긴급좌담회 자료집

사이버테러방지법 제정촉구 긴급좌담회

– 자유민주연구원, 바른사회시민회의 공동주관 –

□ 일 시 : 2016년 3월 10일(목) 14:30-16:30
□ 장 소 : 프레스센터 19층 국화실
□ 주 최 : 바른사회시민회의, 자유민주연구원

자유민주연구원 · 바른사회시민회의

사이버테러방지법 제정촉구 긴급좌담회

– 자유민주연구원, 바른사회시민회의 공동주관 –

Ⅰ. 세미나 개관

■ **일　　시 :** 2016년 3월 10일(목) 14:30–16:30

■ **장　　소 :** 프레스센터 19층 국화실

■ **주　　최 :** 바른사회시민회의, 자유민주연구원

Ⅱ. 세미나 순서

▸ **등　　록 :** 14:00–14:30

▸ **개 회 식 :** 14:30–14:40
- 인사말 (바른사회시민회의 공동대표)
- 참석자 소개

▸ **기조 발제, 휴식 및 토론 :** 14:40–16:30

사　회 : 바른사회시민회의 공동대표

발　제: 유동열 (자유민주연구원 원장)

토　론 : 한희원 (동국대 법대 교수, 한국국가정보학회장)
김철우 (한국국방연구원 연구위원)
박춘식 (서울여대 교수, 전 국가보안기술연구소장)
제성호 (중앙대 법학전문대학원 교수, 한국대테러정책학회장)

Ⅲ. 핵심 토론사항

- 최근 북한의 사이테러도발 양상과 유형 전망
- 북 대남 사이버공작 전술
- 사이버테러방지법 제정의 긴급성과 정당성
- 사이버테러방지법((서상기안)의 문제점과 보완사항
- 사이버테러방지법 입법 전략

Contents

발 제 문

사이버테러 위협과 사이버테러방지법 제정의 긴급성
– 북한의 사이버테러 위협과 법 제정 –

유 동 열

자유민주연구원 원장

발 제 문

사이버테러 위협과 사이버테러방지법 제정의 긴급성
- 북한의 사이버테러 위협과 법 제정 -

유동열 (자유민주연구원 원장)

목 차

자료: 국가사이버테러 방지 등에 관한 법률안
(2016.2.22. 서상기의원 대표발의)

Ⅰ 머리말

새해 벽두부터 북한은 제4차 핵실험을 강행하고 인공위성을 가장한 장거리미사일 실험을 강행하였다. 정부와 UN 등 국제사회는 대북제재안을 잇달아 채택[1]하며 북

1) 한국: 대북확성기 방송 전면 재개(1.8), 개성공단 가동 전면 중단 결정(2.10), 독자제재방안 발표(3.8), 미국: 대북제재법안(H.R.757) 서명,공포(2.18), 일본: 대북 독자 제재조치 채택(2.19), UN: 안보리 결의안 2270호(대북제재안) 채택(3.2), 유럽연합(EU): 대북 제재대상 리스트 추가(3.5) 등

한의 비타협적 군사모험주의노선에 대해 결코 용납지 않겠다는 단호한 의지를 보여주고 있다. 이에 대응하여 북한은 서해상에서 해안포와 동해상에서 단거리 미사일을 발사하고, 2월 23일에는 북한군 최고사령부 중대성명을 발표하며 제1차 타격대상으로 청와대와 정부, 2차 타도대상으로 미국을 직접 지목하며 전쟁불사의 협박공세를 지속하고 있다.

이런 상황에서 북한의 사이버테러 위협이 점증되고 있다. 이미 북한은 1990년대 이후부터 '정보의 바다'로 불리 우는 인터넷 공간을 '남조선혁명의 해방구'로 간주하고 사이버 공간을 활용한 대남테러공작을 다방면에서 정교하게 전개해온바 있다.[2] 지금 이 시간에도 북한의 사이버전사(戰士)들이 평양과 해외거점의 데스크에 앉아 우리의 국가기관망, 금융망, 통신망, 교통망, 에너지망, 교육망 및 민간 상용망 등에 접속하여 정보를 광범위하게 수집하고 더나가 해킹 및 사이버테러도 불사하고 있는 실정이다.

북한은 2009년 7.7 사이버대란과 2011년 3.3 디도스공격, 농협전산망 공격, 2013년 3.20 사이버공격과 6.25 사이버공격, 2014년 한수원(한국수력원자력) 해킹, 서울메트로 해킹, 2016년 청와대 해킹메일 발송 등에서 보듯이 사이버테러를 노골화하고 있는 실정이다. 특히 최근에는 SNS계정과 사물인터넷(IOT) 대상 보안위협도 현실화되고 있다.

지난 3월 8일 정부는 '국가사이버안전 대책회의'를 긴급 개최하고 최근 북한의 사이버테러 공격 사례를 설명한 뒤 각 기관의 대응태세를 점검했다. 북한이 최근 정부 주요 인사 수십명의 스마트폰을 공격, 해킹된 스마트폰에서 문자메시지 · 음성통화 내용까지 가져간 것으로 확인됐다. 또한 인터넷뱅킹이나 인터넷 카드결제 때 사용하는 보안소프트웨어 제작업체의 내부 전산망이 북한에 의해 장악되고, 금융권 보안솔루션 공급업체의 전자인증서가 북한에 탈취되는 등 북한의 사이버공격이 전방위적으로 확산되는 것으로 나타났다.

---

2) 유동열, 사이버공간과 국가안보, 북앤피플, 2012. 6면.

잇다른 사이버테러 사건으로 우리사회에서 사이버테러의 위험성과 폐해에 대해 어느정도 경계감이 형성된 것 같으나, 정치권에서는 정확히 말하면 야당은 '국정원의 권한남용과 인권침해'라는 해묻는 후진적 논리를 내세워 '사이버테러 방지법' 제정을 거부하는 만행(?)을 저지르고 있다. 심지어, 현재 국내 사이버관련 법제는 '사생활 침해 방지, 인권보호, 표현의 자유 보장' 등의 명분으로 정당한 사이버상 안보수사를 저해하는 조항이 버젓이 운용되고 있으나, 국회는 미비 법규를 보완하거나 제정할 노력을 전혀 기울이지 않고 있는 실정이다.

이렇게 사이버 안보환경이 매우 열악하고 엄중한 상황 하에서 **북한 등 국내외 안보위해세력은 사이버공간과 우리 법제의 허점을 최대한 활용하여 사이버테러 등 복합적인 사이버 안보위협활동을 전개**하고 있다. 우리가 사이버테러 등 사이버상 안보위협을 방치한다면, 향후 중대한 위협에 직면할 것인바 이에 대한 최소한의 법적 정치인 사이버테러방지법이 조속히 제정되어야 할 것이다.

Ⅱ 북한의 사이버테러 위협

1. 북한의 사이버테러와 대남전략

북한이 대한민국을 상대로 사이버테러에 주력하고 있는 이유는 첫째, 국내 사이버 인프라가 세계적 수준이기 때문이다. 한국의 인터넷 사용인구(모바일 포함)가 2015년 말 기준으로 4천 6백만명으로 집계되어 전체인구의 91%을 넘어섰고, 인터넷 평균속도는 25.3Mbps로 세계1위인데, 세계 평균 4.5Mbps 대비 약 5.6배 빠른 것으로 평가된다. 이러한 상황을 감안하여, 북한은 '정보의 바다'라고 불리워지는 인터넷(Internet) 즉, 사이버공간을 그들이 추구하는 사회주의혁명을 달성하기 위한 수단의 일환으로 활용하고 있는 것이다.

둘째, 사이버 테러 등 공작이 '저비용-고효율'의 대남공작 수단이기 때문이다. 이전에는 특정한 정보를 수집하기 위해 간첩이 남파되어 활동했으나, 이제는 온라인공간에서 공개정보나 해킹 등을 통해 비밀정보를 수집할 수 있고, 2011년 농협전산망 해킹사례에서 보듯이 사이버테러를 통해 오프라인을 무력화시킬 수 있기 때문이다.

결국, 북한당국이 우리에 대해 사이버테러 등 사이버안보위협을 자행하는 궁극적 목적은 북한정권의 목표인 '전조선의 김일성·김정일주의화와 공산주의사회 건설'으로 귀착된다. 따라서 북한의 사이버공작을 정확히 파악하려면, 북한의 대남(혁명)전략 체계에 대한 이해가 선행되어야 한다.[3)]

북한은 1964년 2월 27일 조선로동당 제4차 8기 전원회의에서 제시한 '전조선혁명을 위한 3대(북한, 남한, 국제) 혁명역량 강화노선' 중 남한사회주의 혁명역량의 강화를 기하여 남조선혁명 달성을 용이하게 하려는 것인데, 바로 이의 일환으로 대남 사이버공작을 전개하는 것이다. 북한은 남한사회주의혁명 역량 강화책의 일환으로 ① 남한 내 반정부 및 종북(좌익용공)세력의 활동지원 ② 남한 국민의 의식화와 조직화 ③ 지하당 및 통일전선 구축 ④ 반혁명역량[4)] 약화 및 제거 등의 대남공작을 자행해 왔다. 북한은 정권목표인 대남혁명전략을 실현하기 위해, 오프라인(off-line)과 병행하여 온라인(on-line)공간인 사이버공간을 통해 해킹 등 사이버테러와 사이버 간첩교신, 사이버심리전 등 사이버 대남공작 등을 수행하고 있는 것이다.[5)]

2. 북한의 사이버테러 조직

북한은 이른바 남조선혁명에서 사이버공간이 차지하는 중요성을 깊이 인식하고 인적-기술적 자원을 총동원해 사이버공작을 전개해오고 있다. 북한은 1991년 걸프전이 미국주도 하의 연합국 승리로 결속된 후 현대전쟁에서 사이버전이 가지는 의

3) 북한의 대남혁명전략에 대한 상세한 설명은 유동열, 북한의 대남전략, 통일부 통일교육원, 2010. 참조.
4) 반혁명역량이란 남한혁명을 방해하는 역량으로 주한미군, 국군, 대공수사기관, 국가보안법 등을 의미하며, 이를 통해 우리사회의 혼돈상태(국론분열, 사회교란 등)를 조성하기 위해 주력하고 있다.
5) 유동열, 사이버공간과 국가안보, 북앤피플, 2012. 52-54면.

의와 중요성을 심각히 받아들여 본격적으로 사이버전에 대비한 연구에 몰두해 왔다. 김정일은 이라크전쟁이후 북한군 최고수뇌부들을 모여 놓고 "지금까지의 전쟁은 알 전쟁, 기름전쟁이었다면 21세기 전쟁은 정보전이다. 즉 누가 평소에 적의 군사기술정보들을 더 많이 장악하고 있는가, 그리고 전장에서 적의 군사지휘정보를 얼마나 강력하게 제어하고, 자기의 정보력을 충분히 구사할 수 있는가에 따라 전쟁의 승패가 좌우된다"고 역설한바 있다.[6]

또한 북한 김정은은 2013년 8월 "사이버전은 핵·미사일과 함께 우리 인민군대의 무자비한 타격능력을 담보하는 만능의 보검"이라고 언급한데 이어, 2014년 정찰총국 사이버전담부서(기술정찰국)을 방문하여 "적들의 사이버 거점을 무력화할 준비를 갖추라"라고 지시하며, 사이버테러를 독려한바 있다.

북한의 대남 사이버공작 실태를 파악하기 위해서는 관련 업무를 수행하는 북한의 대남공작기구를 먼저 파악해야 된다.

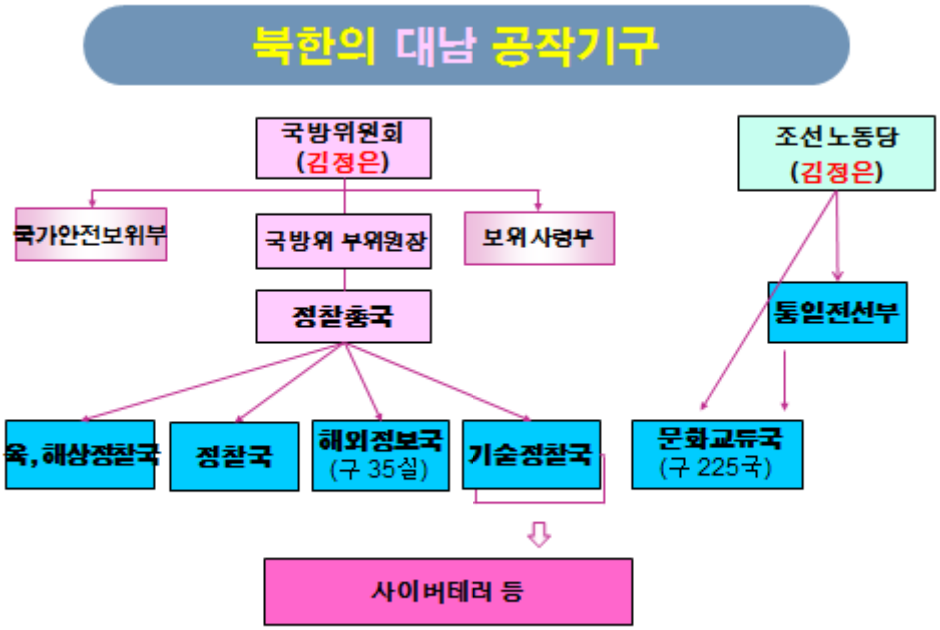
북한은 2009년 초 '2012년 사회주의 강성대국 진입' 일정에 맞추어, 대남공작부서를 전면 개편하였다. 주 내용은 그 동안 '당(조선노동당)'에서 수행하던 대남전략권(대남공작 포함)을 '군'(국방위원회)으로 이관했다는 점이다. 즉 국방위원회 직속으로 「정찰총국」을 신설하고 산하에 작전국(구 당 작전부), 정찰국(구 조선인민군 총참모부 정찰국), 해외정보국(구 당35호실), 기술국(사이버공작 전담) 등을 배치하였으며, 당 대외연락부는 225국으로 변경하여 대외적으로 내각 소속으로 위장하고, 당 통일전선부는 축소 유지하는 것을 골자로 하고 있다.[7]

그러나 2012년 말경 김정은 시대에 이르러 북한은 대남간첩공작 업무를 전담하는 225국을 통일전선부로 흡수 통합하였다. 다만 225국은 통일전선부 소속이지만 업무특성상 활동의 독립성을 보장받고 있는 것으로 보인다. 2015년 초 북한은 225국을 **문화교류국**으로 개칭하며 대남공작기구를 정비하였다. 올초 김정은은 김영철 정찰

6) 김흥광, "북한의 사이버전 대응과 전략" (비공개발표문, 2004).
7) 유동열, "북한의 대남전략과 도발의도", 제24차 세종국가전략포럼 자료집(세종연구소, 2011.4.12.), 12-13면.

총국장(북한군 대장)을 '대남비서'로 임명하고, 통일전선부장과 정찰총국장도 겸직시키고 있는 것으로 보인다.

〈도표1〉 북한의 대남공작기구



북한의 대남공작기구들은 각각 별도의 사이버테러공작을 전담하는 부서를 운영하고 있는데, **정예 사이버공작 작전인력 1,700여명에 지원 및 기술 인력 4,300여명 등 이를 합산하면 6,000여명**에 달하는 것으로 평가된다.[8] 각 대남공작기구의 사이버공작 부서를 정리해 보면 다음과 같다.

8) 2015년 국정원 및 국군사이버사령부 평가. 2016년 국방부는 지원인력이 5,100명으로 증가해 북한의 사이버인력이 총 6천 800명에 달한다고 평가했다.

〈도표 2〉 북한의 대남 사이버테러 운용체계

담당부서			주요 사이버공작 내용
국방위원회	총참모부		- 사이버전사 양성, 연구(지휘자동화 대학 등) - 한국군 대상 사이버심리전 실행(적공국 204소) - 군지휘통신 교란, 사이버전 실행(지휘자동화국) - 전자전 사단 운용 추정(2015.1)
	정찰총국		- 사이버공작 요원 양성, 연구(모란봉대학) - 대남정치, 군사정보 해킹, 사이버공작 실행 - 전담요원 해외파견, 사이버테러 등 공작수행 - 사이버 외화벌이 병행 - 대남사이버심리전(역정보, 허위정부 유포 등) * 정찰총국 내 기술(정찰)국 110연구소,414연락소 등
조선노동당	통일전선부		- 대남 사이버심리전 전담 - 160여개 웹사이트(구국전선, 우리민족끼리 등) 운영 - 트위터 등 활용 SNS공작팀 운영 - 여론조작 댓글팀 운영 허위정보, 사회교란 시도
		문화교류국 (구 225국)	- 한국 내 전략정보 수집, 오프라인 테러 배합 - 국내 간첩망을 통한 흑색선전 등 사이버심리전 병행 - 사이버 드보크, 사이버 간첩교신

첫째, 북한군 총참모부의 사이버전담부서(지휘자동화국 등)에서는 한국군에 대한 정보수집을 위한 해킹, 한국군에 대한 역정보, 허위정보 확산 등 사이버심리전 전개, 군 지휘통신체계 교란 및 무력화 등 사이버전을 전문적으로 연구·실행한다. 2015년 1월경 총참모부 산하에 사단급 전자전 부대를 창설, 운영중으로 보인다.

둘째, 국방위원회 직속 정찰총국이다. 정찰총국에서 주목해야 할 부서는 사이버전담부서인 일명 '**기술(전자)정찰국**'이다. 이 부서는 해킹 등 사이버공작, 암호통신 분석, 통신감청 등 대남공작관련 기술연구, 개발, 기술공작을 실행하는 부서이다. 특히 '110연구소'는 정찰총국의 사이버공작을 전담하는 부서로 종래 121소(일명 기술정찰조)와 100연구소를 통합한 부서인데, 사이버공간을 활용하여 한국,미국 등에 대

한 전략정보 수집, 댓글 공작 등 사이버심리전, 디도스 공격, 사이버 테러 등을 전담하고 있다.

이 부서는 2009년 7.7 사이버대란, 2011년 3.3 디도스공격, 농협전산망 무력화, 2013년 3.20 사이버공격과 6.25 사이버공격, 2014년 한수원 해킹, 2016년 청와대 해킹메일 발송, 외교안보라인 휴대폰 해킹 등을 자행한 것으로 알려져 있다.

또한, 북한은 중국 선양, 다롄, 광저우, 베이징 등 전세계에 무역회사 등으로 위장한 00개의 사이버공작 거점을 두고 사이버공작을 수행하고 있다. 이들은 사이버 테러 외에도 **사이버 도박, 게임 프로그램 개발과 불법 사이버 도박회사를 운영하며 오프라인공작도 배합하고 있다.**

세째, 통일전선부는 사이버전담부서를 운영하며, 반제민전의 웹사이트인 〈구국전선〉과 조평통의 웹사이트인 〈우리민족끼리〉 등 세계 20개국에 서버를 둔 160여 개의 친북사이트를 통해 대남 사이버심리전을 대대적으로 전개하고 있다. 또한 사이버전담 부서에는 이른바 '댓글팀'을 운용하며 국내에 조작된 정보와 여론을 확산시켜 국론분열과 사회교란을 부추키고 있다.[9] 또한 트위터, 유튜브, 페이스북 등과 같은 북한보유 SNS계정 1,000여개를 활용한 진화된 심리전공작도 전개하고 있다.

넷째, 문화교류국(구 225국)에서도 자체 사이버전담부서를 운영하며, 사이버를 통한 사이버드보크 개발 및 설치, 간첩지령, 대북보고 등 간첩교신 수단으로 활용하고 있다. 특히 국내 간첩망과 연계하여 사이버공간을 통해 악성루머 유포, 흑색선전, 대남노선 등을 선전선동하고 있다. 북한이 국내 간첩망에게 간첩통신을 통해 이를 지령한 사실이 당국에 포착된바 있다.

이외, 국방과학연구원, 북한군 총참모부 지휘자동화대학(김일정치군사대학, 구 미림대학), 김일성군사대학, 정찰총국 모란봉대학 등에서는 평양컴퓨터기술대학, 김책

9) 유동열, "북한의 사이버테러에 대한 우리의 대응방안", 북한민주화네크워크 세미나자료집(2011.6.1.).

공대, 김일성종합대 등에서 양성된 사이버요원 중 우수 요원을 차출하여 사이버전을 전문적으로 심화 연구하고 실행하는 정예 사이버요원으로 육성시켜, 북한의 대남공작부서 내 사이버전담부서에 배치하여 실전에 투입하고 있다.

현재 북한의 사이버 인프라는 전반적으로 열악하지만, **사이버테러 역량만은 미국, 중국, 러시아에 이어 세계4위로 평가되고 있다.**

3. 북한의 사이버테러 양상과 최근 동향

북한이 구사하는 대남 사이버안보위협의 유형은 **① 사이버 정보수집(해킹) ② 사이버 심리전(선전선동) ③ 사이버 통일전선 구축 ④ D-dos공격 등 사이버테러 ⑤ 사이버 간첩교신 ⑥ 오프라인과 연계된 사이버 외화벌이 공작** 등이다. **향후 결정적 시기에 대응하여 본격적인 사이버전(戰)**이 전개될 것으로 보인다.

첫째, **사이버 정보수집(해킹) 유형**이다. 북한은 예전 같으면 직파간첩이나 고정간첩을 통해 얻을 수 있는 정보를 이제는 북한 대남공작부서 사이버요원이 평양이나 해외거점의 데스크에 앉아 매일 매시각 한국의 주요 국가기관망, 공공망, 상용포탈망 등에 접속하여 조직동향, 관련자료 등을 스크린하고 각종 정보를 손쉽게 수집, 탐지하고 있다. 북한은 대남공작기구 내의 사이버전담부서들은 필요한 정보수집을 위해 주요 국가 및 공공망에 접속하여 광범위한 정보를 수집하고, 해킹 등을 통해 개인정보 및 특정정보를 대량으로 빼가는 공작을 전개하고 있다. 2000년대 초반 미국 중앙정보국(CIA)과 국방부 등 미군 관련 홈페이지에 가장 많이 접속한 IP를 추적한 결과, 북한인 것으로 파악된 사실에서 보듯이 전세계를 대상으로 광범위한 정보수집에 주력하고 있다.

2014년에도 한수원(한국수력원자력) 해킹사건 및 한국군의 무기 연구개발을 책임지는 국방과학연구소(ADD)에서 컴퓨터 3000여 대가 해킹 당하여 군사기밀 2급 및 3급으로 분류된 보고서가 수백 건 유출된 것으로 확인됐다.[10] 이외에 2000년 이후

만 해도 청와대, NSC, 국회, 외교부, 한국원자력연구원, 산업기술시험원, 고려대정보보호대학원 이메일계정, 중앙일보 등이 해킹을 당한바 있다. 2013년 국군사이버사령부가 국회에 제출한 자료에 의하면, 2009년에서 2013년 까지 북한의 해킹 등으로 입은 피해액이 8천6백억에 달하는 것으로 파악되고 있다.

둘째, 사이버 심리전 구사유형이다. 최근 북한은 다방면의 대남 사이버심리전을 전개하고 있다.

북한이 인터넷을 활용한 초보적인 대남대외선전을 개시한 것은 1996년경이다. 북한은 인터넷이 국내에서 커다란 관심과 호응을 불러 일으키고 있음을 감안하여, 1996년 말부터는 아예 북한이 해외에서 직접 운영하는 홈페이지를 개설하고 대대적인 선전에 주력해오고 있다.[11)]

현재 북한이 해외에 개설해 놓은 인터넷 웹사이트는 구국전선(반제민전 홈페이지), 우리민족끼리(조평통 홈페이지), 조선중앙통신, 류경, 조선인포뱅크, 김일성방송대학, 백두넷 등 무려 160여 개에 달하며, 직영 사이트만 노동신문, 내나라 등 12개에 달한다.

〈도표3〉 북한 직영 및 해외 친북사이트 국가별 현황

국가 / 계	북한	미국	일본	중국	독일	캐나다	싱가폴	이탈리아	태국	네덜란드	체코	덴마크	뉴질랜드	핀란드	폴란드	러시아	영국	프랑스	아르헨티나	홍콩
162	12	58	38	30	5	3	1	1	2	2	1	1	1	1	1	1	1	1	1	1

10) 동아일보, 2014년 4월 10일자 보도.
11) 유동열, “안보의 사각지대, 인터넷과 PC통신”, 자유공론 1997년 7월호(서울: 한국자유총연맹, 1997), 89면, 유동열, “적화된 인터넷매체를 고발한다” 한국발전리뷰 2003년 6월호(서울: 한국발전연구원, 2003), 113면.

북한은 직영 및 해외 친북사이트를 활용하여 북한체제와 조선로동당노선을 미화하고 선전선동하며, 김일성-김정일-김정은 우상화 및 대남심리전공작에 적극 활용하고 있다. 이를 주도하는 것은 북한의 대남공작부서인 통일전선부이다. 통일전선부에서는 심리전차원의 대남사이버공작을 주도하고 있다. 또한 사이버공간의 쌍방향성을 활용하여 허위정보 및 역정보 등을 확산시키는 여론왜곡 공작을 다양하게 전개하고 있다. 특히 통일전전부 및 정찰총국의 사이버전담 부서에는 이른바 '댓글팀'을 운용하며 국내에 조작된 정보와 여론을 확산시켜 국론분열과 사회교란을 부추키고 있다. 또한 공개게시판, 토론방 등에 고의로 정부기관, 주요인사 등에 관한 악성루머를 유포하여 곤경에 빠뜨리는 'Flame'기법도 활용하고 있다.

〈도표4〉의 통계에서도 보듯이, 북한과 국내 안보위해세력들은 인터넷 뿐만 아니라 페이스북, 트위터, 유튜브 등 SNS를 활용한 진화된 사이버 안보위해활동을 지속하고 있다. 2014년 경찰청이 차단한 SNS 계정이 무려 960개 이며, 불법카페 등 폐쇄가 142개이다. **현재 국내에 개설된 안보위해사이트만 1,000여 개가 상회하는 것으로 파악된다.**

세째, **사이버 통일전선의 구축유형**이다. 북한은 사이버공간을 이용하여 광범위한 통일전선 구축공작[12]을 추진해오며 새로운 형태의 심리전을 전개하고 있다. 국내 종북카페로 알려진 〈사이버민족방위사령부〉, 〈세계 물흙길 연맹〉, 〈통일파랑새〉 및 〈자주민보〉등이 사이버상에서 민간 친북통일전선을 구축한 대표적 사례이다. 이는 북한이 직접 심리전을 전개하는 방식에서 '중간매개체'(종북카페 등)를 통해 확대 재생산하는 효과를 거두고 있다.

넷째, **D-DOS공격 등 사이버테러 유형**이다. 북한은 2009년 61개국에 있는 586대의 공격명령 서버를 이용해 총47개 사이트를 공격한 이른바 7.7 사이버대란을 일으켰고, 2011년 3월 3일-5일에도 72개국 748대의 서버를 활용하여 국내 40여개 공공

12) 유동열, "북한의 통일전선론 체계와 구사실태", 북한학보 31집(서울: 북한연구소, 2006), 63-196면 참조.

망에 대한 D-dos(디도스)공격을 행한바 있다.

2011년 4월 농협 전산망의 해킹은 북한의 사이버공작부서는 2010년 9월 이전에 웹하드에 악성코드와 해킹프로그램을 심어놓아 여기에 접속한 국내 200여개의 PC (파악된 통계)를 감염시켰고, 이중 하나가 농협전산망을 관리하는 직원의 노트북임을 파악하고 백도어 프로그램, 도청프로그램, 범행흔적 삭제프로그램 등을 추가 설치하여 7개월 이상 집중 관리한 끝에, 마침내 4월 12일 농협전산망 파괴 공격명령을 내려 1분 만에 농협전산망 전체서버 587개 가운데 273대를 파괴시켰고 30분도 안되어 서버를 완전 다운시켜 농협 금융전산망이 마비되어 버린 초유의 사태가 벌었졌던 것이다. 금융전산망이 마비되어 완전 복구되기 까지는 무려 18일이나 소요되었다.

2013년 3.20 사이버공격시에는 당시 KBS와 MBC, YTN 등 국내 방송사와 금융사 PC 4만 8천여대와 전산장비가 파괴된바 있으며, 6.25 사이버공격시에는 방송·신문사 서버장비 파괴, 청와대, 국무조정실 등 홈페이지 변조, 정부통합전산센터 DDoS 공격, 경남일보 등 43개 민간기관 홈페이지 변조 등 총 69개 기관이 연쇄적으로 공격을 받았다. 특히 대한민국을 대표하는 청와대 홈페이지에 '통일대통령 김정은 만세'라는 구호가 뜨는 화면변조의 망신을 당하기도 했다. 북한의 사이버테러 역량을 과시한 사건이다. 이들 사이버공격은 북한이 향후 자행할 높은 단계의 대형 사이버테러의 예고편이라 할 수 있다

이외 향후 예상되는 사이버공격은 논리폭탄 공격(Bomb Attacks), 비동시성 공격(Asynchronous Attacks), 전자폭탄(E-Mail Bomb), Herf Gun(전자기장 발생을 통해 자기기록을 훼손하는 효과적인 사이버무기), EMP Bomb(강한 전자기장을 내뿜어 국가통신시스템, 전략, 수송시스템, 금융시스템의 컴퓨터나 전자장비 등을 목표로 하여 사회인프라를 일순간 무력화시키는 무기), Nano Machine(개미보다 작은 로봇으로 목표 정보시스템센터에 배포되어, 컴퓨터 내부에 침투하여 전자회로기판을 작동불능케 함으로써 컴퓨터를 불능상태로 만드는 것으로, 하드웨어를 직접 대상으로

하는 무기) 등이 있다.[13)]

다섯째, **사이버 간첩교신 유형**이다. 국내에 직파된 간첩 및 장기간 암약하는 고정간첩들은 과거와 같이 무전기를 통한 대북보고나 무인포스트에 의존하지 않고도, 진일보한 방법으로 인터넷을 통해 간단하게 대북보고나 지령을 하달 받을 수 있게 되었다.

북한의 대남공작부서에서는 이른바 '사이버 드보크'(Syber Dvoke) 란 신종 연락수단을 개발하여, 사이버상 도처에 드보크를 설치하여 간첩간 연락수단으로 활용하고 있다. 2010년 적발된 간첩 한춘길사건에서 본격적으로 '사이버드보크'가 등장한바 있다. 또한 북한은 간첩교신 수단으로 첨단 '스테가노그라피'(Staganography)를 활용하고 있다. 스테가노그라피란 비밀메시지를 이미지, 오디오, 비디오 또는 텍스트 등 커버라 불리우는 다른 미디어에 숨겨서 전송하는 첨단 과학적 기법이다. 이 방식은 메시지를 숨기는 것은 물론 메시지 전송여부를 알지 못하게 하는데 목적이 있다. 이 방식은 2001년 알카에다가 9.11테러 공격의 준비와 실행시 사용한 것으로 알려져 있는데, 2012년 왕재산간첩단 사건에서 발견되었으며, 2013년 전식렬 간첩사건 시에는 진화된 방식의 스테가노그라피로 교신한 사실이 밝혀졌다.

여섯째, **사이버 외화벌이 공작 유형**이다. 또한, 북한은 중국 선양, 다롄, 광저우, 베이징 등 전세계에 무역회사 등으로 위장한 00개의 해외 사이버공작 거점을 두고 사이버공작을 수행하고 있다. 이들은 사이버테러 외에도 **사이버 도박, 게임 프로그램 개발과 불법 사이버 도박회사를 운영하며 연간 10억 달러 규모의 외화벌이사업**도 병행하고 있는 것으로 평가된다.

2014년 4월 2일 캄보디아 경찰은 북한인 8명이 캄보디아 프놈펜 공항에서 현지 경찰에 체포하였는데, 이들은 현지에서 축구 경기 등 스포츠 도박사이트를 불법 개설한 뒤 한 해 우리 돈 100억여 원에 달하는 외화벌이 사업을 해 온 것으로 들어

13) 이미정·한승환, "사이버공간에서의 국가안보위협요인 및 대책방안", 국방연구 제48집(서울: 한국국방과학연구원, 2005.12), 47면

났다. 이들은 사이버보안이 취약한 동남아 국가들에 도박 사이트를 차려놓고, 현재 북한이 장악하고 있는 약 100만대의 좀비PC들을 활용해 가입자 확보에 나서며, 외화벌이와 함께 악성코드를 불법으로 유포하여 사이버테러시 활용하고 있는 것으로 알려졌다.

이런 사실을 종합해 보건데, 현재까지는 북한이 인터넷공간을 이용하여 체제선전 등을 통한 대남 정보수집, 사이버심리전, 사이버 통일전선 구축, 사이버테러 및 간첩교신 및 외화벌이의 수단으로 활용하고 있지만, 향후에는 국가안보망과 군사망을 무력화시키는 사이버전까지 감행할 가능성이 농후하다고 전망된다.

아렇게 사이버공간을 활용한 북한의 안보위협은 1990년 중반 이래 '점에서 선으로', '선에서 면으로', '면에서 공간으로' 확대 발전하며 정교하게 전개되어 오고 있다. 최근 북한이 전개하고 있는 대남 사이버안보위해 활동의 특징을 정리해보면 다음과 같다.

첫째, 북한은 정권적 차원에서 대남혁명전략의 일환으로 사이버공간을 활용한 안보위협을 자행하고 있다. 북한은 대남공작부서 별로 사이버전담부서를 독립적, 기능별로 운영함으로서 사이버공작 기술 개발, 사이버전담요원 양성, 사이버공작 실행 등이 세분화, 전문화, 다각화되는 장점을 가지고 있다. 앞서 지적했지만 무려 6,000여명의 사이버요원이 대남공작에 투입되어 다양한 공작을 전개하고 있는 실정이다.

둘째, **북한은 해외에 개설한 160여개의 웹사이트 외에 자체보유한 1,000여개의 계정 즉 트위터, 페이스북, 유튜브 등 소셜네트워크서비스(SNS: Social Networking Servic)를 활용한 대남심리전도 강화**하고 있다. 이는 인터넷의 발달과 스마트폰 등 모바일 첨단기술화에 배경을 두고 있다. 북한의 사이버공작이 IT기술 발전에 대응하여 진화하고 있는 것이다. 북한이 해외개설 웹사이트를 통해 게시한 대남선전물은 매년 증가하고 있는 추세이다. 이들 선전문들이 국내에 유포되어 확대 재생산되고 있는 것이다.

2013년 당국의 발표에 의하면, 2012년 총선,대선시 북한 통일전선부가 직영하는 중국 선양 사이버거점에서 SNS를 통해 배포한 정부,여당 비방글이 1만 4천여건에 달하며, 정찰총국과 통전부가 보유한 SNS계정이 300여개라고 밝힌바 있다. 실제 2014년 경찰이 차단한 안보위해 트위터 등 SNS계정만 960건에 달한다.

셋째, 북한은 우리사회 정치, 경제, 사회현안에 대한 흑색선전 뿐만 아니라, 북한의 영화, 음악, 소설, 문헌 등을 집중 전파하는 '사이버 문화심리전'을 강화하고 있다. 이는 이른바 '문화 영향공작'의 일환이다. 〈우리민족끼리〉 등 북한이 개설한 웹사이트에 접속하면 손쉽게 이를 자료를 다운로드 받을 수 있다. 북한이 사이버상에서 친북문화 붐(boom)을 조성시키며 고차원적인 적색(赤色) 문화공세를 취하고 있는 것이다.

넷째, 북한의 사이버 댓글공세가 강화되고 있다. 북한은 **사이버 심리전 전담부서를 통일전선부와 정찰총국 등에 이른바 '댓글팀'을 신설하고 사이버심리전공작을 주도하고 있다. 특히 이들 사이버전담 부서에는 300명이 넘는 이른바 '댓글전문요원'이 활동 중인 것으로 있는 것**으로 알려져 있다. 북한의 사이버 댓글요원들은 국내에서 비합법적 방법으로 입수한 개인정보를 가지고 국내 주요 포탈사이트의 영향력 있는 카페 등에 회원으로 가입하고 또는 공개게시판, 토론방이나 직접 블러그 등을 개설하고 우리사회에 조작된 정보와 여론 즉 유언비어, 흑색선전 등을 확산시켜 국론분열과 시위선동 등 사회교란을 부추키고 있다.

다섯째, 북한은 사이버공간을 이용하여 광범위한 통일전선 구축공작을 추진해오며 새로운 형태의 심리전을 전개하고 있다. 북한이 최근에 1990년대 이후 간고한 노력 끝에 구축에 성공한 상층-중층-하층을 연결하는 통일전선의 배합공작을 시도하고 있다. 북한이 구사하는 통일전선의 핵심키워드(keyword)는 '우리민족끼리', '우리민족제일주의', '민족대단결', 및 '민족공조'이다. 북한은 '민족'을 내세워, 국내에 친북반미(親北反美)전선을 구축하고 이를 통해 북한핵문제 해결의 '인질'로 한국국민을 활용하려는 술책을 구사하고 있다.

국내 종북카페로 알려진 〈사이버민족방위사령부〉, 〈세계 물흙길 연맹〉, 〈통일파랑새〉, 〈자주민보〉 등이 사이버상에서 민간 친북통일전선을 구축한 대표적 사례이다. 이는 북한이 직접 심리전을 전개하는 방식에서 '중간매개체'(종북카페 등)를 통해 확대 재생산하는 효과를 거두고 있다. 이들 매체가 폐쇄되자 유사 대체매체를 신설하여 활동해오고 있다. 〈자주민보〉의 경우, 2015년 2월 13일 대법원에 의해 등록취소 확정판결이 나기 이틀 전 명칭을 〈자주일보〉로 변경하여 재등록하고, 서울시가 자주일보 발행정지 처분을 내리자, 서울시가 아닌 전라남도에서 2015년 3월 24일 〈자주시보〉 명칭으로 등록 시도를 한바 있다. 문제는 현행법(신문법)상 이를 규제할 법적 근거가 없다는 점이다.

여섯째, 북한은 온라인과 오프라인을 배합하여 대남 사이버 안보위해 활동을 전개하고 있다. 북한이 전적으로 온라인을 통해 사이버공작을 전개하기엔 제한적이기 때문에 오프라인공간과 배합할 수 밖에 없다. 즉 사이버테러를 하기 위한 준비공작 단계에서 **오프라인상 '매개체'가 필요**한 것이다. 실제 사례를 몇 건 제시해보면 아래와 같다.

2012년 당국은 북한 정찰총국과 연계하여 DDoS 공격용 악성코드와 사행성 게임을 국내에 반입하여, 북한 공작원으로 하여금 DDoS 공격용 악성코드를 웹하드, SNS 통해 유포토록 한 사행성게임 수입브로커 조모씨를 적발하였다. 포커, 바카라 등 게임 설치시 DDoS 공격용 악성코드를 함께 반입했고, 북한 공작원이 이를 유포하여 실제 2,700여대의 컴퓨터가 DDoS 공격용 악성코드에 감염되어 이른바 좀비 PC가 되었으며, 그중 인천공항 등 상대로 악성코드의 전파를 시도한 사실도 확인되었다. 당시 악성코드는 2013년 3.20과 6.25 사이버공격시 사용된 악성코드와 일치하여, 북한소행임을 입증하는 증거로 평가되었다.

2013년 7월 당국은 학생운동권 출신의 국내 정보기술(IT) 업체 대표 김모(50)씨가 북한 정찰총국 간첩과 접촉하여 북한 사이버요원에게 국내 전산망 서버 접속 권한

을 넘겨 국내외 개인용 컴퓨터(PC) 약 11만 대가 좀비PC로 감염된 사실을 적발하고 검거한바 있다. 북한 사이버고작요원들은 이를 이용해 국내 전산망에 침투한 뒤 악성 바이러스를 유포했다. 만약 북한이 좀비PC 11만 대로 디도스 공격 등 사이버테러를 감행했다면 심각한 피해가 발생했을 수 있었을 것이다.

2015년 3월 경찰청은 중국해커로부터 인터넷 보안업체 관계자들이 '도박 사이트를 공격해 달라'는 청탁을 받고 디도스 공격을 한 혐의로 양모씨 등 3명을 구속하였다.

일곱째, 최근 사물인터넷(IOT) 대상 보안위협도 현실화되고 있다. 각종 기기의 인터넷 연결이 증가함에 따라 기존에 PC, 서버 등을 대상으로 하던 사이버공격이 사물인터넷으로 전이되기 시작한 것이다. 2014년 경우 유무선공유기, 홈CCTV, 냉난방 제어기들의 취약점을 악용한 공격이 발생되고 있다.[14] 향후 북한이 이를 활용한 사이버공작이 전개될 것으로 보인다.

여덟째, 북한의 사이버안보 위협 기법이 6.25 사이버공격에서 보듯이 급속히 진화되고 있다. 또한 첨단 간첩교신인 스테가노그라피방식도 2013년 전식렬 간첩사건 시에서 확인되었듯이 진화된 방식을 사용한 것으로 밝혀졌다. 향후 북한은 이제까지의 사이버안보위협이 낮은 단계와 중간 단계에서 높은 단계의 사이버공격 유형을 선보일 것으로 예상된다.

■ 최근 사이버테러 관련 주요 동향

● 2014년 6월, 김정은 정찰총국 방문시, 사이버거점 무력화 방침하달

2014년 6월 김정은은 평양 룡성구역에 신축된 것으로 알려진 정찰총국 소속 사이버전담부서(기술정찰국) 청사를 방문하여, 사이버 전형을 보고받고, “적들의 사이버

14) 국가정보원 외, 2015 국가정보보호백서, 2015, 7-8면.

거점들을 일순에 장악하고 무력화 할 수 있는 만반의 준비를 갖출 것"을 지시했다.

● **2015년 1월, 사단급 전자전 부대 창설**

북한은 2015년 1월경 김정은 지시로 북한군 총참모부에 사단급 규모의 '전자전 부대'(사이버전 부대)를 창설, 운용중인 것으로 알려졌다. 김정은이 2012년부터 전략 사이버사령부를 창설하라고 지시한 것으로 알려져 있으나, 동 명칭의 사령부를 신설되지 않았고 동 전자전부대가 사이버전을 수행하는 것으로 보인다.

● **2015년 7월-8월, 북 사이버테러 실전(實戰) 경연대회 실시**

북한은 김정은의 지시로 2015년 7월 1일부터 3개월에 걸쳐 북한의 사이버공작 전담부서를 참가시켜 한국과 미국을 대상으로 특정사이트를 실제 공격하는 이른바 사이버테러 실전 경연대회을 실시한바 있다. 대회는 1차 평가 및 2차 평가로 이어졌으며. 여기에는 국방위 직속 정찰총국의 기술정찰국, 북한군 총참모부 소속 사이버 전담부서, 당 소속 사이버전담부서 및 컴퓨터 전공 대학 등 전문부서가 참가한 것으로 알려져 있다.

그동안 정찰총국 주도의 사이버테러가 악성코드 유형, 경유지, IP 등 테러패턴이 노출된떼 따라, 해외거점을 재배치하고 다양한 사이버 침투 및 해킹기술을 발굴하려는 시도의 일환으로 평가된다. 북한은 향후 기존의 사이버테러 패턴과는 전혀 다른 새로운 유형의 사이버공격을 자행할 가능성이 높아 졌다. 실제 2015년 7월 북한 소속으로 추정되는 해커가 이탈리아 보안업체 해킹팀에서 유출된 기술을 활용해 최근 국내 인터넷망에서 악성코드를 유포한 것으로 파악됐다.

● **2016년 2월 북 해외주재 해킹요원, 평소보다 10배정도의 고강도 대남사이버공격 시도**

올해 2월에 들어 북한의 사이버요원(해킹)들이 하루 18시간씩 한국과 미국 · 아시

아 등을 대상으로 10배 정도의 고강도 공격을 자행한 것으로 밝혀졌다. 실제 미국 사이버보안업체 노베타가 발표한 자료에 의하면 북한 해커집단은 올 2월에만 하루에 6, 7시간만 쉬면서 한국과 미국은 물론이고 아시아 지역 다른 국가에 대해서도 작전을 펼치고 있으며 아직 사용하거나 공개되지 않은 방법으로 한국에 대한 새로운 공격을 준비 중이라는 정황이 포착되었다고 밝힌 바 있다.

● **2016년 2월 북한추정 악성코드 유형 공격이 5-10배**

올해 2월에 들어 북한 또는 북한 의심 악성코드가 평상시에 비해 2월 들어 적어도 5배, 10배 정도 늘었다는 국내 보안전문그룹(하우리 등)의 평가가 있다,

● **2016년 3월 북한, 스마트폰 해킹 등(국정원 보도자료 인용)**

3월 8일 국가 정보원이 밝힌 최근의 북한 해킹사례를 보면 지난 2월말부터 3월초 사이에 정부 주요 인사 수십명의 스마트폰을 공격, 해킹된 스마트폰에서 통화내역과 문자메시지, 음성통화 내용까지 절취했다. 국정원은 북한이 주요 인사 스마트폰으로 유인 문자메시지를 보내 악성코드를 심는 방식으로 스마트폰을 공격한 것을 확인하고, 정부합동으로 감염 스마트폰에 대한 악성코드 분석 · 차단, 해킹 경로 추적 등 긴급대응에 나섰다.

조사결과 공격대상 스마트폰 중 20% 가까이 감염됐으며, 감염된 스마트폰에 담겨있던 주요 인사들의 전화번호가 추가로 유출된 것이 확인됐다. 북한 해킹조직은 2013~2014년 자체 개발한 스마트폰 게임 변조 프로그램에 악성코드를 은닉, 국내 비공식 앱마켓을 통해 유포하는 방식으로 2만5천여대에 달하는 국내 스마트폰을 해킹해 전화번호와 문자메시지 등을 절취한 바 있다.

지난 2월 국정원은 미래부 · 한국인터넷진흥원과 협조, 북한 해킹조직이 우리 국민 2천만명 이상이 인터넷뱅킹 · 인터넷 카드 결제 때 사용하는 보안소프트웨어 제작업체 내부 전산망에 침투, 전산망을 장악한 것을 확인했다. 국정원은 즉시 업체

와 협조해 보안조치에 들어갔으며, 점검결과 업체 서버 외에 일반 국민의 피해는 없는 것으로 확인됐다.

국정원은 또 금융위 · 금융보안원과 협력, 국내 대부분 금융기관에 인터넷뱅킹용 보안소프트웨어를 납품하는 다른 업체의 전자인증서(코드 서명)도 북한에 의해 해킹, 탈취된 사실이 2월 드러났다. 북한은 다수의 국가 · 공공기관에서 사용하는 내부정보 유출방지 소프트웨어의 취약점을 활용해 해킹한 것으로 확인됐으며, 국정원은 해당 제품을 사용하는 국가 · 공공기관을 대상으로 긴급 보안조치를 실시했다. 전자인증서는 특정 프로그램을 설치할 때 배포한 회사의 정보를 알려줘 사용자가 믿고 내려받을 수 있게 하는 것이다. 흔히 알고 있는 공인인증서가 코드서명에 포함된다.

북한의 이번 공격은 2013년 언론 · 금융사 전산장비를 파괴한 '3.20 사이버테러'와 같은 금융 전산망 대량파괴를 노린 사이버테러의 준비단계로 분석되며 사전에 발견하지 못했다면 인터넷뱅킹 마비나 무단 계좌이체 등 대규모 금융 혼란이 야기될 수도 있었다고 국정원은 설명했다. 이에앞서 북한은 지난 1~2월 2개 지방의 철도운영기관 직원들을 대상으로 피싱 메일을 유포, 직원들의 메일 계정과 패스워드 탈취를 시도했다. 철도교통관제시스템을 대상으로 사이버테러를 하기 위한 준비단계였다. 국정원은 즉시 해당 기관에 관련 사실을 통보하고 메일 계정 등에 대한 차단조치를 했다고 한다.

북한은 지난해 6만여대의 좀비PC를 만든데 이어, 올해 1월에만 세계 120여개 국가에 1만여대의 좀비PC를 만들어 관리하고 있는 것으로 파악된다. 이런 좀비PC들은 북한의 지령에 따라 언제든지 우리 사이버공간을 공격하는 사이버무기가 될 수 있다.

Ⅲ 사이버테러방지법 제정

1. 사이버테러방지법의 긴급성과 필요성

사이버테러방지법은 앞서 지적한 것처럼, 북한 등의 점증하는 사이버안보위협에 효율적으로 대처하여 국민의 생명과 재산 및 국가안보를 보호하기 위한 최소한 필수적인 법적 장치이다.

파리 테러참사 이후 전세계 주요국가들은 신속하게 사이버테러 등 테러관련 법을 강화하고 정보기관에 더 많은 권한을 주는 추세이나, 입법권을 가진 우리 국회는 고속으로 역주행하고 있는 격이다. 초국가적 안보위협에 직면하고 있는 21세기에 세계 12위권의 대한민국이 '국정원의 권한남용 및 인권침해'라는 상투적인 후진적 반대논리로 사이버테러방지법 하나 제정하지 못하고 있는 현실은 **국가의 망신이자 안보위기의 방치**나 다름없다. 국내외 사이버테러정세에 엄중함을 감안할 때, 사이버테러방지 관련 입법은 선택의 문제가 아니라 **필수사항**이다. 만약에 19대 국회 회기 내에도 사이버테러방지법을 제정하지 않는다면, 국회가 정확이 말하면 야당이 **테러분자들의 비호세력**이라는 비난에서 자유로울 수 없을 것이다

서상기 의원이 대표발의 수정안의 법안취지를 보면 다음과 같다.

- 과거 1·25 인터넷 대란과 같은 전국적인 규모의 국가 주요 정보통신망 마비사태 발생과 해외로부터 조직적인 사이버테러로 국가기밀 및 첨단기술의 유출 등 국가·사회 전반에 중대한 영향을 미칠 수 있는 사이버위기 발생 가능성이 날로 증대하고 있음.

- 특히 사이버공간은 국경을 초월하여 범지구적이면서 정부와 민간부분이 상호 밀접히 연계되어 있어 매우 복잡·고도화되며, 시공간의 제약을 벗어나 발생하는

모든 사이버공격을 정부와 민간 어느 하나도 단독으로 차단하기에는 분명한 한계가 있음.

- 그러나 우리나라는 아직 국가차원에서 사이버테러 방지 및 위기관리업무를 체계적으로 수행할 수 있는 제도와 구체적 방법·절차가 정립되어 있지 않아 사이버위기 발생 시 국가안보와 국익에 중대한 위험과 막대한 손해를 끼칠 우려가 있음.

- 따라서 정부와 민간이 참여한 국가차원의 종합적인 대응체계를 구축하도록 하고, 이를 통하여 사이버테러를 사전에 탐지하여 사이버위기 발생 가능성을 조기에 차단하며, 위기 발생 시 국가의 역량을 결집하여 신속히 대응할 수 있도록 하고자 함.

정부당국의 동법 제정 필요성을 인용해보면 다음과 같다.

- 최근 북한에 의한 우리 핵심기반시설 대상 사이버테러는 경제적 피해는 물론 사회 혼란을 유발하고 국가안보를 위협하는 심각한 상황까지 초래

- 특히, 최근에는 국가 · 공공기관보다 상대적으로 보안이 취약한 민간 정보통신망을 대상으로 한 북한의 사이버테러가 크게 증가, * '11.4 농협전산망 마비, '13.3.20 · 6.25 사이버테러 등 대규모 테러는 물론 서울메트로('14.9), 한수원('14.12) 해킹 등 對南 사이버테러 빈번 자행

- 그러나, 이러한 사이버공격에 대한 정부의 대응활동이 국가 · 공공기관에만 적용되는「국가사이버안전관리규정」(대통령훈령)에 근거하고 있어

- 민간분야와의 정보공유는 물론 민간분야에서 발생하는 사이버테러 징후를 사전탐지 · 차단하거나 대책을 강구 · 적용하는데 한계가 있고

- 민간기업은 보안취약점이 발견되어도 비용부담 · 기술부족 등으로 신속한 보호조치를 하지 않아 피해가 반복해서 발생하는 상황임. 평시 사고예방을 위한 법률도 「전자정부법」·「정보통신기반보호법」·「정보통신망법」 등으로 산재, 대응주체간 역할상충 · 혼선 요인으로 작용

- 또한, 미국 · 독일 · 일본 등 주요 선진국들도 사이버위협의 심각성을 인식하고 자국내 사이버안보 관련 법률을 제정. * 美「사이버안보법」('15.12), 獨「IT-보안법」('15.6), 日「사이버시큐리티기본법」('14.11)

- 이에 정부와 민간이 함께 협력하여 국가차원에서 체계적이고 일원화된 사이버테러 예방 및 사이버위기 대응업무를 수행하기 위해 「사이버테러방지법」과 같은 통합법 제정이 필요함

- 책임기관 및 감독기관에게 사이버안전관리 책임을 부여하고 자체 보안대책을 마련케 하는 등 자율 보안관리 체계를 구축토록 명문화

- 평시 위협정보 공유체계 운영 및 대규모 사이버테러 발생시 정부 차원의 경보발령과 대책본부 운영 등 사이버위기 대응체계 확립

2. 사이버테러방지법(서상기안)의 주요 내용

2013년 4월 9일 서상기 의원(새누리당)이 「국가 사이버테러방지에 관한 법률안」 발의하였고, 2016년 2월 22일 직권상정을 위해 정보위 법안심사소위에서 논의한 서상기 의원안의 수정안이 재발의되었다. 주요 내용은 다음과 같다.

- 사이버테러를 '외국, 북한, 해킹 · 범죄조직 및 이에 연계 또는 후원을 받는 자 등이 국가안보 · 공공의 안전을 위태롭게 할 목적으로 정보통신망을 공격하는 행위'로 구체적으로 정의(안 제2조)

- 사이버테러에 대한 국가차원의 종합적이고 체계적인 예방·대응과 사이버위기관리를 위하여 국가정보원장 소속으로 국가사이버안전센터를 둠(안 제6조)

- 책임기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응할 수 있는 보안관제센터를 구축·운영하거나 다른 기관이나 보안관제전문업체가 구축·운영하는 보안관제센터에 그 업무를 위탁하여야 함(안 제8조)

- 국회, 법원, 헌법재판소, 중앙선거관리위원회의 장 및 중앙행정기관의 장은 사이버테러로 인해 피해가 발생한 경우에는 신속하게 사고조사를 실시하고, 중앙행정기관의 장은 그 조사결과를 미래창조과학부장관, 국가정보원장 및 금융위원장 등 관계 중앙행정기관의 장에게 통보하여야 함(안 제9조).

- 정부는 사이버테러에 대한 체계적인 대비와 대응을 위하여 책임기관의 장의 요청과 수집된 정보를 종합·판단하여 관심·주의·경계·심각 단계의 사이버위기경보를 발령할 수 있음(안 제10조)

- 정부는 경계단계 이상의 사이버위기경보가 발령된 경우 원인분석, 사고조사, 긴급대응, 피해복구 등의 신속한 조치를 취하기 위하여 국가 역량을 결집한 민·관·군 전문가가 참여하는 사이버위기대책본부를 구성·운영할 수 있음(안 제11조).

- 정부는 사이버테러 기도에 관한 정보를 제공하거나 사이버테러를 가한 자를 신고한 자 등에 대하여 포상금을 지급할 수 있음(안 제13조).

- 직무상 비밀을 누설한 경우에는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하고, 피해의 복구 및 확산방지를 이행하지 아니한 경우에는 1천만원 이하의 과태료에 처할 수 있음(안 제14조 및 제15조).

- 사이버테러방지법 제정시 기대효과

o 사이버테러 관련 업무는 사전예방, 사고조사 · 분석, 복구지원 등으로 구분

o 우선, 사이버테러 예방 및 위기관리 책임을 국가 · 공공기관에서 국회 등 헌법기관과 민간 주요기관까지 확대 · 적용할 수 있음

- 민 · 관 · 군이 참여하는 국가 차원의 사이버위협 합동대응팀, 사고대책본부 및 위협정보공유체계를 구축 · 운영할 수 있고

- 사이버테러 탐지 · 대응 및 사고조사 · 복구 등에 백신업체, 정보보호시스템 제작자 등 민간기관의 지원 · 협조 등 참여가 가능하게 됨

- 특히, 그간 사이버테러 예방의 사각지대였던 국회, 법원, 헌법재판소, 선관위 등 헌법기관에게 자체 사이버테러 예방 및 점검활동의 책임을 부여할 수 있음

o 또한, 책임기관 및 지휘 · 감독기관에게 사이버안전관리 책임을 부여하고 자체 보안대책 마련 등을 의무화함으로써, 각 기관들이 자체적인 보안관리 체계를 구축 · 운영토록 할 수 있음

o 뿐만 아니라, △사이버테러 방지 및 위기관리 기본계획 △위기관리 시행계획 및 이행여부 확인 △위기관리실태 점검 · 평가 등 사이버테러 예방을 위한 기획 · 관리체계를 운영할 수 있으며

o 신속한 사이버테러 대응이 가능토록 책임기관에게 보안관제센터를 운영하거나 他 기관 또는 보안관제업체에 위탁하도록 의무화할 수 있음

3. 사이버테러방지법 반대논거 비판

(1) 국정원의 권한남용과 인권침해 주장

사이버테러방지법 반대의 대표적 논거는 국정원이 국민사생활을 무제한 사찰하는 등 인권침해 우려가 높고, 권한남용이 예상된다는 것이다. 이는 지난 10여년 간 단골로 등장하는 상투적인 논리이다. 이는 국정원법 개정과 법규정에 의한 활동으로 더 이상 무의미한 문제제기이다.

첫째, 북한 등의 사이버테러를 예방 · 대응하는 업무는 국가안보와 직결된 사항으로, 「정부조직법」(국가안보 관련 정보 · 보안 업무)과 「국가정보원법」(국내외 보안정보 수집, 기밀 문서 · 시설 보호)에 따른 국정원의 고유 임무기능이다. 이러한 국정원의 사이버안보 관련 임무 · 기능은 「국가정보원법」, 「전자정부법」, 「정보통신기반보호법」 등에서 이미 구체적으로 명시되어 있다.

- 「국정원법」상 국외 정보 및 국내 보안정보의 수집 · 작성 · 배포(제3조제1항제1호), 국가기밀에 속하는 문서 · 자재 · 시설 및 지역에 대한 보안업무(제2호)

- 「전자정부법」상 행정기관 정보통신망 보안대책 수립 · 지원 및 이행여부 확인(제56조)

- 「정보통신기반보호법」상 공공분야 기반시설 보호정책 수립, 보호대책 이행여부 확인, 신규지정 권고 및 보호기술 지원 등 실시(제5조의2, 제7조 등)

둘째, 정부는 사이버위기 경보발령시, 관계중앙행정기관은 사고대책본부장 임명시 사이버안보 컨트롤타워인 국가안보실과 협의하여 정하도록 하고 있고, 국정원은 「정보통신기반보호법」, 「전자정부법」 등 각종 법령에 따라 이미 수행중인 업무를

동법에 반영하고 있을 뿐이다. 특히, 민간분야의 경우 대책수립, 이행여부 확인, 위협정보 수집, 사고조사 등 업무 대부분을 미래부 · 금융위와 관계 중앙행정기관이 수행토록 규정하고 있다. 따라서, 동법의 제정으로 국정원의 권한이 강화되기 보다는 오히려 법률 주관기관으로서의 책임이 강화되는 것으로 이해해야 한다.

셋째, 최근 사이버공격이 초국가적 안보위협으로 등장하면서 세계 각국은 자국의 국가기밀 및 주요기반시설 등을 보호하기 위해 정보기관을 중심으로 사이버역량 확대와 함께 국가간 협력을 강화하는 추세이다. 미국의 DNI, 영국의 GCHQ, 이스라엘의 ISA 등은 정보기관이 사이버위협정보를 수집 · 분석하고 있으며, EU는 파리테러 이후 域內 합동정보기구 설립 필요성이 제기되고 있다.

넷째, 북한이 대남적화혁명의 핵심수단으로 사이버공작을 빈번하게 자행하고 있는 상황에서, 북한의 사이버공격에 효율적으로 대응하기 위해서는 ① 기술 전문성과 종합분석 역량을 바탕으로 예방 → 탐지 → 대응 → 복구 · 지원 등 유기적인 활동 수행 능력이 필수적이며 ② 평시 공격조직 추적, 실체확인, 활동감시 등의 활동과 함께 사이버공격시 공격주체에 대한 첩보수집 및 분석 활동이 무엇보다도 중요한데, 이러한 기술적 탐지활동은 물론 해외 정보기관과의 협력 및 휴민트를 통한 첩보수집이 융합되어야 하는 고도의 수집 · 분석 역량이 요구되고 있어, 국가사이버안전센터를 국정원에 두는 것이 타당하다. 국내에 국정원을 대체할 정보기관이 현실적으로 없다.

다섯째, 동법에 민간업체와 관련된 주요 규정으로 '안전센터장의 책임 · 지원기관에 대한 지원요청'(제6조), '위협정보공유'(제8조), '사고조사'(제9조) 등이 있는데, 법안 제6조(사이버안전센터의 설치)에 따라 안전센터의 장(민 · 관 · 군 합동대응팀)이 책임기관 및 지원기관에게 인력 · 장비의 지원을 요청하는 것은 국가기관보다 높은 수준의 전문성과 첨단 장비를 보유한 민간업체의 지원을 통해 사이버위협에 효과적으로 대응하기 위한 것이다.

국정원은 민간업체에 대해 협력과 지원을 요청할 수 있을 뿐, 영향력을 행사할 수 있는 어떠한 권한도 규정하고 있지 않다. 또한 법안 제8조(보안관제센터 등의 설치)는 민간업체를 포함한 책임기관들이 사이버위협정보를 국정원뿐만 아니라 관계 중앙행정기관과도 공유토록 하고 있어 국정원의 영향력 확대와는 무관하다.

법안 제9조(사고조사)의 경우에도 민간업체 관련 사고는 민간부문을 책임지는 미래부 · 금융위 등에 통보하거나 지원을 요청할 수 있도록 하고 있어 국정원이 자의적으로 업체에 접근하거나 영향력을 행사할 수 없다.

(2) 정통망법과 기반보호법으로 충분하다는 주장

첫째, 정통망법(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」)은 정보통신서비스 제공자나 집적정보통신시설 사업자 등 민간의 정보통신 관련 업체와 이들 서비스 이용자의 정보보호에 관한 사항만을 규율하고 있고, 기반보호법(「정보통신기반보호법」)은 주요정보통신기반시설로 지정된 시설(현재 385개)에 대해서만 제한적용하고 있어, 각각 민간 분야 사업자와 기반시설로 지정된 시설에 한정 적용되며, 규율하는 내용과 방법, 절차가 모두 상이하다.

둘째, 이들 법률 이외에도 공공, 국방 및 금융 분야의 사이버안전에 관한 법률들이 존재, 상이한 방법과 절차를 통해 사이버위협에 대응하고 있는데, 공공분야는 「국정원법」, 「전자정부법」 및 「국가사이버안전관리규정」, 국방분야는 「국방정보화법」, 금융분야는 「전자금융거래법」 등 소관 영역의 특수성을 고려, 보호대책을 마련하고 있으나 개별 영역을 불문하여 국가 차원의 사이버위협 정보를 공유하고 사이버 공격을 탐지 · 대응할 수 있는 체계를 규정하고 있지 않음에 따라 안보와 국익을 위협하는 사이버위협에 국가 차원에서 효과적이고 종합적으로 대응하기 위해서는 사이버테러방지법 제정이 필요하다.

Ⅳ 맺는 말

사이버테러법 제정의 긴급성을 감안할 때, 19대 국회처리가 꼭 필요하다. 입법절차상 국회의장의 직권상정 외에는 현실적으로 동법 통과가 불가능한 상태이다. 3월 11일 새누리당 단독으로 임시국회를 소집한 상황인바, 여야 합의에 의한 통과가 가장 바람직하지만 현실적으로 어렵다. 따라서 이번 임시국회 회기 통과를 추진해야 한다. 동 법안의 문제점도 있으나, 이는 차기국회에서 여야 합의에 의해 개정하면 될 문제이다.

다만 19대 국회에서 동 법안이 통과되지 못했을 때, 20대 국회에서 처리해야 할 것이다. 그러나 그 사이에 사이버테러가 발생했을 시 19대 국회는 사이버테러의 방조자, 비호자라는 역사적 책임에서 자유롭지 못할 것이다. 직권상정에 의한 사이버테러방지법 통과가 절실하다.

국가 사이버테러 방지 등에 관한 법률안
(서상기의원 대표발의)

의 안 번 호	18583

발의연월일 : 2016. 2. 22.

발 의 자 : 서상기・강석훈・김도읍・김용남・김정훈・김종태문정림・박대동・박민식・박성호・신동우・신의진・심윤조・원유철・이명수・이상일・이재영・이종배이철우・조원진・홍철호・황영철・황인자・황진하 의원(24인)

제안이유

과거 1·25 인터넷 대란과 같은 전국적인 규모의 국가 주요 정보통신망 마비사태 발생과 해외로부터 조직적인 사이버테러로 국가기밀 및 첨단기술의 유출 등 국가·사회 전반에 중대한 영향을 미칠 수 있는 사이버위기 발생 가능성이 날로 증대하고 있음.

특히 사이버공간은 국경을 초월하여 범지구적이면서 정부와 민간부분이 상호 밀접히 연계되어 있어 매우 복잡·고도화되며, 시공간의 제약을 벗어나 발생하는 모든 사이버공격을 정부와 민간 어느 하나도 단독으로 차단하기에는 분명한 한계가 있음.

그러나 우리나라는 아직 국가차원에서 사이버테러 방지 및 위기관리업무를 체계적으로 수행할 수 있는 제도와 구체적 방법·절차가 정립되어 있지 않아 사이버위기 발생 시 국가안보와 국익에 중대한 위험과 막대한 손해를 끼칠 우려가 있음.

따라서 정부와 민간이 참여한 국가차원의 종합적인 대응체계를 구축하도록 하고, 이를 통하여 사이버테러를 사전에 탐지하여 사이버위기 발생 가능성을 조기에 차단하며, 위기 발생 시 국가의 역량을 결집하여 신속히 대응할 수 있도록 하고자 함.

주요내용

가. 사이버테러에 대한 국가차원의 종합적이고 체계적인 예방·대응과 사이버위기관리를 위하여 국가정보원장 소속으로 국가사이버안전센터를 둠(안 제6조).

나. 책임기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응할 수 있는 보안관제센터를 구축·운영하거나 다른 기관이나 보안관제전문업체가 구축·운영하는 보안관제센터에 그 업무를 위탁하여야 함(안 제8조).

다. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 장 및 중앙행정기관의 장은 사이버테러로 인해 피해가 발생한 경우에는 신속하게 사고조사를 실시하고, 중앙행정기관의 장은 그 조사결과를 미래창조과학부장관, 국가정보원장 및 금융위원장 등 관계 중앙행정기관의 장에게 통보하여야 함(안 제9조).

라. 정부는 사이버테러에 대한 체계적인 대비와 대응을 위하여 책임기관의 장의 요청과 수집된 정보를 종합·판단하여 관심·주의·경계·심각 단계의 사이버위기경보를 발령할 수 있음(안 제10조).

마. 정부는 경계단계 이상의 사이버위기경보가 발령된 경우 원인분석, 사고조사, 긴급대응, 피해복구 등의 신속한 조치를 취하기 위하여 국가 역량을 결집한 민·관·군 전문가가 참여하는 사이버위기대책본부를 구성·운영할 수 있음(안 제11조).

바. 정부는 사이버테러 기도에 관한 정보를 제공하거나 사이버테러를 가한 자를 신고한 자 등에 대하여 포상금을 지급할 수 있음(안 제13조).

사. 직무상 비밀을 누설한 경우에는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하고, 피해의 복구 및 확산방지를 이행하지 아니한 경우에는 1천만원 이하의 과태료에 처할 수 있음(안 제14조 및 제15조).

법률 제 호

국가 사이버테러 방지 등에 관한 법률안

제1조(목적) 이 법은 국가 사이버테러 방지에 관한 기본적인 사항을 규정하여 국가안보를 위협하는 사이버테러를 예방하고 사이버위기 발생 시 국가 역량을 결집하여 신속하게 대처함으로써 국가의 안전보장과 이익보호에 이바지함을 목적으로 한다.

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

1. “사이버테러”란 외국이나 대한민국의 통치권이 사실상 미치지 아니하는 한반도 내의 집단, 해킹·범죄조직 및 이들과 연계되거나 후원을 받는 자 등이 국가안보 또는 공공의 안전을 위태롭게 할 목적으로 해킹·컴퓨터 바이러스·서비스방해·전자기파 등 전자적 수단에 의하여 정보통신망을 공격하는 행위를 말한다.
2. “사이버안전”이란 사이버테러로부터 정보통신시설과 정보를 보호하기 위하여 수행하는 관리적·물리적·기술적 수단 및 대응조치 등을 포함한 활동으로서 사이버위기관리를 포함한다.
3. “사이버위기”란 사이버테러로 인하여 국가 기반시설의 핵심기능이 훼손·정지·무력화 또는 국가기밀과 중요정보가 대량 유출되어 국가안보에 영향을 미치거나 사회·경제적 혼란을 유발하는 상황을 말한다.
4. “사이버테러정보”란 정보시스템 및 정보보호시스템(소프트웨어를 포함한다) 등에 의해 사이버테러 행위로 판단되는 정보로서 사이버테러 근원지를 파악하기 위한 인터넷프로토콜주소(IP)와 네트워크카드주소(MAC)를 포함한다.
5. “사이버테러 방지 및 위기관리 책임기관(이하 “책임기관”이라 한다)”이란 사이버테러 방지 및 위기관리에 관한 업무를 수행하고 있는 다음 각 목의 기관을 말한다.
   가. 「대한민국헌법」, 「정부조직법」, 그 밖의 법령에 따라 설치된 국가기관(그 소속·산하기관을 포함한다)과 지방자치단체(그 소속·산하기관을 포함한다) 및 「국가정보화 기본법」 제3조제10호에 따른 공공기관
   나. 「정보통신기반 보호법」 제5조제1항에 따른 주요정보통신기반시설을 관리하는 기관
   다. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제46조제1항에 따른

집적정보통신시설사업자 및 같은 법 제47조의4제2항에 따른 주요정보통신서비스 제공자

라. 「산업기술의 유출방지 및 보호에 관한 법률」 제9조에 따른 국가핵심기술을 보유한 기업체나 연구기관

마. 「방위사업법」 제3조제9호에 따른 방위산업체 및 같은 법 제3조제10호에 따른 전문연구기관

6. "사이버테러 방지 및 위기관리 지원기관(이하 "지원기관"이라 한다)"이란 사이버테러에 대한 신속한 탐지·대응 및 사고조사·복구 등을 지원하는 다음 각 목의 기관 또는 업체를 말한다.

가. 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조에 따른 한국전자통신연구원

나. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 한국인터넷진흥원

다. 「소프트웨어산업 진흥법」 제24조에 따라 소프트웨어사업자로 신고한 자 중 컴퓨터바이러스 백신소프트웨어를 제작 또는 판매하는 자

라. 「국가정보화 기본법」 제3조제6호의 정보보호시스템을 제작하거나 수입하는 자

마. 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호 전문서비스 기업

바. 관계 행정기관의 장이 지정한 보안관제전문업체

제3조(사이버안전관리의 책임) ① 책임기관의 장 및 이를 지휘·감독할 의무가 있는 기관의 장은 사이버안전관리에 대한 책임을 진다.

② 책임기관의 장은 소관 정보통신망에 대한 보안대책을 마련하는 등 사이버안전관리를 위해 자율보안관리 체계를 구축·운영하여야 한다.

제4조(국가사이버테러 방지 및 위기관리 기본계획 수립 등) ① 정부는 사이버테러 방지 및 위기관리 대책의 효율적이고 체계적인 추진을 위하여 국가사이버테러 방지 및 위기관리 기본계획(이하 "기본계획"이라한다)을 수립·시행하여야 한다.

② 국회, 법원, 헌법재판소, 중앙선거관리위원회의 장(국회사무총장, 법원행정처장, 헌법재판소 사무처장, 중앙선거관리위원회 사무총장을 말한다. 이하 같다) 및 중앙행정기관의 장은 제1항의 기본계획에 따라 소관 책임기관의 장이 활용할 수 있도

록 국가사이버테러 방지 및 위기관리 시행계획(이하 “시행계획”이라고 한다)을 작성하여 소관 책임기관의 장에게 배포하여야 한다.

제5조(시행계획의 이행여부 확인) ① 국회, 법원, 헌법재판소, 중앙선거관리위원회의 장 및 중앙행정기관의 장은 소관 책임기관에 대하여 매년 시행계획의 이행여부를 확인하여야 한다.

② 정부는 제1항의 확인결과를 종합하여 국가사이버테러 방지 및 위기관리 실태를 점검·평가하여야 한다. 다만, 국회, 법원, 헌법재판소, 중앙선거관리위원회에 대한 점검·평가는 해당기관의 장이 요청한 경우에 한정한다.

③ 제1항 및 제2항의 절차와 방법 등에 관하여 필요한 사항은 대통령령으로 정한다.

제6조(국가사이버안전센터의 설치) ① 사이버테러에 대한 국가차원의 종합적이고 체계적인 예방·대응과 사이버위기관리를 위하여 국가정보원장 소속으로 국가사이버안전센터(이하 “안전센터”라 한다)를 둔다.

② 안전센터는 다음 각 호의 업무를 수행한다.

1. 국가사이버테러 방지 및 위기관리 정책의 수립
2. 사이버테러 관련 정보의 수집·분석·전파
3. 사이버테러로 인하여 발생한 사고의 조사 및 복구 지원

③ 국가정보원장은 제1항의 안전센터를 운영함에 있어 국가차원의 종합판단, 상황관제, 위협요인 분석, 사고 조사 등을 위해 민·관·군 합동대응팀(이하 “합동대응팀”이라 한다)을 설치·운영할 수 있다.

④ 국가정보원장은 합동대응팀을 설치·운영하기 위하여 필요한 경우에는 책임기관 및 지원기관의 장에게 인력의 파견과 장비의 지원을 요청할 수 있다.

제7조(사이버테러 방지대책의 수립·시행) ① 책임기관의 장은 소관 정보통신망과 정보 등의 안전성 및 신뢰성 확보를 위한 사이버테러 방지대책을 강구하여야 한다.

② 국가정보원장은 관계 중앙행정기관의 장과 협의하여 제1항에 따른 사이버테러 방지대책의 수립에 필요한 지침을 작성 배포할 수 있다. 다만, 국회, 법원, 헌법재판소 및 중앙선거관리위원회의 경우에는 해당 기관의 장이 필요하다고 인정하는 경우에 적용한다.

제8조(보안관제센터 등의 설치) ① 책임기관의 장은 사이버테러 정보를 탐지·분석하여 즉시 대응 조치를 할 수 있는 기구(이하 “보안관제센터”라 한다)를 구축·운영

하거나 다음 각 호의 기관이 구축·운영하는 보안관제센터에 그 업무를 위탁하여야 한다. 다만, 「정보통신기반 보호법」 제16조에 따른 정보공유·분석센터는 보안관제센터로 본다.

1. 제2조제5호가목의 기관
2. 제2조제6호바목의 보안관제전문업체

② 책임기관의 장은 제1항에 따른 사이버테러 정보와 정보통신망·소프트웨어의 취약점 등의 정보(이하 "사이버위협정보"라 한다)를 관계 중앙행정기관의 장 및 국가정보원장과 공유하여야 한다.

③ 정부는 제2항의 사이버위협정보의 효율적인 관리 및 활용을 위하여 관계기관의 장과 공동으로 사이버위협정보통합공유체계를 구축·운영할 수 있다.

④ 누구든지 제2항에 따라 공유하는 정보에 대하여는 사이버위기관리를 위하여 필요한 업무범위에 한하여 정당하게 사용 관리하여야 한다.

⑤ 제1항에 따른 보안관제센터와 제3항에 따른 사이버위협정보통합공유체계 구축·운영 및 정보 관리에 관한 사항과 제2항에 따른 사이버위협정보의 공유에 관한 범위·절차·방법 등에 관한 사항은 대통령령으로 정한다.

제9조(사고조사) ① 국회, 법원, 헌법재판소, 중앙선거관리위원회의 장 및 중앙행정기관의 장은 사이버테러로 인하여 소관분야에 피해가 발생한 경우에는 그 원인과 피해내용 등에 관하여 신속히 사고조사를 실시하여야 한다. 또한, 중앙행정기관의 장은 그 조사결과를 미래창조과학부장관, 국가정보원장 및 금융위원장 등 관계 중앙행정기관의 장에게 통보하여야 한다.

② 제1항의 경우 피해가 중대하거나 확산될 우려가 있는 경우 중앙행정기관의 장은 즉시 미래창조과학부장관, 국가정보원장 및 금융위원장 등 대통령령으로 정하는 전문기관의 장에게 사고조사 등 기술적 지원을 요청할 수 있다. 다만, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 해당기관의 장이 필요하다고 인정하는 경우에 한한다.

③ 미래창조과학부장관, 국가정보원장 및 금융위원장 등 관계 중앙행정기관의 장은 제1항에 따라 사고조사 결과를 통보받거나 제2항에 따라 기술적 지원을 한 결과, 피해의 복구 및 확산방지를 위하여 신속한 시정이 필요하다고 판단되는 경우 책임기관의 장에게 필요한 조치를 요청할 수 있다. 이 경우 책임기관의 장은 특별한 사유가 없는 한 이에 따라야 한다.

④ 누구든지 제1항 및 제2항에 따른 사고조사를 완료하기 전에 사이버테러와 관련된 자료를 임의로 삭제·훼손·변조하여서는 아니 된다.

제10조(사이버위기경보의 발령) ① 정부는 사이버테러에 대한 체계적인 대비와 대응을 위하여 책임기관의 장의 요청과 제8조제2항에 따라 수집된 정보를 종합·판단하여 관심·주의·경계·심각 단계의 사이버위기경보를 발령할 수 있다. 이 경우 국가안보실장과 미리 협의하여야 한다.

② 정부는 제1항의 사이버위기경보를 발령할 경우 관계기관의 장과 경보 수준을 사전 협의하여야 한다.

③ 책임기관의 장은 제1항에 따른 사이버위기경보가 발령된 경우 즉시 피해발생의 최소화 및 피해복구를 위한 조치를 취하여야 한다.

④ 사이버위기경보 발령의 주체·절차·기준 및 책임기관의 장의 조치 등에 관하여 필요한 사항은 대통령령으로 정한다.

제11조(사이버위기대책본부의 구성) ① 정부는 경계단계 이상의 사이버위기경보가 발령된 경우 원인분석, 사고조사, 긴급대응, 피해복구 등의 신속한 조치를 취하기 위하여 국가 역량을 결집한 민·관·군 전문가가 참여하는 사이버위기대책본부(이하 "대책본부"라 한다)를 구성·운영할 수 있다.

② 대책본부의 장(이하 "대책본부장"이라 한다)은 관계 중앙행정기관의 장이 국가안보실장과 협의하여 정하고, 대책본부의 구성·운영 등에 관하여 필요한 사항은 대책본부장이 관계 중앙행정기관의 장과 협의하여 정한다.

③ 대책본부장은 제1항에 따른 대책본부를 구성·운영하기 위하여 책임기관 및 지원기관의 장에게 필요한 인력의 파견 및 장비의 제공을 요청할 수 있다.

제12조(비밀 엄수의 의무) 이 법에 따라 사이버테러 방지 및 위기관리 업무에 종사하거나 종사하였던 자는 그 직무상 알게 된 비밀을 타인에게 누설하거나 직무상 목적 외에 이를 사용하여서는 아니 된다.

제13조(포상 등) ① 정부는 사이버테러 방지 및 위기관리와 관련하여 다음 각 호의 어느 하나에 해당하는 자에 대하여 포상하고, 예산의 범위에서 포상금을 지급할 수 있다.

1. 사이버테러 기도에 관한 정보를 제공한 자
2. 사이버테러를 가한 자를 신고한 자
3. 사이버테러의 탐지 및 대응·복구에 공이 많은 자

② 제1항에 따른 포상과 포상금 지급의 기준·방법과 절차, 구체적인 지급액 등 필요한 사항은 대통령령으로 정한다.

제14조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

1. 제8조제2항 및 제4항을 위반한 자
2. 제9조제4항을 위반한 자
3. 제12조를 위반한 자

② 업무상 과실로 인하여 제1항의 죄를 범한 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

제15조(과태료) ① 제9조제3항을 위반한 자는 1천만원 이하의 과태료에 처한다.

② 제1항에 따른 과태료는 대통령령이 정하는 바에 따라 관계 중앙행정기관의 장이 부과·징수한다.

부 칙

이 법은 공포한 날부터 시행한다.

토 론 문

사이버테러방지법 토론

한 희 원

동국대 법대 교수, 한국국가정보학회장

토 론 문

사이버테러방지법 토론

동국대학교 법과대학 학장 한희원 (한국국가정보학회 회장)

1 세계는 사이버 전쟁 - 제5의 전장

- 총성 없는 '제5의 전장' 지구촌 사이버 군비경쟁
- 월스트리트저널(WSJ) 보도 '디지털 무기' 각축전 보도
- "최소 29개국 군 · 정보기구 보유", 미국 사이버사령부 · NSA '최강'
- 중국은 '피싱' · 러시아는 '해킹', 적 · 아군 따로 없이 공격 강행

사이버전 주요 당사국과 활동(추정) 자료: 〈월스트리트저널〉

미국	군 사이버사령부에서 작전. 외국 네트워크에 악성 프로그램 심음
러시아	해킹 도구 개발에 능숙. 미국 국방부 · 국무부 · 백악관 침투
중국	육군 사이버 부대가 피싱 전문. 미국 첨단 스텔스 전투기(F-35) 계획 빼냄
이란	사우디 아람코와 라스베이거스 샌즈 컴퓨터 파괴. 미국 은행 공격 부인
북한	소니픽처스 해킹으로 이메일 등 유출

2 북한의 대남 사이버 공작

○ **핵공격의 원칙**

- 전통적: 상호확증파괴(mutual assured destruction)
- 미국의 대북핵정책: 일방적 확증파괴

○ **사이버 공격 탈린 매뉴얼의 대원칙: 상호확증의심**

- 북한의 대남 사이버 공격: 사이버 반달리즘

○ **북한의 사이버테러 담당 인력: 약 6000여 명**

- 실제 작전에 투입되는 정예요원: 약 1700여 명

○ **북한의 정보기구(공작기구)는 누구를 상대로 하려고 만들어졌는가?**

- 외형적 평화는 암흑세계에서의 소리 없는 만행

3 사이버테러방지법 제정의 방향성

가. 국가 사이버테러방지 등에 관한 법률(안) 개관

제1조(목적)

제3조(사이버안전관리의 책임)

제4조(국가사이버테러방지 및 위기관리 기본계획 수립 등))

제5조(시행계획의 이행여부 확인)

제6조(국가사이버안전센터의 설치)

제7조(사이버테러방지대책의 수립 · 시행)

제8조(보안관제센터 등의 설치)

제9조(사고조사)

제10조(사이버위기경보의 발령)

제11조(사이버위기대책본부의 구성)

나. 평가: 현실은 사이버 전쟁 그런데 추진 입법은 과연 이를 뒷받침하는가?

다. 현실적 필요수단과 합법적 사이버 정보활동

(1) 사이버테러방지법의 기본이념

(2) 영역의 파괴와 확장

4 외국 입법례와 교훈

가. 중국의 반테러법과 국가안전법

나. 미국의 교훈

토 론 문

주요국의 사이버테러 대응 실태 고찰

김 철 우
한국국방연구원 연구위원

토 론 문

주요국의 사이버테러 대응 실태 고찰

김철우 (한국국방연구원 연구위원)

1 주요국 사이버테러 대응 추세

▲ **기본인식 :** 사이버 공간을 국가안보의 최전선으로 인식(안보현장)!

- **선제적 대응 개념 : 사이버 테러 발생 이후의 사후 대응 방식 탈피**
  * 헌법이 보장하는 기본권(사생활 보호) 가치와 상충되는 요인을 인정하지만 사이버 감시까지 허용하면서 법적 장치 마련 및 정보기관의 대응역량 강화 조치
- **테러 발생 사후 반응적(Reaction) ⇨ 선제적(Proactive) 활동으로 전환**
  * 사건 발생 이후 대응할 수 없을 규모의 막대한 폐해 때문에 미연에 차단
  예) 자살폭탄테러범 : 테러 이후 대처 방식으로는 억제효과 자체가 성립하지 못함
- **충격적 테러 사건 이후 조치 : (미국 9/11, 영국런던 지하철, 프랑스 파리테러)**
  ① 감시기능 증강(Increasing Surveillance)
  ② 정보역량 첨예화(Sharpening Intelligence)
  ③ 불법자금 옥죄기(Cutting off illicit Financial Flows)
  ④ 정보공유 증진(Enhancing Intelligence Sharing with allies)
- **정보기관의 선제적 활동 긴요 (AUMF에 의한 군사적 대응은 한계)**
  * Authorization for the Use of Military Force, 사이버전 역량 강화

* 정보통신기술 발전 ⇨ 사이버 환경자체가 끊임없이 진화하는 사이버위협 (Advanced Persistent Threat) 양상에 비해 법적 뒷받침 미흡

☞ 주요국들은 국가안보 차원에서 사이버 안보전략 정립 ⇨ 법적·제도적 뒷받침 및 전문 인력을 양성하고 대응 시스템 혁신을 지속적으로 추진

▲ 사이버 안보 위협의 주요 특성

- 범죄, 테러, 심리전, 전쟁양상이 혼재하여 구분이 불명확한 특성
- 국가차원의 '컨트롤 타워' 기능이 필수적이며 정보기관 기능과 융합
- 국가기반시설 공격은 전쟁행위로 간주하여 자위권 정당화하는 추세 (사이버테러에 대응 범위와 수준, 권리행사 주체 등 국제적 공감대 미흡)
- 공격용 악성코드, 전자폭탄 등 사이버무기 개발에 박차, 비밀조직까지 운용

2 미국의 사이버 위협 대처 역량 강화

▲ 주요조치 경과

- 1996년 클린턴 대통령행정명령: '국가 기반구조 및 경제 기반시설을 보호'에 착수, 1998년 5월 대통령훈령(PDD 63)으로 '국가기반구조보호센터(PCCIP)'를 설치
- 1999년 국가기반시설보호센터(NIPC) 및 주요기반시설보증국(CIAO) 설치 운용
- 2001년 9/11 테러 이후 2003년 3월 국토안보부(DHS)가 신설, 사이버안보 구축
- 국방부는 2005년 12월 사이버공간에 대한 작전개념을 정립하고 구체적 조치
- **2008 국토안보부(DHS) 산하에 국가사이버안보센터(National Cyber Security Center) 설치하여 범정부차원에서 사이버안보 기능을 총괄**
- 2009년 1월 백악관이 사이버안보를 조정 통제 (2009년 사이버안보 보좌관을 신설 등)
- **2009년 5월 '사이버공간 정책 검토(Cyberspace Policy Review)'** 보고서 발표

* 사이버안보 기본전략서이며 국가안보차원의 기본 방향을 제시(특히 기술력 강조)

- 2009년 국방부, 국토안보부와 '사이버 스톰(Cyber Storm)' 명칭으로 사이버보안훈련 실시
- 2009년 6월 사이버사령부(USCYBERCOM) 창설, NSA 국장 겸임(현재 Rogers 해군제독)
- 2010년 4월 '국가 사이버보안 교육 이니셔티브(NICE)' 발족 : 전문인력 집중 양성
- 2011년 7월 '사이버 공간에서의 국방부 운용전략 (Department of Defense Strategy for Operating in Cyberspace)' 발표: 새로운 작전영역(operational domain)으로 천명
- 2011년 8월 '국가 사이버안보 마스터플랜' 발표

※ 예산 긴축와중에도 사이버안보 예산은 지속적으로 증액(수년간 전년대비 20% 증가)

▲ 사이버안보 주요 입법 조치

- 미국 의회 : 사이버안보 법률 제정 또는 개정하는 입법조치를 전향적으로 추진
- 주요 법적근거 : 컴퓨터보안법,[15] 국토안보법,[16] 애국법(USA Patriot Act),[17] 사이버보안강화법,[18] 해외정보감시법,[19] 등 다차원적 법적 근거 확충

15) 컴퓨터보안법(Computer Security Act)는 1987년에 제정되어 미국표준기술연구소(National Institute of Standards and Technology)를 중심으로 컴퓨터보안 관련된 사항을 규정하고 있다.

16) 국토안보법(Homeland Security Act)은 2002년도에 각종 테러로부터 미국의 국가기반을 보호하기 위해 제정되었다. 사이버보안에 관한 규정은 총 17개장 중 제2장(정보분석 및 기반시설 보호) 및 제 10장(정보보호)에 제시되어 있다.

17) 2001년 9.11테러 직후에 제정된 법률로서 통신감청을 포함한 각종 테러위협 수사권을 포괄적으로 보장해 주고 있다. 컴퓨터 해커에 관한 형량까지 규정하는 등 사이버테러의 억제와 처벌의 법적 근거를 제공하고 있다.

18) 사이버보안강화법(Cyber Security Enhancement Act)은 2002년에 국토안보법에 포함되어 제정되었다. 사이버공격에 대한 상세한 처벌 근거를 규정하고 있다.

19) 해외정보감시법(Foreign Intelligence Surveillance Act)는 1978년에 제정되어 해외정보 수집 차원의 감청 권한을 인정하는 조항을 포함하고 있다.

- The Electronic Communications and Privacy Act of 1986(ECPA)
  * 전자감시를 규정한 대표적 법률 : 도청 및 감청을 컴퓨터, 인터넷, 이메일 등 전자통신으로 확장
- 1987년 컴퓨터보안법(Computer Security Act) 제정
- 1996년 국가정보기반보호법(National Information Infrastructure Protection Act) 법제화
  * 국가정보기반 무단침입과 손해야기를 연방범죄로 취급: 형사처벌 근거 조항 마련
- 1987년에 제정된 **외국정보감시법(Foreign Intelligence Surveillance Act) 보완 개정**
  * 1994년 개정하여 보안수사에 관련된 물리적 잠입수사 허용,
  * 1998년 전화이용 기록 및 추적 명령을 법제화
  * 9.11테러 이후 외국정부 첩보요원에 대한 전자적 감청, 도청까지 허용
- **애국법(Patriot Act)을 통해 수사권한의 대폭 확대**
  * 국가안보범죄 또는 테러범죄의 혐의를 받는 사람들의 통신을 차단 권한 부여
  * 영장없는 전자감시를 허용하는 긴급조항 및 테러용의자에 대한 행정구금까지 허용
  * 추가적으로 온라인과 컴퓨터와 관련된 전자감시 근거법 확보
  * 테러차단과 방지에 필요한 적절한 수단의 제공에 의한 미국의 통합 및 강화법(Uniting and Strengthening America b Providing Appropriate Tools Required to Intercept and Obstructing Terrorism Act of 2001).
- The Communications Assistance for Law Enforcement Act(CALEA)
- 2010년 5월 '연방정보보안관리법(Federal Information Security Management Act)' 개정
  * 2002년 제정된 FISMA의 연방정보 및 정보시스템 보안강화 조치 부가
- 2010년 사이버보안 법안(Cyber Security Act) 보완, 강화

* 강력한 통신중단 조치 권한을 대통령에게 부여

- 2013년 3월 회계연도 예산법안에 연방정부의 중국산 정보기술제품 구매금지 조항 포함

* 장비제조 단계에서부터 악성코드 삽입하여 필요시 작동시킬 가능성 원천적으로 차단

- **2015년 2월 국가안보전략(NSS) 발표 :** 사이버안보 위협을 핵심적 대응기조로 재천명

▲ 법적 근거에 의한 대표적 수사사례

- 2014년 5월, 연방수사국(FBI), 중국 인민해방군 산하 61398부대 장교 5명을 자국 기업을 상대로 한 해킹 및 사이버 스파이 행위로 기소

* 2006년부터 중국의 군사정보 시설을 이용하여 미국의 원자력, 철강, 태양에너지 분야 관련 기업을 해킹한 혐의로 기소하여 외국군 관계자를 기소한 첫 사례(미국이 이례적 공개하여 심리적 압박을 가하는 효과를 겨냥)

- 2013년 6월 국가안보국(NSA) 출신 에드워드 스노든(Edward Snowden)이 사이버감청 PRISM 실태 폭로하여 세계 각국은 물론 자국내 사이버감청 문제에 대한 논란 증폭

* 자국민 통화기록 및 인터넷 정보 수집: 해외정보감시법(FISA)을 법적 근거로 제시

- 2014년 12월 FBI, 소니영화사 해킹사건의 배후로 북한 지목, 제제조치 및 인터넷 불통 조치

3 주요국 사이버 안보 역량 강화 동향

가. 중국

▲ 주요 조치

- 사이버안보전략 미공개상태나 사이버전을 위한 '새로운 형태의 전투력'을 개발 시인
- 국가안전부, 공안부, 국가보밀국, 인터넷 경찰, **중국침해사고 대응센터(CN-CERT) 등이 있으며 국가안전부가 국가차원의 사이버안보 조직을 총괄**하는 역할을 담당
- 중국군이 '사이버 공간에서의 국가안보 이익 수호'를 공개적으로 언급하며 사이버 및 우주공간에서 괄목할 수준으로 군사능력을 강화
- 2000년 2월 '인터넷 기초총부'로 지칭하는 사이버전 부대(Net-Force)를 창설
- 2011년 5월 광저우 군구 : 사이버전 부대를 창설하는 등 군구별 사이버전 역량 확충
- 인터넷 검열시스템 '만리방화벽(Great Firewall of China)' 구축
- 인민해방군에 전문해커 매년 약 5만 명을 양성하는 것 추정되고 있음. 사이버전 관련 인원은 정부, 민간 IT 산업, 학계의 정보민병 등을 40만명 포함하여 '홍커(red hacker)'로 지칭되는 100만 명에 이르는 민간 해커들이 활동 중

▲ 주요 입법 조치

- 2000년 10월 제15차 중국공산당 중앙위원회 제5차 전체회의부터 인터넷에 대한 법적 규제는 엄격하게 통제하며 **사이버공간의 질서 유지를 명분으로 각종 통제 합법화**
  * 중국은 Chinanet를 통한 일괄접속 방식 채택, 국가인트라넷 방식으로 인터넷 통제

- **주요 법률 :** '중화인민공화국 인민경찰법', '전국인민대회 상무위원회의 인터넷 보안 유지에 관한 결정', '컴퓨터정보시스템 보안보호 조례' 등
- 2014년 10월, 중국 중앙군사위원회는 시진핑 국가주석이 '군 정보보안 강화안'을 승인

* 사이버시스템 보안조치를 위해 자국산 제품 사용 조치(외국 업체 제품 제외 조치)

나. 일본

▲ 주요 대응 조치

- 2000년 1월 정부기관의 웹사이트가 중국 해커들에 의해 해킹당한 이후 다각적 조치
- 자위대는 2000년 10월 사이버 테러 대응 조직을 창설
- 2005년 4월 내각관방 국가정보보안센터(National Information Security Center)가 국가차원 총괄조직 역할 ⇨ 국민생활 보호, 국제협력 증진, 법률 시스템 조치를 전담
- 2006년 정보보안정책회의(Information Security Policy Council)에서 'Information Security Strategy for Protecting the Nation'을 발표
- 2008년 육해공 자위대가 참여한 상설 통합부대로서 '지휘통신시스템대' 창설
- 2010년에 사이버기획조정관을 신설
- 2013년 3월 방위성에 '사이버방위대' 발족하여 자위대 방위 ⇨ 국가기반시설 보호로 영역 확대
- 2013년 5월 도쿄에서 '미 · 일 제1회 사이버대화' 개시, 제2차 대화는 워싱턴에서 개최하며 미국과 긴밀한 공조체제 유지하며 EU, 이스라엘 등과 사이버안보 관련 국제공조에 주력

▲ 주요 입법 조치

- 사이버안보 관련 주요 법률로는 전기통신사업법,[20] IT기본법,[21] 등 법적기반

구축

- ASEAN 국가 등 세계 각국에 진출한 기업 피해발생 범죄수사를 위한 국제 공제 활성화

다. 러시아

▲ 주요 대응조치

- 연방보안부(FSB), 정보보안센터(ISC), 연방정부통신정보부(FAPSI) 등이 중추적 역할

*** FSB 산하 정보보안센터가 사이버보안에 대한 총괄기능을 담당**

- 2002년 세계 최초로 해커부대를 창설 : 해커들을 고용해 사이버 공격에 활용

* 2007년 에스토니아에 대한 사이버 공격의 배후로 지목되었음

* 2008년 11월 러시아 해커가 미군의 네트워크 시스템에 바이러스 침투시키는데 성공

- 2008년 그루지아를 대상으로 전면적인 사이버전 공격
- 사이버 무기 자국 시스템 구축을 위해 지속적으로 연구

▲ 주요 입법 조치

- 2006년 7월에 발효된 '정보, 정보기술 및 정보보호법(149-f3호)' 제정

* 자국의 정보자산에 대한 보안유지를 위해 러시아 기술진에 의해 시스템 개발

- 연방보안국(FSB)이 사이버안보 관련 예방 및 범죄수사권 행사

* 민간영역에 대한 수사권도 광범위하게 인정

---

20) 1984년 12월에 제정되어 2006년 6월 개정되어 전기통신 서비스 관련 공공복리 증진 차원의 이익보호에 관한 법률이다.

21) 공식명칭은 '고도 정보통신 네트워크 사회형성 기본법'으로서 2001년 1월에 제정되었으며 사이버안전 및 신뢰성에 관한 제반 사항을 규정하고 있다.

라. 영국

▲ 주요 대응조치

- 국가안보 차원에서 대테러와 사이버안보 대응체계 확립에 우선적 가치를 부여
- 국가차원의 사이버대응센터 '퓨전셀(Fusion Cell)' 구축하여 정부와 민간이 공동 대응
  * 정보통신본부(GCHQ)가 언론계까지 사이버감청 활동
- 내무부 보안정보부(MI5) 산하 국가기반보호센터(CPNI),[22] 외무부 산하 정보통신본부(GCHQ), 통신전자보안단(CESG) 등이 역할 분담
- 2009년 사이버안보국(Office of Cyber Security and Information Assurance) 및 사이버안보작전센터(Cyber Security Operations Centre)를 설립
  * OCS는 정부차원의 전략적 지도력과 응집력을 제공, CSOC는 운용적 차원에서 사이버 공간을 모니터 하면서 즉각적 대응조치
- 2010년에 공표한 'The National Security Strategy'에 사이버안보 대응 방향을 천명
  * 사이버 공간에서의 안보적 도전요인을 신속하게 대처
- 정보기관들이 사이버안보 첩보 및 정보 수집을 강화하여 선제적 대응

▲ 주요 입법 조치

- 조사권한규제법(RIPA),[23] 컴퓨터부정사용법,[24] 대테러범죄 및 안전보장법,[25]

---

22) 국가기반보호센터(Center for the Protection of National Infrastructure)는 2007년 2월에 창설되어 국가보안국(MI5) 국장이 Security Service Act(1989)에 따라 지휘한다. CPNI는 영국의 국가 기간망에 대한 보안자문, 테러위협 차단 등의 기능을 담당하며 다수의 정부부처와 기관이 공조하는 시스템으로 구성되어 물리적 보안과 사이버 보안을 융합하는 기능을 수행한다.

23) 조사권한규제법(Regulation of Investigatory Powers Act)은 2000년도에 제정되어 통신감청, 인터넷 및 컴퓨터 관련 모니터 관련 법적권한을 영국경찰에게 부여하는 근거를 규정하고 있다.

24) 컴퓨터부정사용법(Computer Misuse Act)는 1990년에 제정되어 비인가자에 의해 컴퓨터 접속을 금지하고 해킹방지 및 구체적 처벌조항도 제시하고 있다.

25) 대테러 범죄 및 안전보장법(Anti-terrorism, Crime and Security Act)는 2001년에 제정되어 각종 테러행위 대응에 필요한 사항을 폭넓게 규정하고 있다. 동법에 전화, 인터넷, 우편 등 통신테이터 보안조치를 위한 조항이

* RIPA는 영장없이 경찰이나 당국이 전화통화기록이나 인터넷 정보 등을 수집 허용

- Terrorism Act 2006 : 종합적인 테러방지법

마. 독일

▲ 주요 대응조치

- 1991년 설립된 내무부 산하 '연방정보기술안전청(BSI)'이 사이버안전 업무를 총괄[26)]
- 2011년 2월 연방정부 내무부가 'Cyber Security Strategy for Germany' 발표
- 사이버안보를 위해서 필요시 무력사용을 포함한 자위권 발동에 대한 논거를 제시
- 사이버안보의 주체가 민간을 중심으로 이루어져야 하고 군대는 보완적 기능을 담당
- 국가사이버대응센터(National Cyber Response Centre) 설치하여 컨트롤타워 기능 수행
- 독일군은 2010년에 창설된 해커부대를 모체로 2011년 1월 '사이버 국방센터'를 신설
- 총리실 주관 '국가사이버보안위원회(National Cyber Security Council)' 정책 조정기능

▲ 법적 장치 발달

- 정보통신법(TKG), 연방정보기술안전청설치법 등을 통해 사이버안보를 뒷받침
- 유럽의 '사이버 범죄 협약(Cyber Crime Convention)'에 따라 사이버 범죄 수사
- 제네바협약, 헤이그 협약 등 기존 전쟁조약의 사이버 공간에서 위상 논의 지속

포함되어 있다.

26) BSI(Bundesamt fur Sicherheit in der Informationstecchnik)는 정보보호, 보안인증, 사이버테러 감시, 정보보안 기술 등에 관한 활동을 한다.

4 주요국 사이버안보 대응 시사점

▲ 주요국의 대응조치 방향

① 국가차원의 사이버 총괄조직 창설(재편),

② 군차원의 사이버전 부대 통합(창설),

③ 사이버 범죄 관련 법제 보강

④ 사이버 전사 및 전문인력 양성 등

※ 국가안보전략 차원의 총체적 접근

▲ 교훈으로 삼아야 할 포인트

- 2003년 1월 인터넷 대란을 겪고 난 후 사이버 안전에 대한 대응조치가 국가안보차원에서 착수되었지만 후속 법제화 조치 미진

*** '국가 사이버안보 종합대책' 발표(2013년 7월)**

- 주요국들은 국가안보 차원의 **자위권 개념에 따라 사이버공격의 역량 강화**

* 국내법 정비를 마치고 국제법적 근거 확보를 위한 논리개발과 국제공조를 활성화

- 북한의 대남사이버 테러 및 국내외 조직의 사이버안보 도전 : **법적 뒷받침 긴요**

* 우리나라는 IT강국임을 자부하지만 사이버안보 수사와 관련된 분야는 취약점 많음

※ 세계 각국은 **사이버전을 국가안보의 핵심적 도전으로 인식**

* 2015년 9월 중국의 시진핑 국가주석이 미국을 방문하여 오바마 대통령과 정상회담 과정에서도 사이버전을 둘러싸고 날카로운 공방

5 북한의 사이버테러 위협 고찰

▲ 단순한 해킹 수준 ⇨ **사이버테러, 사이버심리전, 사이버간첩활동 등 끊임없이 진화**

* 사이버테러 위협은 국가마비 및 사회혼란 획책: 스마트폰 해킹 도발
* 한수원 원자력, 서울메트로, 철도기관 서버와 같이 국가기반 인프라까지 겨냥

▲ 북한의 핵미사일 위협 공세 + **사이버전 도발과 복합되어 나타날 것으로 예상**

▲ **북한 사이버 인프라의 특징**

- 인터넷과 인트라넷을 철저히 분리하여 이중화
  * 1996년 9월 북한체제 내부에서만 사용하는 국가단위 인트라넷을 구축
  * 인트라넷은 일반기관/주민용 '광명', 국가보위부용 '방패', 인민보안성용 '붉은검', 군부용 '금별' 등 차단의 원칙에 입각한 시스템.
- 정보통신 인프라를 국가차원에서 독점하여 철저히 통제
  * 외부의 침해를 방지하기 위해 방화벽 프로그램 '능라', 백신 프로그램 '클락새' 및 '주작', 전화통신 암호화 장비 '청송과 번개', 접근통제 솔루션인 '보검' 등을 개발하여 보안대책을 강구
  * 개인용 PC는 인터넷 접속장치가 제거되며 전기사정 악화로 PC 사용 시간도 제한
- 광통신망 회선은 단둥과 신의주를 잇는 '차이나 텔레콤'사의 회선을 할당 받아서 중국의 IP를 통해 이용
  * 인터넷 필터링 정책에 의해서 걸러진 콘텐츠에만 접속, 일부 무선 인터넷 접속은 독일서버에 위성 접속하여 이루어지고 있는데 이는 외신기자 등 극소수 인원에 한정
- 중국의 선양, 다롄, 베이징, 칭다오 등에서 위장 취업하면서 사이버전사로 활동
  * 선양이 북한 해커 조직의 핵심 근거지

★ **정찰총국 산하에 사이버 전담부대들이 편성**되어 사이버테러를 주도

* "북한이 7개 해킹 조직에 1,700여명 규모의 전문해커를 보유하고 있으며 프로그램 개발 등 해킹지원 세력은 13개 조직 4,200여명에 달한다"고 국회 정보위원회에 보고

* 통일전선부 산하의 사이버 조직(204호)은 사이버심리전을 중심으로 활동

6 결론 및 제언

▲ **사이버 테러 수법이 점점 '지능화 · 고도화 · 특정화'되면서 진화**하는 추세

▲ 사이버 위협 대처를 위한 **법제화 조치가 극히 미진**한 상태[27]

▲ **사이버안보 수사와 관련된 분야**도 취약

- 스테가노그라피 등 사이버공간을 이용한 간첩교신(왕재산간첩단)[28]

▲ 사이버테러는 당면한 안보위협 ⇨ **사이버테러 방지를 위한 법률 제정 시급**

---

27) 2015년 6월 산업발전 토대 마련을 위해 정보보호산업진흥법을 제정되었으나, 사이버테러방지법 등 사이버안보에 관한 기본법이 아직 제정되지 못하고 국회에 계류되어 있는 상황이다. 현재는 대통령 훈령 '국가사이버안전관리규정', '정보통신기반보호법' 등에 한정되어 국가차원의 체계적인 대응에 결정적 제한요인이 되고 있다.

28) 2011년 7월 지하당 '왕재산' 간첩사건에 대한 수사결과, 왕재산 핵심지도부는 북한의 255국으로부터 지령을 받고 군 작전계획, 컴퓨터 암호화 기술 등을 북한에 보고했다. 사이버안보와 관련된 주요한 특징은 '신문기사로 위장한 최첨단 프로그램(스테가노그라피)를 간첩통신에 활용하는 등' 첨단공작 기법으로 수사기관의 추적을 회피해 왔다.

토 론 문

사이버테러방지법 제정 촉구 간담회

박 춘 식

서울여대 교수, 전 국가보안기술연구소장

토 론 문

사이버테러방지법 제정 촉구 간담회

박춘식 (서울여자대학교 정보보호학과)

1 최근 북한 사이버테러 도발 양상과 유형 전망

- 2009, 2011(농협 등), 2013(KBS 등), 2014(한수원, 미국 소니픽쳐스 해킹 등), 2016년 청와대 사칭 이 메일 유포 등 북한발 해킹(경찰청 라오닝 IP 등)
- 빙산일각/성동격서/사이버공격에 필요한 우리나라 공격목표 관련 다량의 정보 사전 수집(전화번호 등 개인정보, 관련 정보 등)
- 강경파 김영철 통일전선부장 전면 등장: 북한발 사이버테러 총괄 총괄국장, 천안함/연평도 포격사건, 미국 소니픽쳐스사 해킹 관여 추정
- 북한발 월평균 100여건 정도가 300여건으로 최근 사이버 공격 급증 추정되며 2013년 사이버 테러 발생 전초전 분위기 유사한 급박한 분위기
- 대북제재 회피를 위한 사이버 게임 머니, 도박사이트, 취약성 정도 매매 등 금융권 해킹(피싱, 랜섬웨어 등)을 통한 외화벌이 강화 예상
- 국내 정보보호 기업 취약점 이용(코드서명 등) 해킹 시도(악성코드 감염 등) 및 한미훈련동향 파악 스마트 폰 해킹, 서울지하철, 코레일 등 철도
- 불특정다수에서 특정 및 목표지향적, 정보수집 및 탈취 형태에서 기반시설 파괴 및 한미협력 탐지 수단으로 단순 공격에서 심리전 병행 등 특징 보임
- 사이버 테러는 사이버 간첩, 사이버 심리전 등 복합적이며 동시 다발적 발생 예상

2 사이버테러방지법 제정의 긴급성과 정당성

- 현대 테러는 물리적 공간과 사이버 공간을 모두 활용하여 발생하며(테러 정보 수집, 테러 계획 수립 및 작전 지시, 명령 등 모두 첨단 IT 기술 및 사이버 공간 활용) 사이버 공간을 통한 사이버 테러가 물리적 공간에서 시스템 마비 및 주요 시설 파괴로 나타남
- 사이버 공격은 북한의 3대 보검 전략(핵, 미사일, 사이버공격)이며 경제성 및 기대효과 우수, 원점타격 회피 및 역추적 공격, 국제 제재 수단 없음 등의 사유로 북한이 공격할 가장 가능성이 높은 수단
- 사이버 심리전 등을 통하여 정부 불신, 남남 갈등, 후방 교란 및 전복 획책 등 사회적 혼란 야기 수단으로 북한 적극 활용
- 우리나라는 IT 의존도가 아주 높고 수준 높지 않은 북한 사이버 공격에도 쉽게 큰 혼란에 빠질 수 있으며 전력, 철도, 통신, 금융 등 국가주요시설이 공격 대상이 되기 쉬우며 피해 규모 막대
- 북한발 사이버 위협은 안보 차원의 문제이며 정부 단독으로 대응하기에는 역부족이며 민관합동으로 대응해야 하며 효율적 대응을 위한 국가 차원의 사이버 위기 관리를 위한 제도 수립 시급함
- 국가정보원의 사이버안전센터는 실무 총괄 수행 중이나 법령 미흡으로 효율적 역할 수행 한계 봉착
- 기존 정보보호 법률은 일상적인 정보보호 활동 관련 법령으로 산재되어 있어 북한 사이버 공격을 대응하기에는 역부족
- 첨단화되고 집요하고 목표지향적이며 파괴적인 북한발 사이버 공격에 대응하기 위해서는 수십년간 대응한 전문조직 및 경험 보유 그리고 북한 해커 인적 정보 수집 가능한 국가정보원을 중심으로 정부 종합 체계적인 사이버 위협 대응을 위한 법 제정으로 국가안전 및 이익 그리고 국민의 생명 보호 필요

3 사이버테러방지법((서상기안)의 문제점과 보완 사항

- 사이버 테러 용어 정의를 행위 주체 및 목적 등을 명시한 명확한 용어로 보완
- 국정원 권한 집중을 국정원장에서 정부로 변경, 국정원 역할을 국가안보실로 수정(경보발령을 국가안보실과 협의하여 발령 등)
- 사고조사 통보 및 기술지원기관을 국정원에서 미래부, 금융위, 국정원으로 변경 등
- 각급기관 책임 부여 및 소재 명확화 그리고 헌법기관도 자체 계획 수립과 이행 추가

4 사이버테러방지법 입법 전략

- 국정원 권한 남용과 인권침해 등은 법 조항에 존재하지 않으나 야당의 우려를 고려하여 국회 정보위 상설화, 국정원장의 역할을 정부로 표현하는 등 정부안으로 추진
- 정부 수정안에 대하여 여야 정보위 소위 간담회 등 조속 개최 최종 합의 추진
- 현재 야당이 신청한 안건조정위원회(90일계류 및 위원회 미 구성)를 통해서는 19대 통과 불가 판단
- 19대 국회 통과될 수 있도록 국회의장 직권만이 유일한 전략으로 판단되므로 법 제정의 시급성과 정당성 등을 홍보하고 야당의 이해 촉구 활동 등 필요

토 론 문

국가사이버테러방지법 제정의 필요성

제 성 호

중앙대 법학전문대학원 교수

토 론 문

국가사이버테러방지법 제정의 필요성

제성호 (중앙대 법학전문대학원 교수)

1 최근 북한의 사이버테러 실태

ㅇ2010년대에 들어와 농협전산망 마비(2011.4.), 서울메트로(2014.9), 한수원(2014.12) 해킹 등 북한에 의한 대남 사이버테러가 빈번하게 자행되고 있음.

ㅇ특히 금년 2월 북한의 해킹조직원들이 하루 18시간씩 한국과 미국 · 아시아 등을 대상으로 10배 정도의 고강도 공격을 자행한 것으로 알려지고 있음.

- 현재 북한은 사이버 인력으로 6,000여명을 확보하고 있고, 이 중 1,700여명은 핵심 작전요원이라고 함.

ㅇ또한 북한의 4차 핵실험(2016.1.6) 및 장거리 미사일 광명성 발사(2016.2.7) 후 북한은 우리의 외교안보부처 고위급 인사들 간 의 스마트폰 통화, 이메일 등을 해킹하기 위해 다양한 형태의 사이버 공격을 하고 있음.

ㅇ이처럼 정권 차원에서 조직적으로 전개되는 북한의 사이버테러는 막대한 경제적 피해는 물론 사회 혼란 및 국가안보를 위협하는 심각한 상황을 초래하고 있는 상황임.

2 사이버테러방지법 제정의 당위성

가. 국가 차원의 사이버테러 방지를 위한 통합법의 필요성

ㅇ북한의 사이버공격에 대한 정부의 대응활동이 「국가사이버안전관리규정」(대통령훈령)에 근거해 실시되고 있는 것이 현실임.

- 그런데 이 규정은 국가 · 공공기관(즉 공무원)에만 적용됨으로써 민간부문에 대해서는 구속력이 없음.
- 따라서 민간 부문과의 정보공유가 어려운 것은 말할 것도 없고, 민간분야에서 발생하는 사이버테러 징후를 사전 탐지 · 차단하거나 대책을 강구하는데 한계가 있음.
- 또한 민간기업은 보안 취약요소가 발견되더라도 비용부담 · 기술부족 등으로 신속한 보호조치를 하지 않아 피해가 반복적으로 발생하는 양상을 노정하고 있음.

ㅇ이러한 점에 비추어 공무원만 구속하는 행정명령이 아니라 정부, 기업, 국민 모두에게 적용되고 이들이 보유하고 있는 기반시설을 보호하는 명실공히 '국가' 차원의 사이버테러방지법의 제정이 절실함.

- 그럴 때 정부와 민간이 함께 협력하여 국가차원에서 사이버테러 예방 및 사이버위기 대응업무를 체계적이고 일사분란하게 수행할 수 있을 것임.

나. 사이버테러 방지행정과 법치주의의 요구

ㅇ사이버테러의 심각성, 특히 국민경제 및 안보 등에 미치는 영향 등을 감안할 때 사이버테러 방지 행정은 매우 중요한 국가행정작용임.

ㅇ이 같은 행정은 법률에 따라 이루어져야 한다는 것이 법치주의의 요구이자 법치행정의 원칙이라고 할 수 있음.

ㅇ이런 시각에서 볼 때 국회가 사이버테러방지 활동을 대통령훈령으로 대처하라고 하고 입법을 해태(懈怠)하는 것은 직무유기라고 할 만함.

ㅇ국회는 법을 제정하고 관계기관에 대해 법에 근거한 권한을 행사토록 하고 그에 따른 응분의 책임을 묻는 구조를 만드는 것이 민주국가의 올바른 국회상이라고 할 것임.

ㅇ이와 관련, 미국 · 독일 · 일본 등 주요 선진국들도 사이버테러 위협의 심각성을 인식하고 사이버안보 관련 법률을 제정·실시하고 있음.

- 미국의 「사이버안보법」(2015.12)
- 독일의 「IT-보안법」(2015.6),
- 일본의 「사이버시큐리티기본법」(2014.11) 등

3 사이버테러방지법 제정 시 기대효과

ㅇ우선, 민 · 관 · 군이 참여하는 국가 차원의 사이버위협 합동대응팀, 사고대책본부 및 위협정보공유체계를 구축 · 운영할 수 있음.

ㅇ사이버테러 탐지 · 대응 및 사고조사 · 복구 등에 백신업체, 정보보호시스템 제작자 등 민간기관의 지원 · 협조 등 참여가 가능함으로써 사이버테러에 대한 방지활동의 실효성이 제고될 수 있음.

ㅇ나아가 그동안 사이버테러 예방의 사각지대였던 국회, 법원, 헌법재판소, 선거관리위원회 등 헌법기관에게 자체 사이버테러 예방 및 점검활동의 책임을 부과할 수 있음.

ㅇ또한 책임기관 및 지휘 · 감독기관에게 사이버안전관리 책임을 부여하고 자체 보안대책 마련 등을 의무화함으로써, 각 기관들이 자체적인 보안관리 체계를

구축 · 운영토록 할 수 있음.

- 뿐만 아니라 신속한 사이버테러 대응이 가능하도록 책임기관에게 보안관제센터를 운영하거나 다른 기관 또는 보안관제업체에 위탁하도록 의무화할 수도 있음.

4 국정원 권한 강화 등 법제정 반대론 비판

ㅇ북한 등의 사이버테러를 예방 · 대응하는 업무는 국가안보와 직결된 사항으로, 「정부조직법」(국가안보 관련 정보 · 보안 업무)과 「국가정보원법」(국내외 보안정보 수집, 기밀 문서 · 시설 보호)에 따른 국정원의 고유 임무기능임

ㅇ이러한 국정원의 사이버안보 관련 임무 · 기능은 국가정보원법, 전자정부법, 정보통신기반보호법 등에서 이미 구체적으로 명시하고 있음.

- 국정원법상 국외 정보 및 국내 보안정보의 수집 · 작성 · 배포(법 제3조 제1항 제1호), 국가기밀에 속하는 문서 · 자재 · 시설 및 지역에 대한 보안업무(제2호)
- 전자정부법상 행정기관 정보통신망 보안대책 수립 · 지원 및 이행여부 확인(제56조)
- 정보통신기반보호법상 공공분야 기반시설 보호정책 수립, 보호대책 이행여부 확인, 신규지정 권고 및 보호기술 지원 등 실시(제5조의2, 제7조 등)

ㅇ따라서 동법에 규정된 사이버테러 정보의 수집 · 분석이나 사이버테러 예방 · 대응에 관한 사항들은 국정원의 기존 직무범위를 초과하는 것이 아니며 또한 국정원에게 새로운 권한을 부여하는 것이 아님.

- 이미 노무현 정부 때인 2006년부터 국가사이버테러 방지업무를 수행하여 왔으며,
- 기존부터 국정원법 등에 따라 행사해 오던 권한을 통합법률 에 의해 제도화하는 것이라고 볼 수 있음.

ㅇ한편 정부는 사이버위기 경보 발령시, 관계중앙행정기관은 사고대책본부장 임명시 사이버안보 컨트롤타워인 국가안보실과 협의하여 정하도록 하고 있음.

- 전술한 바와 같이 국가사이버테러방지법은 국정원이 정보통신기반보호법, 전자정부법등 각종 법령에 따라 이미 수행중인 업무를 반영하고 있고, 민간부문의 경우에는 대책수립, 이행여부 확인, 위협정보 수집, 사고조사 등 업무 대부분을 미래부 · 금융위와 관계 중앙행정기관이 수행토록 규정하고 있음.

ㅇ요컨대 국가사이버테러방지법의 제정으로 국정원의 권한이 강화되는 것이라기보다는 오히려 법률 주관기관으로서의 '책임'이 강화되는 것으로 이해함이 타당하다고 할 것임.

- 국정원은 법률 주관기관일 뿐 관계 중앙행정기관에 대해 일방적으로 명령·지시하는 컨트롤타워가 아님.

ㅇ이 밖에도 정보통신망법(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」)과 기반보호법(「정보통신기반보호법」)으로 충분하며 국가사이버테러방지법이 불필요하다는 견해가 있지만, 여기에 동의하기 어려움.

- 정보통신망법과 기반보호법은 각각 민간 분야 사업자와 기반시설로 지정된 시설에 한정 적용되며, 규율하는 내용과 방법, 절차가 모두 상이함.
- 또한 정보통신망법은 정보통신서비스 제공자나 집적정보통신시설 사업자 등 민간의 정보통신 관련 업체와 이들 서비스 이용자의 정보보호에 관한 사항만을 규율하고 있음.
- 기반보호법(「정보통신기반보호법」)은 주요정보통신기반시설로 지정된 시설(현재 385개)에 대해서만 제한 적용되고 있음.

ㅇ또한 상기 법률 이외에도 공공분야에는 국정원법, 전자정부법 및 국가사이버안전관리규정이, 국방분야에는 국방정보화법이, 그리고 금융 분야에는 전자금융거래법이 각각 적용됨으로써, 상이한 방법과 절차를 통해 사이버테러 위협에 대응하고 있음.

- 이들 법률들은 소관 영역의 특수성을 고려하여 각기 보호대책을 마련하고 있

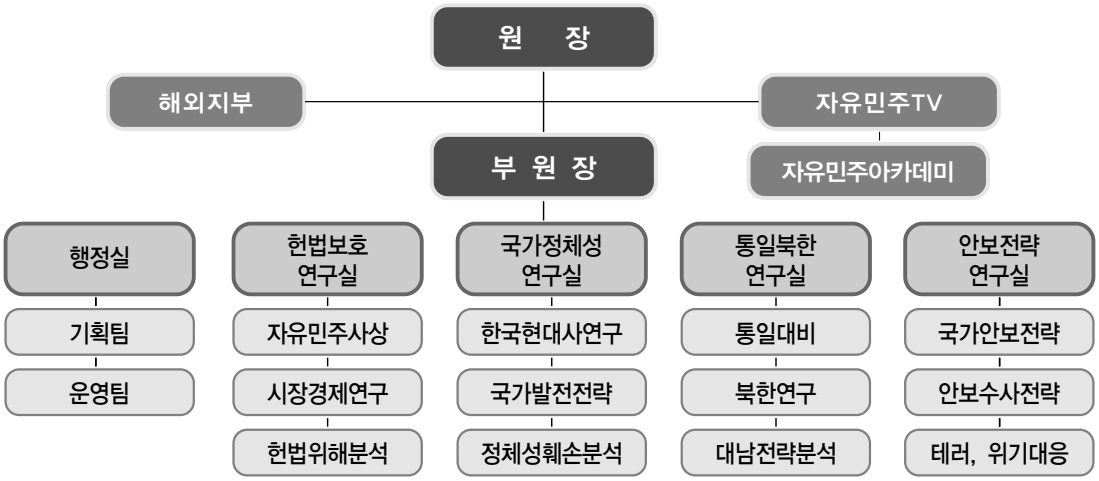
으나 개별 영역을 뛰어넘어 국가 차원의 사이버위협 정보를 공유하고 사이버 공격을 탐지·대응할 수 있는 체계를 규정하고 있지 않음.

- 그러므로 안보와 국익을 위협하는 사이버위협에 국가 차원에서 효과적이고 종합적으로 대응하기 위해서는 사이버테러방지법 제정이 절실하다고 할 것임.

• 자유민주연구원 소개

자유민주연구원은 헌법 정신에 기초하여 대한민국의 자유민주주의체제를 수호·발전시키기 위한 제반 전략을 학술적으로 연구, 전파하는 것을 목적으로 2014년 3월3일 설립되었으며, 국세기본법상 '수익사업을 하지 않는 비영리법인'(법인으로 보는 단체)으로 2014년 3월 27일 등록하였습니다.

▸ 자유민주연구원 조직과 사람들



▸ 자유민주연구원 고문

이철승(서울평화상 이사장, 전 신민당 대표최고위원, 7선 국회의원), 정기승(변호사, 전 대법관), 안응모(전 내무부장관), 이동복(전 국회의원), 최대권(서울대 법대 명예교수), 송대성(전 세종연구소장), 김현욱(국제외교안보포럼 대표, 전 민주평통 수석부의장, 4선 국회의원)

▸ 자유민주연구원 정책자문위원

고영주(위원장)(변호사, 국가정상화추진위원장, 전 서울남부지검장), 고성진(덕우회장, 전 안기부 대공수사실장), 김길자(대한민국 사랑회 회장, 전 경인여대 총장), 김성만(예비역 해군중장, 전 해군작전사령관), 김석우(통일준비위원회 위원, 전 통일원 차관), 김영수(서강대 교수, 전 서강대 부총장), 김혁수(예비역 해군준장, 전 해군잠수함 전단장), 권영철(전 국정원 국장), 류석춘(연세대 사회학과 교수, 연세대 이승만연구원장), 박광작(전 성균관대 교수(경제학)), 안충준(전 3사단장, 초대 PKO 사령관), 박정이(예비역 육군대장, 전 1군사령관), 안영섭(전 명지대교수), 양동안(한국학중앙연구원 명예교수), 여영무(전 동아일보 논설위원), 유호열(고려대 교수, 코리아정책원장), 이봉엽(예비역 육군소장, 전 기무사 참모장), 이병진(경우회 부회장, 전 경찰청 보안국장, 경북경찰청장), 이주영(뉴데일리 이승만연구원장, 전 건국대 부총장), 조용연(삼성에스원 상임감사, 전 경찰청 보안국장, 충남경찰청장), 전경만(한국국가정보학회장, 전 통일부 통일교육원장), 정순영(세종대 석좌교수, 전 부산동명대 총장), 한광덕(전 국방대학원장, 5사단장), 서석구(변호사, 전 판사)

▸ 자유민주연구원 정책연구위원 – 헌법보호연구실

장영수(고려대 법학전문대학원 교수 – 헌법수호, 발전), 김상겸(동국대 법대학장 – 헌법수호, 발전), 권혁철(자유경제원센터장 – 자유시장경제), 함귀용(변호사, 전 대검공안연구관–헌법위해상황), 백병훈(T뉴스미디어그룹 부회장)

▸ 자유민주연구원 정책연구위원 – 국가정체성연구실

유광호(연세대 연구교수), 이주천(원광대 교수 – 현대사 훼손), 김광동(나라정책원장 – 국가발전전략), 강규형(명지대 기록대학원 교수 – 교육, 현대사), 이동호(자유민주연구학회 사무총장 – 종북문제), 김진술(북앤피플 대표 – 문화예술), 권유미(블루유니온 대표 – 인터넷), 장원재(방송인, 전 숭실대 교수 – 언론, 미디어)

▸ 자유민주연구원 정책연구위원 – 통일북한연구실

실장 강석승(서울교대 겸임교수, 전 민주평통 운영위 간사, 전 통일부 과장 – 남북대화), 김정봉(한동대 교수, 전 국가안보전략연구소장 – 북한정치, 군사), 조영기(고려대 북한학과 교수 – 북한경제), 임상철(상지대 교수 – 북한사회 농업), 이백규(변호사 김앤장), 전 서울고법 판사 – 북한법제), 유동열(자유민주연구원장 – 대남전략), 제성호(중앙대 교수, 통일준비위원회 위원 – 일대비), 황윤덕(전 국정원 단장 – 통일대비, 통일정세, 국제정치), 최봉수(단국대 교수 – 통일대비), 정병윤(전 국가정보대학원 교수)

▸ 자유민주연구원 정책연구위원 – 안보전략연구실

실장 문순보(전 세종연구소 연구위원), 김용석(군사문제연구원 연구위원 – 국방안보전략), 김철우(한국국방연구원 연구위원 (군사전략), 정찬권(한국위기관리연구소 연구위원 – 국가위기대응), 박춘식(서울여대 교수, 전 국가보안기술연구소장 – 사이버안보), 정준현(단국대 법대 교수 – 사이버안보), 박노형(고려대 법학전문대학원 교수 – 해외안보법제), 허태회(선문대 교수, 전 국정원 전문위원 – 테러), 성시웅(변호사, 전 부천지청장, 대검 공안연구관 – 안보수사), 김원환(전 안기부 대공수사단장 – 안보수사), 김재권(전 경찰대 교수 – 보안수사 담당 – 안보수사), 이덕기(전 기무사 방첩단장 – 안보수사), 조춘성(박사), 구정환(박사), 김수민(연구원)

▸ 해외지부

미국 동부지부 원장 민경원(미주애국연대 의장)
미국 시카고지부(준비위)
미국 L.A.지부 원장 김봉건(자유대한민국지키기 국민운동본부 회장)
미국 오렌지카운티 지부 원장 JOY 안(대한민국애국동포총연합회 회장)
유럽지부 준비위원장 김정록(재향군인회 영국지회장)

▸ 자유민주연구원 정책연구위원 – 자유민주아카데미

• MEMO •

• MEMO •

• MEMO •

• MEMO •