기관의 정보통신망을 이용한 전자문서 보관, 유통 관련 보안조치 및 이행여부를 확인토록 하고 있고, 이와 유사하게 「공공기록물 관리에 관한 법률 시행령」 제5조(전자기록물의 보안관리)에 의거, 공공기관 전자기록물의 생산, 이관, 보존, 폐기 등 관리과정에서 보안조치 및 이행여부도 확인토록 하고 있다. 또한 「정보통신기반보호법」 및 동법 시행령에는 국정원으로 하여금 공공분야 정보통신기반보호실무위원회 운영(법 제3조제4항, 시행령 제5조), 공공분야 주요정보통신기반시설 지정 권고, 보호계획의 수립, 보호대책 이행여부의 확인(법 제5조의2, 제6조, 제7조, 제8조의2 및 시행령 제9조의2), 국가안보 관련 주요정보통신기반시설에 대한 직권에 의한 보호지원(법 제7조제2항) 등 공공분야의 기반시설 보호를 주관하도록 규정하고 있다.

2005년1월 제정된 「국가사이버안전관리규정」(대통령훈령)상의 국정원 역할로는 국가사이버안전 관련 정책 및 관리에 대한 총괄·조정, 사이버안전대책의 수립 지원, 민·관·군 합동대응팀 운영, 사이버위기 대응훈련, 보안관제센터의 설치·운영, 공공분야 사이버위기 경보 발령, 사고조사 및 처리 등을 규정하고 있다. 이울러 2003년 1.25 인터넷 대란을 계기로 국가차원의 사이버공격에 대한 종합적이고 체계적인 예방 및 대응을 위하여 2004년2월에 국가사이버안전센터(NCSC)를 설치하고 법령 및 규정·지침에 의거하여 사이버안보 업무를 수행하고 있다. 또한 사이버위협에 관한 정보공유를 활성화하고 공조체계를 강화하기 위해 국가사이버안전센터 내에 민·관·군 유관기관이 참여하는 '합동대응팀'을 운영하면서 상황판단, 정보공유, 합동분석·조사 등 분야별 업무를 협업하며 수행하고 있다[2].

한편, 2009년 이후 대규모의 사이버공격에 체계적으로 대응하기 위한 정부차원의 종합대책에서도 정보기관의 역할을 찾아볼 수 있다. 모든 종합대책을 정보기관이 주관하여 작성하고 대통령에게 보고하고 시행하였는데, 이는 사이버안보 총괄기관으로서 정보기관의 역할을 반증하고 있다고 할 수 있다. 종합대책상 정보기관의 역할로는 2011년의 「국가 사이버안보 마스터플랜」에는 민·관·군 사이버위협 합동대응팀 구축·운영, 업무망·인터넷망 분리 및 외주업체 보안관리 강화 내용이 포함되어 있고, 2013년의 「국가 사이버안보 종합대책」에는 사이버위기가 발생할 경우 청와대와 정보기관에 관련 상황을 동시에 전파하고, '주의'단계 이상의 경보 발령 시 범정부 차원의 사이버위기 대책본부를 운영할 수 있도록 하였으며, 2015년 「국가 사이버안보 태세 강화 종합대책」에는 주요정보통신 기반시설 지정 확대 및 보호대책 강화, 사이버테러방지법 제정 등 법령 정비가 포함되어 있다[3].

이외에도, 관계부처 합동으로 작성, 배포하는 「국가정보보호 백서」에 따르면, 정보기관이 국가·공공기관 대상 정보보안 관리실태 평가, 정보통신망 안전측정, 국가·공공기관이 도입하는 정보보호시스템 등에 대한 보안적합성 검증, 암호모듈 검증 등 사이버보안 업무를 직접 수행하고 있는 것으로 보인다[4].

또한, 2017년7월 국정기획자문위가 발표한 <문재인정부 국정운영 5개년 계획>의 국가 사이버안보 대응역량 강화 실천과제를 정보기관이 주관키로 한 바 있고[5], 2017년4월 더불어민주당의 <19대 대선 정책공약집-나라를 나라답게>에는 '테러 및 사이버 보안업무와 관련해 정보기관이 권한을 남용하거나 인권침해 행위를 하지 않도록 국회 통제장치 강화'를 제시하고 있는데[6], 이는 원천적으로 정보기관으로 하여금 사이버보안 업무를 수행토록 인정하는 것을 의미하면서도 우려되는 권한 남용이나 인권침해를 차단하기 위한 조치를 하겠다는 의지를 표명한 것으로 보인다.

2.2 사이버안보 법제 최근 논의 동향

2.2.1 사이버안보 관련 법안

사이버안보 관련 법안은 2006년 이후 정보기관 중심으로 '사이버위기대응법안'을 정부법안으로 발의를 추진하였으나 일부 부처의 반대로 무산된 바 있으며, 공성진 前의원이 사이버위기 예방과 대응관련 개별 법안들을 국회에 제출하기 시작하였다.

또한, 2016년5월30일 이철우 의원이 대표 발의한 「국가사이버안보에 관한 법률안」이나 2017년1월 정부가 국회에 제출한 「국가사이버안보법안」에서 정보기관의 역할을 확인할 수 있는데, 그 내용은 대동소이하다고 할 수 있으나 정부안의 경우 정보기관의 권한남용이나 국민의 사생활 침해 우려 등 그간의 일부 시민단체에서 제기한 내용들을 정부 협의과정에서 반영하여 정보기관의 주도적 역할을 합리적으로 조정하고 기관 간에도 기능을 분장함으로써 다소 완화된 것이 특징이라 할 수 있다. 두 개의 법안에서 정보기관의 주요 역할로는 사이버안보 기본계획 수립·시행, 실태평가, 사이버위협 정보공유센터 운영, 사고조사, 경보 발령 등이며, 현재 국가·공공기관을 대상으로 수행하고 있는 정보기관의 업무 대부분이 그대로 법안에 반영되어 있다고 할 수 있다. 다만 정부안의 경우 민간분야인 정보통신서비스 기업과 전자금융기반시설 운영기관을 법 적용대상에서 제외하였으며, 정보기관의 국가사이버안보센터 설치도 삭제하였다. 안보위협 사이버공격에 대한 사고조사 시 민간분야의 경우 정보기관이 단독으로 조사토록 허용하는 것이 아니라 관계 중앙행정기관, 수사기관 등이 합동으로 조사팀을 운영토록 하고 있으며, 아울러 사이버안보 강화를 위하여 처리되는 개인정보에 대하여 「개인정보보호법」의 예외를 인정하면서도 일반 국민의 기본권이 침해되지 않도록 필요한 법적 보호조치와 절차를 명시하였다[7][8].

2.2.2 국회의 사이버안보법안 검토보고서[10]

국회 정보위 수석전문위원(임진대)은 '국가사이버안보법안' 검토보고서에서 시민단체(민주사회를 위한 변호사모임, 민주주의법학연구회, 인권운동사랑방, 진보네트워크센터, 참여연대, 천주교인권위원회)에서는 제정 법안이 대통령훈령인 「국가사이버안전관리규정」에 있는 정보기관의 권한을 법적으로 보장하는 것으로, 이는 「국정원법」에 규정된 직무범위를 벗어난 것이고, 민간의 정보통신망까지 정보기관의 권한을 확대하여 민간에 대한 국가감시가 확대되고, 실질적으로 정보기관이 컨트롤타워의 역할을 하는 등 권한 강화로 관련 기관에 부당한 영향력을 행사할 수 있다고 하였다[9][10]. 또한, 사이버안보를 명분으로 「개인정보보호법」의 적용 예외를 받아 특정이용자를 감시 사찰할 수 있는 위험성이 크고, 비밀정보기관에게 사이버보안의 컨트롤타워 역할을 맡기는 나라는 없으므로 사이버보안 관련 기존의 정보기관의 권한도 다른 행정기관으로 이양해야 한다는 반대의견을 유지하고 있다고 하였다[9][10]. 동 검토 내용은 2017년2월14일 위 6개 시민단체가 국회 정보위 사무처에 제출한 '국가사이버안보법 국회 발의안에 대한 의견서'를 바탕으로 작성되었다[10].

또한 검토보고서는 정부안 제7조제6항에서 대통령령으로 정하는 바에 따라 국정원장과 관계 중앙행정기관 합동으로 지원기관의 기술적 지원 실태를 점검할 수 있는 권한을 부여하고 있는데, 그 이유는 지원에 필요한 충분한 기술을 갖추도록 하여 국가적 사이버위기 시 신속히 대비하기 위한 것이라고 보이나, 지원기관들은 이 규정에 따라 점검을 받을 의무가 생긴다고 할 수 있기 때문에 정보기관이 민간에 대한 통제력을 강화하려는 수단으로 보일 여지가 생긴다고 하였다[10].

아울러, 사고조사의 통보 및 조사에 있어서도 국가안보위협 사이버공격에 관한 사항은 정보기관에게 통보하도록 하고 있는데, 어떤 사이버공격이 국가안보위협에 포섭되는지 여부에 대하여 분류하기 어려울 수 있기 때문에 모든 사고를 대상으로 할 것이 아니라 대통령령에서 정하는 경미한 사고는 통보대상에서 제외하도록 하는 방안을 강구할 필요가 있다고 하였다[10]. 또한 상급책임기관의 사고통보를 받은 경우 모든 사고에 대해 정보기관이 조사하도록 하고 있는데, 경미한 사고의 경우 정보기관의 조사가 필요하지 않을 수도 있는데도 불구하고 정보기관이 모든 경우에 조사하도록 하는 것은 지나칠 수 있으므로 국가안보위협 사이버공격에 대해서만 정보기관이 조사하도록 하는 방안을 검토할 필요가 있다고 하였다[10].

2.2.3 「국가정보원법」 개정 법안

사이버안보 관련 사항을 「국가정보원법」 개정안에 반영하기 위한 노력들도 전개되었다. 국회의 의안정보시스템에서 의안을 검색한 결과, 2008년11월6일에 이철우 의원과 2009년2월24일에 박영선 의원이 각각 대표 발의한 「국정원법」 개정안에 기존의 국가

기밀에 대한 보안업무와 더불어 '국가정보통신망에 대한 사이버안전업무'를 최초로 추가시킨 사례가 있으며, 이후 여야 공히 국정원의 사이버안보 업무에 대해 공감대를 형성한 것으로 보이나 정치적인 역학관계로 법안이 제대로 처리되지 못하였다.

최근 정보기관의 개혁 일환으로 현재 국회에 제출된 「국가정보원법」 개정 법률안은 5개로 파악되고 있는데, 2017년6월27일 발의된 진선미 의원안, 2017년7월5일 발의된 천정배 의원안, 2018년1월8일 발의된 박홍근 의원안, 2018년1월15일 발의된 김병기 의원안, 2018년3월23일 발의된 이완영 의원안이 있다. 이들 법률안은 현행 국가정보원의 명칭 변경부터 그 직무와 권한, 통제방법, 처벌규정 등을 신설하거나 폐지하는 내용을 주로 담고 있는데, 진선미, 천정배 의원안은 국가기밀에 대한 보안업무는 유지하면서도 정보 및 보안업무의 기획·조정 직무는 삭제하였으며, 박홍근 의원안은 제3조 직무조항에서 국가안전보장과 관련된 정보의 수집·작성 및 배포 범위에 '사이버안보'를 추가하고 또한 국가기밀에 대한 보안업무와 더불어 '국가정보통신망에 대한 사이버안보업무'를 병기하였다. 김병기 의원안은 사이버안보와 관련하여 직무 조항에서 '국가안보와 직접적으로 연계된 국가·공공기관 대상 사이버공격에 대한 예방 및 대응' 업무를 신설하였고, 이완영 의원안은 '국가기관, 지방자치단체, 그 밖의 공공기관 및 그 소속기관에 대한 사이버공격의 예방 및 대응' 업무를 추가한 것이 주목할 만하다.

한편, 2017년11월29일 국정원이 국회 정보위에 보고한 「국가정보원법」 개정안에 대한 언론의 보도를 종합해보면, 그 직무범위 중 '사이버공격 예방'을 추가하였는데[11], 그 이유로 전자통신망 또는 사이버공간은 과거 개인 간의 단순한 연락수단 및 정보수집 수단으로 활용되던 것에서 그치지 않고 행정작용·경제질서 등 국가 운영시스템 전반에 걸친 영역으로 확대됨에 따라 사이버안보가 전 세계 정보기관의 필수역량으로 대두되고 있는 상황이라고 하면서 이에 따라 북한 및 해외의 사이버위협에 대응하기 위해서는 해외 첩보수집과 함께 북한과 연계된 국내에서의 사이버공격 관련 정보를 수집하는 한편, 그 취약점 분석 및 평가와 재발방지를 위한 정책수립 등이 필요하다는 고려 하에 동 직무를 신설하게 되었다고 한다. 결론적으로, 사이버안보 업무를 추가한 것은 급변하는 정보환경에서 사이버안보 수호에 대한 국가정보기관의 강력한 의지를 표명한 것으로 보인다.

2.2.4 국회 정보위 주관 공청회[12]

2018년1월31일 국회 제3회의장에서 개최된 국정원 개혁에 대한 공청회에서 석재왕 건국대 안보재난관리학과 교수는 정보환경의 변화를 반영, 국가차원의 정보활동 수행을 위한 제도적 장치가 구축되었다고 설명하면서 사이버정보활동을 명기한 것은 정보화시대 상당수 유가치 첩보는 사이버공간에서 입수되고 있는 실정임을 고려해볼 때 정보활동의 역량을 강화하는 조치라고 평가하였다[12].

허태회 국가정보학회장은 각 개정안에서 제시된 직무범위의 명확화 및 구체화와 관련하여 언급하면서 사이버공격에 대한 예방 및 대응의 내용을 포함시킨 것에 대하여 김병기 의원안의 '국가안보와 직접적으로 연계된 국가·공공기관 대상 사이버공격에 대한 예방 및 대응'과 국정원안의 '국가·공공기관 대상 사이버공격에 대한 예방 및 대응'의 내용을 직무범위에 명확하게 한 것은 바람직한 것으로 보인다고 하였다[12]. 특히, IT 강국이지만 역설적으로 사이버공간의 보호에 취약한 우리나라로서는 ATP 공격 등 갈수록 첨예해지고 고도화되고 있는 북한 및 외부 적대세력의 사이버공격에 능동적이고 예방적인 대응활동을 펼쳐나가야 하겠으며 그런 차원에서 사이버안보를 직무범위로 명확하게 규정하는 것은 적절한 것으로 보인다고 하였다[12]. 다만, 미국 정보기구의 경우 사이버 역량을 중심축으로 정보수집 파트와 정보분석 파트의 업무기반과 조직편제를 혁신시켜 나가고 있는 바, 사이버안보 문제에 대한 전향적인 인식과 태도가 중요한데 일각에서 과거의 사이버댓글 활동과 사이버안보 활동을 헷갈려서 사이버안보 강화를 오해하는 것은 유감스러운 일이라고 하였다[12].

2.3 정보기관의 역할에 대한 시사점

사이버위협과 관련한 정보공유와 대응에 있어 정보기관의 역할도 국가 기능의 변화 경로를 따라 진화해 왔는데, 사이버위협을 정보보안 또는 사이버보안의 시각에서 수동적인 침입탐지와 방어 위주로 대응해오던

시기에 정보기관의 역할은 그리 크지 않았을 수도 있었다. 그러나 사이버공격으로 인해 국가기밀이 유출되고, 주요 정보통신 기반시설이 마비되며, 기업의 금전이 탈취되는 등 심각한 결과가 초래되면서 세계 각국은 사이버위협 탐지와 차단, 대응은 물론 이를 위한 정보공유 활성화 등 법과 제도를 정비하면서 정보기관들의 역할도 증대되어 왔다고 할 수 있다.

사이버안보 분야에서 미・영 등 정보기관들의 웹사이트를 검색하면 기관들의 사이버안보 역할이나 대외활동들을 찾아보는 것이 쉽지 않는데, 이는 아마도 정보기관의 비밀성, 비노출성 등 기본 속성상 정보기관이 실제로 사이버안보 역할을 충실히 하고 있는 경우에도 이를 공식화하거나 공개하는 것은 어렵기 때문일 것이다. 그렇다고 해서 일반적으로 사이버 세상과 물리적 공간이 구분되는 것이 어려울 정도로 물리적 공간에서의 활동이 사이버 상에도 동시에 일어나고 있다는 점에서 보면 정보기관이 사이버 상에서의 사이버안보를 위협하는 정보에 대한 수집, 분석을 하지 않고 있다고 단언하기는 어렵다고 할 것이다. 그리고 이러한 사이버상의 위협정보가 대통령, 총리 등 최고정책결정자에게 보고되고 주요 정부부처에도 제공되어 공유될 것이라는 점은 충분히 짐작할 수 있다.

우리나라는 1960년대 이후 정보기관이 국가차원의 사이버보안 정책을 수립하여 정부부처, 공공기관 중심으로 지원하면서 각종 사이버위협으로부터 사고를 미연에 방지함으로써 국가의 안전과 국익 보호 활동을 주도적으로 수행해오고 있다. 특히 남북 대치 상황 지속으로 인한 북한으로부터의 사이버공격에 대응하기 위해 2004년2월 국가사이버안전센터를 설립하고 국내외 사이버안보 유관기관들과 협업하며 사이버위협을 사전 차단하고 사고 발생 시 적극 대응하고 있다.

우리나라의 사이버안보 체계는 민간영역은 과기정통부・금융위 등 분야별 소관부처, 공공영역은 국가정보원, 국방영역은 국방부 등으로 분산되어 있는 것처럼 보이나 국정원의 국가사이버안전센터가 실무총괄을 하면서 컨트롤타워 기능을 수행하는 구조를 취하고 있다. 다만, 국가안보실이 사이버안보 현안 해결의 정점에 위치하여 의사결정 체제를 유지하면서 대통령을 보좌하는 형식을 갖추고 있다. 전반적으로 상징적인 조정자로서 국가안보실에 집권화된 거버넌스에다가 분야별 소관부처가 책임을 지면서 다시 국정원이 일부 통합적 조정 권한을 지닌 복합적인 분산형 거버넌스로 보여지며, 기관간 적절한 조화가 이루어지고 있는 것으로 보여 거버넌스 자체에는 큰 문제가 없는 것으로 여겨진다. 다만 국정원이 공공분야의 주관기관으로서 역할을 수행하고 있고 청와대 중심의 사이버안보 보좌 체계에서도 실무총괄 역할을 수행하고 있어 정보기관으로서 공식적으로 중요한 역할을 하고 있다고 할 수 있다. 이는 다른 국가와 달리 남북 대치 상황으로 인하여 지속적인 사이버공격 위협의 상당부분이 북한의 소행이라는 점 때문인 것으로 보이며, 결국 사이버안보를 국가안보 차원의 문제로 접근해왔기 때문인 것으로 판단된다. 또한 우리나라의 경우 사이버안보 이슈 자체가 특정한 사회 분야의 이슈가 아니라 우리나라가 지닌 세계 최고 수준의 인터넷 환경으로 인해 공공과 민간을 구분하지 않고 동시다발적으로 全 분야가 사이버공격과 위협에 지속적으로 노출되고 있다는 것도 정보기관의 역할 강화의 한 요인이 된 것으로 보인다.

3. 정보기관의 역할 정립 방안

정보기관의 역할은 「국가정보원법」 제3조 직무상 방첩・대테러・국제범죄조직 등에 대한 국외정보 및 국내 보안정보의 수집・작성・배포, 국가기밀에 속하는 문서・자재・시설・지역에 대한 보안업무, 정보 및 보안업무의 기획・조정 등을 통해 각종 위협으로부터 국가의 안전을 보장하고 국민의 생명을 보호하는 것이라고 볼 수 있다. 특히 사이버위협이 글로벌 안보이슈의 핵심요소로 대두되고 있는 상황에서 국내법이 허용하는 범위 내에서 사이버안보 수행체계 보강을 위한 방편으로 정보기관의 역할 정립을 위한 방안을 다음과 같이 제시하고자 한다.

3.1 사이버안보 첩보 수집・분석 집중

정보기관에 대한 권한남용 논란이나 정보공유의 한계 등이 지적받고 있고, 남북이 대치하고 있는 현실을 감안하여 사이버안보 실무총괄 기관인 정보기관의 역할을 재정립할 필요가 있다. 현행 규정상 보안책임이

관계기관의 장 및 개인 실무자에 있는 만큼, 단기적으로는 각급기관에 대한 사이버안보 활동이나 사고조사 등 공개적인 대외활동을 점진적으로 지양하고 비노출 간접활동으로 전환하면서, 장기적으로는 사이버안보 관련 첩보를 신속하게 수집, 분석, 평가하는 업무에 집중하여 청와대, 정부부처 등 각급기관에 제공, 활용토록 하는 한편 국가안보 차원의 사이버위협 상황 발생에 대비한 교육·훈련 지원 등 정보기관 고유의 업무와 조화롭게 조정하는 방향으로 사이버안보 체계를 정비해 나갈 필요가 있다.

3.2 사이버위협 예측 및 대응역량 제고

국가가 전적으로 주도해왔던 안보 문제는 제4차 산업혁명 시대를 맞아 국가가 시민사회와 개인 부문의 협조는 물론 국제사회와 공동으로 해결해야 하는 양상으로 바뀌게 될 것이다. 특히, 사이버공간에서는 초연결성으로 인해 국가, 비국가 행위자 및 비인간 행위자와 같은 다양한 실체들이 사이버공격 활동에 관여하게 될 것이며, 이에 따라 사이버위협의 발생 원인, 확산 경로 및 파급효과도 복합적인 형태로 나타나게 될 것이다. 또한, 사이버공간이 물리적 공간과 결합하는 사이버물리시스템(CPS)의 진전으로 해킹으로 인한 사고 발생 시 사이버공간을 넘어 국민의 일상적 경제생활 및 국가운영 핵심시스템 등 현실세계에 상상할 수 없는 큰 재앙을 불러와 심각한 국가안보 문제로 비화될 가능성이 다분하다고 할 것이다. 이러한 하이브리드 위협에 선도적으로 대응하기 위하여 우리 정보기관은 세계 여러 정보기관과 긴밀한 협력과 독자적인 사이버위협 수집·분석시스템을 가동하여 각종 위협요인을 사전에 발굴하여 예측하는 한편 대처방안을 제시할 수 있는 대응역량을 제고하는 방향으로 업무를 재설정할 필요가 있다.

3.3 법과 원칙 준수를 위한 법적 토대 구축

우리나라의 경우 정보기관 자체의 과거 업보와 오랜 기간의 국민 불신으로 인해 권한남용이나 개인의 프라이버시 침해 우려 등이 잔존하고 있는 상황에서 국민의 기본권을 보장하는 한편 정보기관의 정보수집, 분석, 제공 등 본연의 임무를 충실하게 하고, 정치·사회적 환경변화에 따른 외부의 압력에도 굴하지 않고 법과 원칙에 따라 업무를 제대로 수행하게 하기 위해서는 명확한 법적인 토대를 구축하고 지원할 필요가 있다. 미국의 사례처럼 정보기관의 비밀활동에 대한 대외보안을 철저히 지켜주면서 관련보고서 또는 활동사항을 주기적으로 국회, 대통령에게 동시에 보고토록 하되, 국회는 정보예산을 비공개 하에 엄격하게 통제하고, 대통령은 정보기관의 업무수행 방향을 오직 국가안위와 국민보호를 최우선으로 설정토록 하여야 한다. 특히 일정기간(예, 30년, 50년) 경과 후 비밀이 자동적으로 의무 공개되는 법적 절차를 우리도 적극 도입할 필요가 있다. 다만, 공개될 경우 국가안보에 치명적인 영향을 미치거나 국가 간의 외교적 분쟁에 악용될 소지가 있는 비밀은 국익 보호 차원에서 비공개 처리를 하는 방안도 고려해야 할 것이다.

4. 결 론

제4차 산업혁명 시대가 진전되어 정보통신기술이 획기적으로 발전하면서 사이버위협은 점점 더 지능적이고 고도화될 것이다. 그렇기 때문에 사이버안보관련 법안의 정비를 통해 사이버위협에 대한 대비책을 마련하면서 사고 발생 시에도 체계적이고 신속한 조치를 취하기 위해서는 정보기관의 역할이 중요하다고 할 것이다. 그러나 우리나라는 이와 관련된 '국가사이버안보법안' 제정이나 「국가정보원법」 개정안에 대한 논의가 지난 2006년부터 진행되어 왔으나 정치적인 역학관계로 처리되지 못하고 지지부진한 상태가 지속되고 있어 안보 차원의 사이버위협에 선제적으로 대응하는데 어려움이 있는 실정이다.

이에 본 논문에서는 「전자정부법」, 「정보통신기반보호법」, 「국가사이버안전관리규정(대통령훈령)」 등 현행 법 체계상 정보기관의 사이버안보 기능을 고찰하고, 이를 바탕으로 우리 실정에 맞는 정보기관의 역할에 대한 시사점을 살펴보았다. 또한, 향후 사이버안보 수행체계 보강을 위해서는 '국가사이버안보법안'을 제정하거나 「국가정보원법」을 개정하여 법적 허용범위 내에서 정보기관의 역할을 정립해야 하는데, 그 방안으로 사이버안보와 관련된 첩보수집과 분석에 집중하고, 사이버위협을 사전 예측하고 대응역량을 제

고하며, 법과 원칙을 준수하기 위한 법적 토대를 구축할 필요가 있음을 제시하였다. 이렇게 함으로써 궁극적으로 우리나라의 사이버안보를 한층 더 강화하는데 일조할 수 있을 것이다.

참고문헌

[1] 한희원, 「국가정보학 원론」, 법률출판사, 2011.2.

[2] 국정원, “국가사이버안전관리규정”, 대통령훈령 제316호, 2013.9.2.

[3] 윤오준, “사이버위협 정보공유 시스템 확산에 영향을 미치는 핵심요인에 관한 연구”, 숭실대대학원 박사학위논문, 2017.8.

[4] 과학기술정보통신부 등, 「2018 국가정보보호백서」, 2018.5.

[5] 국정기획자문위원회, “문재인정부 국정운영 5개년 계획”, 2017.7.

[6] 더불어민주당, 19대 대통령선거 정책공약집 “나라를 나라답게”, 2017.4.

[7] 이철우 등, “국가 사이버안보에 관한 법률안”, 의안번호 32, 2016.5.30.

[8] 정부, “국가사이버안보법안”, 의안번호 2004955, 2017.1.

[9] 민변 등 6개 시민단체, “국가사이버안보법 국회 발의안에 대한 의견서”, 2017.2.14.

[10] 임진대, “국가 사이버안보에 관한 법률안(이철우 의원 대표발의) 및 국가사이버안보법안(정부 제출) 검토보고”, 2017.2.

[11] 중앙일보, “국정원 직원 설문조사까지 거친 끝에 ‘대외안보정보원’ 낙찰…개혁안 뜯어보니”, 2017.11.29.

[12] 국회 정보위, “국가정보원 개혁에 대한 공청회 자료집”, 2018.1.31.

〔저자소개〕

윤 오 준 (Oh-jun Yoon)
1990년 2월 서울대학교 학사
2013년 8월 건국대학교 석사
2017년 8월 숭실대학교 IT정책경영학과 공학박사
2017년 3월~ 단국대학교 대학원 법학과 재학 중
email : ojyoon27271@naver.com

사진 생략

김 소 정 (So-jeong Kim)
1998년 8월 부산대학교 학사
2001년 2월 경희대학교 석사
2005년 2월 고려대학교 정보보호대학원 공학박사
2004년~현재 국가보안기술연구소 정책연구실장
email : sjkim@nsr.re.kr

정 준 현 (Jun-hyeon Jeong)
1982년 2월 성균관대학교 학사
1984년 2월 성균관대학교 석사
1991년 2월 고려대학교 법학박사
1997~2007 선문대학교 법학과 교수
2013~2017 한국사이버안보법정책학회 회장
2007~현재 단국대학교 법학과 교수
email : jeongjh@dankook.ac.kr