2016 겨울 | 제 1권 2호(통권189호)

ISSN 2508-2728

신안보연구

The Studies of New Security Challenges

국가안보전략연구원
Institute for National Security Strategy

2016 겨울 I 제 1권 2호(통권189호)

ISSN 2508-2728

신안보연구

The Studies of New Security Challenges

국가안보전략연구원
Institute for National Security Strategy

신안보연구

2016년 겨울 | 통권 189호

발행처: 사단법인 국가안보전략연구원
발행인: 신 언
주 소: 서울특별시 강남구 언주로 120
인스토피아 B/D 13-18층
전 화: (02)572-7090, FAX:(02)572-3303
E-mail: policy@inss.re.kr

인쇄일: 2016년 12월 15일
발행일: 2016년 12월 30일

* 국가안보전략연구원은 2016년부터 『정책연구』를 『신안보연구』로 제호를 변경해서 연속 발행합니다. 본지에 실린 내용은 집필자 개인의 견해이며 본 연구원의 공식입장이 아닙니다.

Contents 신안보연구
2016 겨울 | 통권 189호

Ⅳ 신안보 요소로서의 재난 개념의 변화와 법 제도적 함의

이창주 (성균관대학교)

Ⅴ 온라인 뉴스 기반 국가안보 이슈 변화 분석

이영환 (건국대학교) **김찬우** (영남대학교)

Ⅵ 글로벌 기후변화 대응을 위한 차세대 지구관측위성 탑재체 획득 방안

은종원 (남서울대학교)

I

중국내 테러 발생 요인의 다양화와 그 대응

곽덕환 (한남대학교)

Summary

중국에서 전통적으로 테러를 유발하는 요인은 분리주의라고 말할 수 있지만, 최근 경제 성장 결과 이루어진 부의 분배가 불공정하게 이루어짐에 따라 또 다른 갈등 요인이 발생되었고 이것이 테러 유발 요인이 되고 있다. 그 해결 방법으로 소수 민족 간에 대화 강화가 제시되고 부패 방지 등 그 불만 해소 방안도 검토되는 한편, 테러 발생 시 대처 능력을 제고하기 위한 훈련과 테러 관련법을 새롭게 정비해야 하는 필요성도 논의되고 있다.

최근 국제 테러 빈발로 인해 중국도 그들의 국익과 국민의 안전이 위협받고 있다. 중국은 그 대책으로써 국제 공조를 강화하며, 국제 연합과 지역 조직들과의 긴밀한 협력을 기하고 있다. 특히 “일대일로” 사업의 원만한 수행을 위해서 중동 과격 테러 단체들의 억제는 필수적인 과제로 대두되고 있다. 약자의 투쟁 수단인 테러는 근본적인 동기가 불평등이기 때문에 이 문제를 직시하여 해결하지 않고는 세계 평화를 이룰 수 없다고 본다.

| **키워드** | 테러, 분리주의, 부패방지, 불평등

1. 서론

테러라는 용어는 “거대한 공포”라는 라틴어에서 기원하며, 그 정의는 정치적 반대파를 진압하기 위해 억압과 폭력을 사용하여 상대를 공포에 빠뜨리게 하는 행위라고 일컬어지고 있다. 그렇지만, 공격을 받는 국가의 입장에서 본다면 테러리즘은 공포를 확산시키기 위해 폭력을 계획적으로 사용하거나 폭력을 행사하겠다는 위협을 통해 정부 또는 사회를 굴복시키거나 협박하는 것 혹은 정치적, 종교적, 이데올로기적 행동 방침을 실행할 목적으로 개인의 목숨 또는 재산에 대해 치명적인 폭력을 사용하거나 위협하는 것이다.[1)]

이것은 약자가 강자에게 정상적인 방법으로 대항하기 어려운 상황이기 때문에 자신의 희생을 무릅쓰고 그 억울함을 다른 사람에게 알리고 그 상대에게 피해를 주려는 행위라고 볼 수 있다. 그러나 이런 억울함을 호소한다는 다소 긍정적인 면이 있다하더라도 일반적으로 테러리즘은 상식의 논리에서 일탈하는 것으로 정당화 될 수 없을 뿐만 아니라 잔혹하고 영혼이 결여된 광기라고 평가되고 있다.[2)] 테러리즘이 정치적 조류와 행위로 주목받기 시작한 것은 20세기 60년 대 후반에 스페인, 북아일랜드와 중동 지역 폭력사건이 빈발하면서 부터이다. 학자들이 테러에 대해 본격적으로 연구하기 시작한 것은 2001년 9·11테러 이후 이다.[3)]

그동안 중국학자들은 이러한 테러리즘이 하나의 정치사상적 사조(思潮)인지 아니면 범죄 행위인지에 대한 의견이 일치하지 않았다. 테러리즘을 정치적 사조로 보는 측면에서는 테러의 시도는 다른 정치적 경향이나 이해득실에서 유발되지만, 테러의 폭력과 전쟁에서의 폭력은 그 의미가 다르지만 겹치는 부분도 있다고 보았다. 범죄 측면으로 본다면 테러는 다음과 같은 죄를 추가해야 된다고 주장되는데 첫째는 공공질서 위해(危害) 죄이고, 둘째는 재산 파괴 죄이며, 셋째는 인질납

1) 찰스 타운센드 저, 심승우 역『테러리즘, 누군가의 해방투쟁』, (서울: 한겨레출판사, 2002), p.12.
2) 찰스 타운센드 저, 심승우 역(2002), p.9.
3) 潘志平,「中國對恐怖主義的研究述評」,『國際政治研究』, 제3期, (北京: 北京大學, 2011), p.100.

치 죄, 넷째 불법위험물질 우편 취급 죄, 다섯째 특별감면 규정의 분별력있는 적용 등이라 말할 수 있다.[4]

일반적으로 테러리즘의 근원으로 종족주의, 민족분열주의, 종교의 극단주의를 들 수 있다.[5] 중국에는 신장(新疆)분열 투쟁에서 일어난 "동투르키스탄(東突)"문제가 이러한 종족주의를 근거로 한족에 항거하고 그들의 종교인 이슬람교를 신봉하고 전파하려 한다는 면에서 가장 두드러진 특징을 지니고 있다고 볼 수 있다. 중국은 2001년 9.11테러 발생 직전까지 특별한 반응을 하지 않고 자신들은 평화를 추구하는 국가이며 파괴적 테러행위를 비판한다는 원론적 언급을 해왔을 뿐 국제적 테러 대응에 소극적인 태도를 취해 왔었다. 그 이유는 자국 내에서 발생하는 소수민족의 분규나 소요, 분리운동 혹은 종교집단의 시위는 내정의 일부분이라 보았기 때문이다.[6]

그러다가 9.11테러 발생 직후 중국정부는 불특정 다수 민간인들을 대상으로 하는 반인륜적인 테러행위에 반대한다고 하며 매우 적극적으로 비난하는 태도로 나왔다.[7] 이러한 태도 전환은 물론 미국과 충돌보다는 협력이라는 중국 정부의 전략적 고려에서 나온 것임에도 불구하고 중국도 과거 전통적으로 민족분규가 테러를 유발하는 주된 요인에 더하여 이제는 경제 발전에 따른 경제 분규와 종교적 갈등도 두드러지고 있는 상황을 고려한 것으로 해석할 수 있을 것이다.

이 글은 중국의 테러를 유발시키는 요소들과 중국의 사회발전과 국력 증대에 따라 새롭게 등장하는 요소들을 분석하고, 중국이 대외 개방 정책을 펼치면서 상대적으로 안보 취약 가능성이 증대하고 전 세계적으로 분규와 갈등이 증가하면서 새로운 대테러 대응 전략을 어떻게 전개하려 하였는지를 논의할 것이다.

---

4) 潘志平, 앞의 글, p.103.
5) 潘志平, 앞의 글, p.109.
6) 김상호, "2009년 7월 신강테러와 중국정부의 대응," 『대테러 연구』, 33집(2010), p.109.
7) 테러는 세계 평화와 안정에 대해 중대한 위협이고, 어떤 형태의 테러에도 단호하게 반대한다고 밝혔다. 이동률, "9.11테러와 중국의 갈등과 선택," 『당대비평』(2001), p.203.

2. 사회 변화와 테러의 다양화

덩샤오핑(鄧小平)의 개혁개방 정책이래 자본주의 생산방식 도입으로 인해 중국 경제에서 사적영역이 증대되면서 이제는 갈등의 원인이 단순히 이데올로기 갈등이나 민족분규의 발생 뿐 만아니라 사회, 경제적 불만에서 나오는 갈등 대립형 부문까지 확대되고 있는 상황이다. 테러방법도 다양화되면서 독극물테러나 병원체 테러, 인터넷테러 등도 발생하고 있다. 전통적 민족분규와 더불어 과거와는 다른 새로운 비전통적 분규에 따른 테러요인이 증대되고 있어 중국 사회내의 위협과 위기 역시 커지고 있는 상황이라고 볼 수 있다.

가. 분리주의

일반적으로 테러 행위는 정치적 목적을 가지고 있는데, 첫째가 민족의 분리, 분립, 분열, 종교 극단주의 혹은 극단적으로 정부나 사회에 반대한다는 면에서 일반적인 범죄와 성격이 다르다고 말할 수 있고, 조직적으로 폭력을 사용하고 위협하며, 이를 통해 그 주장과 의도를 특정 사회집단에 전달한다는 면에서 형사범죄와 다르다.

일반적으로 테러의 대상은 관공서, 경찰서 등과 같은 경성 목표와 불특정 다수 시민을 목표로 하는 연성 목표를 하고 있다.[8] 또한 테러리즘은 피해의 대상이 비무장인원이나 민간인이며 부녀자, 노인, 아동들도 가리지 않기 때문에 그 잔혹함이 심하고, 대규모일 가능성이 높다. 더 나아가 이런 이유 때문에 많은 국민들의 주목 대상이 되면서 자신들의 주장을 보다 용이하게 정부에게 전달하여 압력을 가할 수 있는 특징을 가지고 있다.[9]

중국에서 전통적 테러유발 요인으로써 가장 두드러진 것은 역시 신장지역에서의 분리주의, 극단주의 움직임이라고 말할 수 있을 것이다. 크게 범 이슬람주의와

8) 이대성, 김태진, "중국의 테러리즘 분석과 그 전망," 『한국콘텐츠학회논문지』, 제14권 9호(2014), p. 221.
9) 潘志巍, 『中國政府應對恐怖主義的危機管理研究』(上海: 華東師範大學, 2005), p.10.

범 투르쿠주의가 그것이라고 볼 수 있다. 최근 십여 년간 260여 테러사건이 발생하여, 160여명이 죽고, 440여명이 부상을 당하였다.[10] 중국경찰에서 파악하기로는 이들은 이미 국제테러조직인 탈레반 조직과도 연관되어 있다고 알려지고 있다.

이들 테러 세력은 그들의 목적을 쉽게 달성하기 위하여 그들의 운동 중에 폭력적 요소를 약화시키고, 국제조직과의 연계를 강화시키며, 타 조직과의 유대를 강화하면서 이데올로기와 극단적 민족주의 요소를 강화시키고 있다고 분석되고 있다.[11] 더 나아가서 중국 최대 소수민족인 장족(藏族)과도 연계하며 식량과 무기 문제에 있어 상호지원을 모색하는 협의를 진행하고 있는 것으로 파악되고 있다. 또 다른 분리세력인 달라이(達賴)집단과도 협력을 모색하고 있는데, 달라이 세력은 20세기 70년대 초 6만 정도의 인구로 국가를 세워 활동하고 있었다. 초기에는 주된 구성원이 유망 장족 출신들이었는데, 자신들의 장족의 문화와 독립에는 별 관심이 없다가 나중에 시장(西藏) 지역에 개입하여 시장 청년세력을 조직하고, 시장 독립을 주목표로 활약하고 있는 것으로 분석되고 있다.

타이완 독립을 도모하는 타이완 독립세력(臺獨)도 역시 중국 분리주의의 하나의 세력으로 볼 수 있을 것이며, 중국정부는 이러한 대만독립주의에 대항하여 2005년에 "반국가분열법(反國家分裂法)"을 제정하여 대항하고 있다. 중국 정부의 입장에서 볼 때 타이완 독립 세력은 극단적으로 중국 대륙에 폭력을 행사하려는 테러 세력의 하나이다.

나. 갈등형 테러 증가

물질문명의 발달에 따라 많은 사람들이 물질의 지나친 추구로 인해 인간관계가 냉담해지고, 심지어는 정신적으로도 공허감이 심해지면서 반사회적, 반인도적, 사교조직이 형성되고 그에 따른 테러가 빈번하게 발생한다, 대표적인 예가 사교 집단인 파룬공(法輪功)의 출현이라고 볼 수 있다.[12] 다른 사례로는 2001년 허난핑

10) 黃金成, "論中國面臨的恐怖主義威脅," 『法制與社會』(云南: 云南省法學會, 2009), p.210.
11) 黃金成(2009), p.211.
12) 이들은 물론 국제테러 활동이 빈번하게 발생한 것에 영향을 받았지만, 교주 이홍즈(李洪

(河南平)의 컴퓨터 게임방에서 중학생 17명이 살해당하는 사건이 발생하였고, 스지아좡(石家庄)지역에서 폭탄테러가 발생하였으며, 2002년에서 다리엔(大連)에서는 비행기 납치사건이 있었고, 2003년 베이징대, 칭화대에서 폭탄 폭발사건이 있었다. 2008년에는 쿤밍(昆明)에서 대중버스 폭발사건이 있었고, 술집에서 폭탄 폭발사건도 발생하였다.

이러한 테러 발생은 중국 사회 전환기에서 구성원 서로 간 모순과 대립이 극단적으로 나타나는 현상이라고 설명할 수 있다. 또한 이러한 현상은 경제가 발전 성장함에 따라 이익이 분화되고 이에 따라 갈등과 충돌도 쉽게 일어날 수 있는 것이라 할 수 있다. 특히 사회 내 저소득층이나 소외 계층들은 정부나 구성원들에게 불만을 가질 수 있는데 이러한 불만들이 극단적으로 테러 등 모습으로 나타나고 있다.

현재 농촌 지역 낙후 상태에서 발생하는 모순들을 살펴보면 개혁 개방 정책이 시행되었음에도 불구하고 여전히 극심하게 가난한 농민들이 존재하는 주된 원인은 지불되는 보상이 공정하지 못하기 때문이다.[13] 도시에서 일하는 농민공(農民工)들이 최근 공사 현장을 이탈하는 일이 빈번하게 발생하는 것도 오랫동안 그들을 차별하고 대우를 잘해주지 않아 발생하는 문제라고 볼 수 있다.

문제의 심각성은 도시에서도 빈번하게 발생하는데 개혁, 개방 이래 시장 원리에 따라 기업을 운영하다 보니 파산, 정상 운영 정지 등으로 직장을 잃거나 저소득과 생활 곤란으로 퇴직하는 사람들이 다수 존재하고 있다. 지역적으로는 중서부 지역이 빈곤 인구의 85%를 차지하고 보다 구체적으로 보면 중부지역이 56%이고, 서부지역이 29%를 점하고 있는 것으로 분석되고 있다.[14] 물론 중국의 지도자들은 소수민족 지역이나 농촌 지역의 구조적인 낙후를 우려하여 그에 맞는 산업을 발전시키거나 민생 프로젝트 건설, 교육 강화를 추진하고 있다.[15]

志)는 신도들을 시켜 살인, 방화, 자살 등을 저지르게 하여 사회를 파괴하고, 사람들로 하여금 공포를 느끼게 하는 행위를 자행하였으며 해외에서 중국 대사관을 공격하는 등 공공연하게 중국 정부에 대적하는 행위를 하였다. 黃金成(2009), p.211.

13) "임금이 너무 저조하고 그것도 제때에 지불되지 않고 계약에 의거하여 이행되지 못하고 있기 때문이다. 沈立人, 『中國弱勢群體』(北京: 民主與建設出版社, 2005), p.52.

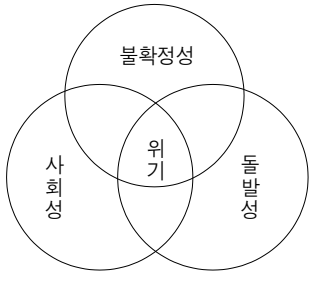
14) 沈立人, 위의 책, p.57

문제는 이러한 현상이 최근에 와서 까지도 근본적으로 개선되고 있지 않다는 것이다. 일반적으로 이와 같이 사회에서 소외당했다고 하는 사람들은 사회에 보복하는 수단으로 대중에게 테러를 자행하는 것을 크게 주저하지 않고 택하고 있는 것이다.[16] 이러한 테러 범죄는 불 특정적이고 무고한 대중을 공격 대상으로 하고 있으며, 폭력적이고, 돌발적이기 때문에 예방이 매우 어렵다는 특징을 지니고 있다.

이러한 문제들을 시급히 해결하는 것도 중요하지만 처리하는 과정 중에서 더욱 중시해야할 점은 정부의 위기관리 능력의 제고라고 할 것이다. 중국 사회가 만약 법률적으로 잘 갖추어진 국가라면 이러한 불만들이 주어진 법의 절차에 따라 처리 될 수 있겠지만 현재와 같이 정보처리 능력 약화, 사법 제도 불공정, 정부의 사회 모순을 처리 조절할 능력이 취약하다면 그 모순은 격화되고 테러 등 범죄가 발생할 확률은 높아질 수밖에 없을 것이다.[17]

다시 말해 개혁, 개방 이후 경제적 성과를 개인들이 소유할 수 있게 되었지만, 그 분배 과정이 공정치 못하여 분쟁과 갈등이 많아진 반면, 사회 내 그것을 통제할 수 있는 법률 제도가 잘 갖추어지지 않은 상태가 지속된다면 그 불만이 쉽게 테러라는 폭력적 수단과 형태로 나타날 수 있다.

[표 1] 위기의 불확정성, 사회성과 돌발성의 관계[18]



15) 김상호(2010), p. 123
16) 孫正,『當代中國社會衝突與政治調控問題研究』(長春: 東北師範大學, 2007), p.16.
17) 尹淑艷,『后冷戰時代的中國政治安全』(北京: 中共中央黨校, 2004), p.117.
18) 중국 사회의 위기는 사회에서 불확정성과 돌발성이 결합되어 나타난다는 것을 그림으로

3. 대외 확장과 테러 위협

중국의 덩샤오핑은 과거 마오쩌뚱(毛澤東)의 외교적 폐쇄정책에서 대외 개방 외교 정책으로 전환함에 따라 적극적으로 국제간의 협력에 나서게 되었다. 더 나아가 중국 국력이 증대됨에 따라 중국이 국제간 문제에 개입하는 범위가 현격하게 증대되었다. 새로운 국가 발전 전략인 "일대일로(一帶一路)" 정책 수행을 위해서라도 국제적 테러 문제에서 과거와는 달리 적극적 반대로 나올 수밖에 없을 것이다. 물론 중국의 의도에는 이런 것을 구실로 티베트 독립, 타이완 독립 등에 대한 서방의 개입을 차단하려는 목적도 있다고 볼 수 있다.

가. 대테러 인식의 전환

중국은 과거 공산주의 운동 당시 제국주의 세력에 대항하기 위해 모든 수단을 동원하였다. 1932년 상하이 홍코우(虹口) 공원에서의 윤봉길 의사의 거사 성공도 중국인의 협력이 없었다면 성공하기 힘들었을 것이다.[19] 이 시기에 중국 공산당은 약소국으로서 이러한 반제국주의 운동에 동정적이었다고 말할 수 있다. 또한 과거 낭만적 공산주의자들이 그들의 적인 유산계급과 싸우기 위한 방법으로 혁명적 폭력 테러를 지지하였다.[20]

그러나 오늘날 중국 스스로가 아직 영토적으로 통일이 되어 있지 못한 국가라는 인식하에 그러한 임무 완성에 저해가 되는 분리주의에 반대하고 그들이 펼치는 폭력 테러 행위에 분명히 반대한다는 목소리를 내고 있다.[21] 2001년 9·11테러 발생이후 국제적 테러는 더욱 빈번하게 발생하고 있지만, 이러한 테러를 저지

표시해 보았다. 潘志巍(2005), p.13.

19) 당시 독립투사들은 피압박자 입장에서 불합리하고 불평등한 질서를 바꾸기 위한 절명적인 선택을 할 수 밖에 없었다고 보기 때문이다. 何彤梅, 『中國-朝鮮·韓國關係史』(天津: 天津人民出版社, 2001), p.867.

20) 트로츠키 저, 노승영 역, 『트로츠키: 테러리즘과 공산주의』(서울: 프레시안 북, 2009), p. 76.

21) 陳以定, "淺析中國反空的國家利益與實踐體系," 『東南亞縱橫』, (南寧: 廣西社會科學東南亞研究所, 2003), p.69.

할 수 있는 국제적인 명확한 협약은 아직 이루어지지 못하고 있는 것이 현실이다. 국제 평화가 위협받고 있는 상황 하에서 중국의 국제적 지위가 높아지고 국제 교류가 확대됨에 따라 중국은 어떤 형태이든 국제 테러의 위협에 노출되고 위험이 더 높아지고 있는 실정이다.

현재의 세계는 기독교 문명국가와 이슬람 문명국가들과의 갈등과 충돌이 주된 이슈인데, 문제는 이들 종교는 둘 다 상대방을 인정하지 않는 유일 신앙을 주장함으로 인해 타협의 여지가 없다고 말할 수 있다.[22] 기독교, 동방정교, 불교와 인도교는 모두 정부 조직 내 그들의 종교 조직이 자리 잡고 있지 않으나, 반면 이슬람 각국은 그들의 정부 조직 내에 종교 조직이 함께 존재하는 관계로 이슬람 국가들 내에서 조직적인 테러 단체가 쉽게 생성되고 이들 테러 조직들이 서방 세계와 빈번이 충돌을 일으키고 있다.[23]

헌팅턴은 오늘날 세계가 어둡고 야만적 상태로 접어들고 있으며, 종잡을 수 없는 다국적 범죄조직, 마약 조직, 폭력적 테러 조직들이 판을 치고 있다고 보고 있다. 중국도 이러한 조직적 범죄의 목표에서 예외일 수 없다고 보기 때문에 자신들의 국가 이익을 지키기 위해서 이러한 테러를 방치할 수 없다.[24]

전 세계에서 이미 테러가 발생한 국가는 30여 개국인데, 중국에서의 테러는 80년대 항공기 납치 사건이 처음이라 하겠다.[25] 오늘날 과거에 비해 국력이 상승하고 더 개방적인 중국이지만 이러한 국제 테러에서 자유로울 수 없고, 또한 더 높은 차원의 국가이익을 위해서 실행하려고 기획된 “일대일로(一帶一路)” 정책의 원만한 수행을 위해서도 과격한 이슬람 폭력세력과의 투쟁은 피할 수 없다고 할 것이다.

---

22) 정항석, 『왜 21세기 화두는 미국과 테러인가』(서울: 평민사, 2002), p.222.
23) Huntington, 『文明的衝突與世界秩序的重建』, (北京: 新華出版社, 1998), p.372.
24) Huntington, 위의 책, p.191.
25) 陳以定, 위의 글, p.70.

나. 대외 진출과 테러 위협

덩샤오핑의 대외 개방 정책 채택과 이행으로 중국은 본격적으로 대외 교류를 전개하였는데, 중국은 우선 경제 무역 성장을 발전시키기 위해 미국을 비롯한 서방과의 관계 개선에 주력하였다. 오늘날 서방과의 관계 개선 후 중국은 대외 교류 영역을 중동 지역과 브릭스(BRICS) 등 개발도상국과의 관계로 확대하는데 주력하고 있는 것으로 보인다.

물론 중국 건국 초기 외교 관계를 미국 등 서방진영이나 소련 진영에 속하지 않았던 제3세계 진영과의 관계 개선에 매진한 경험은 제3세계 국가와의 관계개선에 도움이 될 것이다.[26] 최근 구소련의 해체로 인해 러시아와 중앙아시아 국가들과의 관계가 느슨해짐에 따라 중국은 이들 국가와의 관계를 긴밀하게 하는 정책을 펼치고 있다.

공식적으로 "상해협력조직(SCO)" 이라는 국제조직 구성으로 인해 중국은 러시아, 카자흐스탄, 키르기즈스탄, 타지키스탄, 우즈베키스탄 등 국가와 교류를 확대하며 경제적 협력과 자원개발에 주목하고 있지만, 더 나아가서 이 지역에 영향력을 행사하고 있는 이슬람 과격파를 견제하는 것도 소홀히 하지 않고 있다.

오늘날 국제테러주의 특징을 살펴보면 확산 범위는 다국적이고, 수단은 기민하며 방식은 내부 침투성이 강하다고 말할 수 있다. 테러 횟수를 살펴보면 2001년 400여회 이었던 것이, 2011년에는 3500여회 2013년에는 9000여회를 넘어섰던 것으로 조사되고 있으며 2014년 이후에는 더욱 더 기승을 부리는 상황으로 파악되고 있다.[27]

최근 이러한 테러 조직들은 다음과 같은 특징을 보이고 있는데, 원래 그 지역에 뿌리내리고 있던 테러 조직과 연합하려는 경향을 보이고 있고, 그들과의 교류 방식은 주로 인터넷을 사용하고 있는 것으로 보인다. 한편 어느 지역의 토박이 조직

---

26) 중국은 아시아, 아프리카, 라틴아메리카 등 국민들이 제국주의, 식민지주의, 종족주의 등에 반대하고 국가 독립을 쟁취하려는 노력에 적극 지지하였다. 韓念龍, 『當代中國外交』(北京: 中國社會科學出版社, 1990), p.133.

27) 劉靑建, 「恐怖主義的新發展及對中國的影響」, 『國際問題研究』, (北京:中國國際圖書貿易總公司, 2015), p.119.

은 국제테러 조직의 자금, 기술과 인터넷 통신망을 이용하여 세력을 확대하려는 모습을 보이고 있다.

중국은 현재 중앙아시아, 남아시아, 중동, 북아프리카 등 국가들과 거의 모두 외교 관계를 수립하면서 무역, 자원에너지 방면에 협력을 하고 있으며, 특히 "일대일로" 정책의 성공은 이 지역과의 평화적 협력 여부에 달려있다고 말할 수 있다. 그러므로 국제테러 조직의 활동과 영향력 확대는 이러한 중국의 국가적 사업과 대척점에 위치해 있다고 할 수 있다.

더구나 그들이 단순히 중국의 경제적인 면에서만 위협을 주는 것이 아니고 국가 안보 면에서도 심각한 위협을 주고 있다. 중국내 이미 존재 활동하는 테러 세력과 연합하여 그들을 지원하고 있기 때문이다. 심지어는 중국내 주된 테러 조직인 "동투르키스탄(東突)" 요원들을 데려다가 훈련시키고 경비를 지원하며 무기 탄약 등을 원조해주는 등 중국정부의 테러 정책에 도전하고 직접적으로 국내 안정을 위협하는 활동에 가담하고 있는 것으로 보인다.[28]

이와 같이 현재의 국제테러 조직은 중국의 경제 뿐 만아니라 안보 면에서도 엄청난 교란 세력이 되었으며, 이들의 움직임이 과거와 같이 단순히 중국을 대신하여 미국을 괴롭히는 역할을 지나 중국의 국익을 직접적으로 위협하는 존재로 변모되고 있다.

물론 중국의 장기적 국가 이익의 관점에서 볼 때, 우선 대만 독립 세력을 견제하고 북방 지역의 과격 분리주의자들을 소탕할 수 있는 명분을 갖는 것이 중요한데 국제 테러조직에 대적한다는 것은 중국 정부로 하여금 이들 분리주의자에게 지나치게 반인권적으로 대응한다는 오해를 받지 않을 구실을 제공하고 있다. 그러므로 중국의 대테러 전략은 중앙아시아 국가들과 협력하고 러시아와 함께 중앙아시아, 아프가니스탄, 파키스탄 같은 지역에서 발언권을 높이는 기회라고 말할 수 있을 것이다.

---

28) 劉靑建, 위의 글, p.124.

4. 다층적 대응

현재 중국은 그들의 국내 정치적 안정을 기하고 국가적 사업을 원만히 수행하기 위해서 국내외 테러 세력에 효율적으로 대응하는 것이 매우 시급한 과제라고 말할 수 있다. 특히 중국 경제 침체에 대한 돌파구 전략으로써 새롭게 전개하고 있는 "일대일로" 사업은 절대적으로 이들 국제 테러가 활동하고 있는 지역과 연관되어 있기 때문에 이들의 교란을 극복하지 못하면 그 수행이 원만치 못할 것이다.

이에 국내적으로는 우선 법률 체제를 새롭게 정비하고 국제적으로는 우선 국제 연합 기구를 십분 활용하여 대처해야하고 지역적으로는 미국을 비롯한 서방과의 협력 뿐 만아니라 러시아 또한 "상해협력조직(SCO)" 등 기타 지역 국제 조직과 긴밀한 협력을 강화하는 전략을 취하고 있다.

가. 테러대처 능력제고

테러가 중국 인민들에게 주는 영향은 테러에 대한 공포감을 느끼게 하는 것이다. 그러므로 중국 정부는 먼저 그 대책으로 중국 인민들 대상의 대테러 심리전에 착안하고 있다. 일반 국민들에게 테러에 대한 공포감을 갖지 않도록 교육시키고 더 나아가 테러분자들의 생각이나 행동에 동조하지 못하도록 사상 교육을 강화하고 있다. 만약 한족과 소수 민족 간에 불화 또한 종교 갈등이 존재한다면 이는 타국이 중국의 내정에 간섭할 구실을 주며, 동시에 테러가 발생할 토양이 조성되기 때문에 민족 간에 대화를 강화하고 종교와 정치를 분리하여 법제도 안에서 종교의 자유를 허용하는 정책을 구사하는 것이다.[29]

다른 하나는 부패 문제인데 부패를 중국 사회에서의 최대의 사회 오염이고 중국 공산당과 정부의 합법성에 도전하며 중국 사회를 분열시키는 것으로 보고 있다.[30] 특히 시진핑(習近平)이 집권한 이래 이 문제에 주목하여 부패 척결을 중국

29) 趙紀梅, "當前中國反空政策探析,"『工會論壇』, (濟南: 山東省工會管理學報, 2005), p.118.
30) 胡鞍鋼,『中國: 挑戰腐敗』, (杭州: 浙江人民出版社, 2001), p.35.

내부 정치의 최대 과제로 설정하여 노력하고 있다.

반면, 위기 발생 시 효율적으로 대처하기 위한 교육과 훈련을 강화하고 있는데, 2004년 10월 상하이시에서 최초로 테러 발생 시 상하이시의 안전을 구축하고 평온을 유지하기 위한 훈련을 실시한 것이 그 예이다. 경찰, 소방, 위생, 민방, 외사, 언론계 등 거의 400여명의 관련 부서 인원이 참석하여 인질을 구출하고 독가스가 퍼지는 것을 효율적으로 방어하는 실전 훈련을 통해 테러 대응 능력을 제고 시켰다고 평가하고 있다.[31] 또한 최근 사이버 공간을 이용한 테러에 대비하기 위해 중국 형법 120조에 추가로 사이버 테러 관련 직접 참여하는 사람 뿐 만 아니라 그런 교육을 받은 자들 까지 엄격하게 처벌할 수 있는 조항을 신설하였다.[32]

그러나 위기 예방과 처리 과정에서 단순히 정부 조직만을 의존하는 것은 한계가 있으며 비정부조직의 역할이 중요시 되는데, 특히 이러한 조직은 정책을 설명하고 주도하며 여론을 선도하고 위기 발생 시 자발적으로 서로 돕고 스스로 대책을 세워 대처해가는 능력이 뛰어난 것으로 평가되고 있다.[33]

[표 2] 정부와 비정부조직 위기 대처 관리[34]

비교내용	정부	비정부조직
대처목표	- 국민 생명재산 안전 보장 - 사회질서 유지 - 사고 발생 시, 국가 안보 유지	- 피해자의 기본 권리 보장
중립성	- 사고 발생 시 중립성 유지 부족	- 기본적으로 중립성 유지
발생지	- 관할구역	- 정부관할 지역보다 소규모
행정결정과정	- 중앙과 지방의 권리와 책임 규정	- 책임과 효율 사이에서 균형유지, 독립성 높음
자원이동	- 정부재정 지출	- 주로 모금으로 재정자원 조달
대처수단	- 위기 발생 시 경찰 및 군대 동원	- 인원 파견, 물자원조 및 심리적 지원

31) 潘志巍(2005), p.43.
32) http://china.findlaw.cn/bianhu/xingshidongtai(검색일 : 2015. 9. 17)
33) 潘志巍(2005), p.42.
34) 비정부 조직의 적극 활용으로 정부 역할이 미치지 못하는 부분을 보완하여 위기를 대처해 나아가야 한다는 설명이다. 薛瀾, 『危機管理-轉型期中國面臨的挑戰』, (北京: 清華大學出版社, 2003), p. 137.

중국은 대테러 문제에 대한 법률 체계가 다른 나라에 비해 미비하다고 비판받고 있다. 미국의 “종합적 범죄 대처법”이나 “반 국제테러 활동법”, 러시아의 “반테러리즘 조치에 관한 결정”, 일본의 “경찰법” 등은 모두 테러리즘에 대한 엄격한 규정을 갖추고 있는데 중국의 법률은 이런 것들에 못 미치고 있다고 평가받고 있다.[35] 이에 대한 보완으로 2001년 12월 테러활동 범죄에 대한 새로운 규정을 마련하였다.[36]

국제법의 규정에 테러 범죄인들은 정치범이 아니기 때문에 “정치범 불인도(不引渡)”와 “정치적 비호”에 적용되지 않는데 중국의 법률은 이점에 있어 불명확하다고 지적되고 있다. 또한 중국 국내법에 테러가 범죄라는 확실한 규정이 없어 범죄자에게 형량을 정할 때 어려움이 있는 것으로 분석되고 있다. 이러한 문제를 해결하기 위해 많은 중국 법학자들은 일반 범죄와 테러 범죄를 분리하고 테러범죄에 대해 가중 처벌해야 한다고 주장한다. 다른 나라의 경우 테러 범죄에 대해 사법부의 권한을 강화하는 내용의 입법을 하여서 테러 범죄에 전국가적으로 투쟁을 하고 있는데 이점에 있어 중국은 아직 부족한 것이 현실이라는 지적을 많이 받고 있는 것이다. 다른 한편 오늘날 테러 활동이 고도로 과학화되어 있으며 금융 분야와 깊게 얽혀 있어서 효율적 대처를 위해서는 이러한 분야와도 긴밀한 협조가 필연적이라고 지적되고 있다.[37]

현재 중국은 대테러를 강화하기 위해 부단히 노력하고 있는 것은 사실이지만 아직까지 다른 나라에 비해 미흡한 면이 많으며, 이 문제를 잘 해결하기 위해서 더 적극적인 노력이 기대된다고 보고 있다.

나. 국제 공조 강화

국제테러는 일반적으로 다음과 같은 네 가지 특징을 지니고 있는데, 첫째 테러

35) 陳以定(2003), p.72.
36) 테러 활동 지원죄, 허위 위험 물질 투여죄, 허위테러 정보의 조작, 고의 전파죄를 증설하였다. 음건봉, “중국의 테러 활동범죄에 관한 입법 연구,” 『동아법학』, 49집(2010), pp.250-262.
37) 趙紀梅(2005), p.117.

행위는 그 동기로 볼 때 개인적 이익을 추구하기 보다 이데올로기적이고 정치적 의도를 지니고 있다. 다음으로는 테러 목표를 일반적으로 무고한 시민이나 공공재산을 공격하며, 그 수단으로는 폭력을 사용하고 있다. 마지막으로는 폭로성의 추구라고 할 수 있다. 특히 최근 발달한 신문 매체나 전자 메일 등을 통해 급속하게 대중들에게 그 위협이 전달되기를 겨냥하고 있는 것이다.[38] 비록 오늘날까지 이러한 국제테러에 대해 국제법에서의 명확한 규정이 없음에도 불구하고 공통적으로 국제테러는 국제사회를 해치는 좋지 않은 범죄 행위로 인식되고 있으며 모종의 특정 범죄 행위로 규정하고 있다.[39]

국제 체제 속에서는 어느 국가나 홀로 존재할 수 없고 서로 상호 의존할 수밖에 없는데, 중국도 역시 대테러 문제에 대해 국제 공조를 중시하고 있다. 이러한 인식과 행동은 1997년에 체결한 "테러리즘의 방지와 처벌공약"의 국제공약에 근거하고 있고, 아태 지역에서는 2001년의 "아태경제협력 지도자들의 반테러리즘 성명"에 의거하여 행동하고 있다고 말할 수 있다. 대테러 문제 국제 공조에 있어 사법적 부분을 살펴보면, 우선 범죄자에 대한 강제적 조치이고, 조사나 자료 수집에 대한 협력이며, 정보의 교환 의무, 범인 이송 등의 문제라고 말할 수 있다.[40]

중국 정부는 우선 대테러 대응전략으로 국제연합 안보리 상임이사국으로서 역할과 의무를 다하여 국제연합의 대테러 전략을 제정하고 실시하며 테러 발생을 예방하는데 주력하고 있으며, 동시에 이러한 대테러 전략의 이행에 불리한 타국의 이기적인 어떠한 행위에도 반대하는 전략을 구사하고 있다. 특히 일부 서방 국가들의 반테러 전선을 혼란시키는 이중적인 기준 제시에 극력 반대한다는 전략이다.[41]

다음으로는 "상해협력조직" 같은 지역 협력조직에 적극 참여하여 그들과의 경

---

38) 馬福威,『論反恐中的國際合作原則』(北京: 中國政法大學出版社, 2003), p.9.

39) 예를 들어 1997년 국제연합에서 제정한 <폭탄테러리즘제지에 관한 국제공약> 등이 그것이다. 馬福威(2003), p.13.

40) 2001년 성명 내용은 비록 금융, 운수, 전신, 인터넷, 기술, 투자, 인명 등 광범위하게 대테러 규정이 있지만 그 규정이 매우 세부적이기 때문에 활발한 협력을 이루고자 하는 데에는 한계가 있다고 할 것이다. 馬福威, 위의 책, p.22.

41) 劉靑建(2015), p.125.

제, 안보 협력도 강화하고 동시에 대테러 방면에도 발을 맞추어 나가는 전략을 취하고 있다고 보겠다. 또한 비록 그리 영향력이 크지 않은 “아프리카 동맹”, “서아프리카 국가경제공동체” 등 지역협력 조직에도 참여하여 반테러 관련 활동에 대해 자금, 교육 및 기술을 지원하고 하고 있다. 중국의 현 정부가 현재 주도적으로 추진하고 있는 “일대일로” 정책은 단순히 관련된 국가들과의 경제, 무역, 에너지 등 분야에 대한 협력에만 그치지 않고, 대테러 관련 상호 협력이 수반되어야 성공할 수 있는 것으로 분석되고 있다.[42)]

과거 중국이 추진해왔던 대테러 국제공조의 구체적 사례를 살펴본다면, 9·11 사태 발생이후 중국은 미국과 협력하여 금융업무 관련 반테러 협력 기구를 만들었고, 러시아와는 대테러 업무 협력 부서를 설치하여 양국의 경찰, 위생 관련 업무 협력을 전개하였다. 또한 파키스탄, 인도와도 대테러 업무 협력을 강화하였고, 또한 영국, 프랑스, 독일과 대테러 문제 관련 협의를 강화하는 동시에 2002년에는 키르기스와 대테러 군사 훈련도 시행하였다. 2003년에는 “상해협력조직” 5개 국가가 함께 카자하스탄 국경 지역에서 테러 관련 군사 훈련도 전개하였었다.[43)]

중국은 현재 대테러 국제 공조를 위해 매우 적극적으로 활동하고 있으며, 국제연합에서의 지지 뿐만 아니라 지역적 협력에도 매진하고 있다고 말할 수 있다. 이것은 과거 단순히 미소 양국의 주도권에 대항하여 제3세계 국가들과의 협력을 통해 자신의 존재감을 드러내는 저항적 민족주의의 관점에서 만이 아니고 새로운 시대에 진정한 세계의 지도국이 되겠다는 생각에서 나온 것으로 평가할 수 있을 것이다.

42) 劉青建(2015), p.126.
43) 陳以定(2003), p.72.

5. 결론

중국에서의 테러는 이제 지속적 국가 발전을 위해서 더 이상 방치할 수 없는 시급한 문제가 되었다. “동투르키스탄” 의 분리 독립 움직임으로 대변되는 중국 분리주의는 전통적으로 중국의 테러를 유발하는 요인이라 말할 수 있다. 티베트 및 대만의 분리 독립 외침 또한 주목해야 하며 종교 자유 미비로 인한 종교적 갈등도 역시 중국 사회 불안 요인이 되어왔다고 할 것이다.

그러나 자본주의 생산 방식의 도입으로 인해 이루어진 개인의 부(富)가 축적되는 과정에서 불공정한 분배가 이루어짐에 따라 사회 내 불만과 갈등이 팽배되면서 또 다른 갈등 요인인 동시에 테러 유발 요인이 되고 있다고 할 것이다. 이러한 문제들을 해결하기 위해서는 선제적으로 불만 요인 제거에 노력해야 하는데, 예를들어 소수 민족 간에 대화를 강화하고, 테러 발생 시 대처 능력을 제고하기 위한 훈련은 물론 테러 관련되는 법을 새롭게 정비해야 할 것으로 본다.

중국이 대외 개방 정책 채택으로 인해 국제 사회 간의 관계가 매우 중요한 국가적 업무가 되고 있다. 최근 국제 사회에 유행되고 있는 국제 테러로 인해 중국도 피할 수 없이 국제 테러의 위협에 노출되고 있으며 중국의 국익과 국민의 안전이 위험에 처해 있는 것이 현실이다.

특히 시진핑(習近平) 등장 이후 강력하게 추진하고 있는 “일대일로” 정책은 과격 이슬람 테러 세력이 영향력을 행사하고 있는 지역을 통과해야 하기 때문에 이러한 테러 세력을 적절하게 통제하지 않고는 이 정책의 원만한 추진을 기약할 수 없는 것이다. 현재 중국은 그 대책으로써 국제 공조를 강화하고 있는데 국제 연합 내에서의 협력을 긴밀히 하고 “상해협력조직” 등 지역협력 조직을 이용하여 이들과의 투쟁에 만전을 기하고 있다.

종합적으로 볼 때 테러 행위는 스스로에게 자신감이 없는 약자의 행위이며 절망자의 몸부림이라 말할 수 있을 것이다. 그러나 그것은 만약 대중의 지지를 얻지 못하면 승리하지 못하는 빈곤한 전략이라 말할 수 있을 것이다.[44] 그럼에도 불구

하고 테러의 근본적인 동기는 불평등이기 때문에 이러한 불평등을 근본적으로 제거하지 않고는 진정한 세계 평화를 이룰 수 없다는 분명한 사실을 우리 모두가 직시해야 할 것이다.

44) 馬福威(2003), p.54.

참고문헌

정항석.『왜 21세기 화두는 미국과 테러인가』. 서울: 평민사, 2002.

트로츠키 저, 노승영 역.『트로츠키: 테러리즘과 공산주의』. 서울: 프레시안 북, 2009.

찰스 타운센드 저, 심승우 역.『테러리즘, 누군가의 해방투쟁』. 서울: 한겨레출판사, 2002.

음건봉. “중국의 테러 활동범죄에 관한 입법 연구.”『동아법학』, 49집(2010).

김상호. “2009년 7월 신강테러와 중국정부의 대응.”『대테러 연구』, 33집(2010).

이대성, 김태진. “중국의 테러리즘 분석과 그 전망.”『한국콘텐츠학회논문지』, 제4권 9호(2014).

이동률. “9.11테러와 중국의 갈등과 선택.”『당대비평』(2001).

馬福威.『論反恐中的國際合作原則』. 北京: 中國政法大學出版社, 2003.

潘志巍.『中國政府應對恐怖主義的危機管理研究』. 上海: 華東師範大學, 2005.

潘志平. “中國對恐怖主義的研究述評.”『國際政治研究』, 제3期(2011).

薛瀾.『危機管理-轉型期中國面臨的挑戰』. 北京: 清華大學出版社, 2003.

孫正.『當代中國社會衝突與政治調控問題研究』. 長春: 東北師範大學, 2007.

沈立人.『中國弱勢群體』. 北京: 民主與建設出版社, 2005.

劉青建. “恐怖主義的新發展及對中國的影響.”『國際問題研究』, 北京: 中國國際圖書貿易總公司, 2015.

尹淑艷.『后冷戰時代的中國政治安全』. 北京: 中共中央黨校, 2004.

趙紀梅. “當前中國反空政策探析.”『工會論壇』, 濟南: 山東省工會管理學報, 2005.

陳以定. “淺析中國反空的國家利益與實踐體系.”『東南亞縱橫』, 南寧: 廣西社會科學東南亞研究所, 2003.

何彤梅.『中國-朝鮮・韓國關係史』. 天津: 天津人民出版社, 2001.

韓念龍.『當代中國外交』. 北京: 中國社會科學出版社, 1990.

胡鞍鋼.『中國: 挑戰腐敗』. 杭州: 浙江人民出版社, 2001.
黃金成. “論中國面臨的恐怖主義威脅.”『法制與社會』, 云南: 云南省法學會, 2009.
Huntington.『文明的衝突與世界秩序的重建』, 北京: 新華出版社, 1998.

Abstract

Diversification and Countermeasures against Terrorism in China

Kwak DukHwan (Hannam University)

While a traditional factor of terrorism in China can be separatism, the unfair distribution accumulated by the recent economic growth has emerged as another factor of terrorism and conflict.

Communication between ethnic minorities and anti-corruption agencies is suggested as a solution to this problem. Additionally, china should revise the newly enacted terror-related laws and train people to raise their terror-fighting capabilities.

Chinese interests and its security have been threatened by the spread of terrorism occurred around the world. China emphasizes international cooperation based on the close cooperation between the United Nations and regional organizations. In particular, suppressing extreme terrorist groups in the Middle East for the successful progress of “Belt and Road Initiative” business implementation has become an essential task.

Although terrorism is the means of struggle of those minorities and their fundamental motivation is diverse, without addressing this problem, it is not possible to achieve more peaceful world.

Key Words: terrorism, separatism, security, distribution

투고일 : 2016.10.20. 심사일 : 2016.11.20. 게재확정일 : 2016.12.10.

II

미국의 사이버안보 수행체계 특징 및 시사점 고찰

전완주 (국가안보전략연구원)

Summary

미국은 2009년 백악관이 국가 사이버안보 업무를 총괄함으로써 사이버 부처간 기능과 역할 등이 정착되었다. 2009년 12월 처음 대통령 직속으로 사이버안보조정관을 임명하고 백악관 내에 사이버안보국을 신설해 국가 사이버안보정책을 총괄, 지휘하고 있다. 그리고 2010년 5월 국방부내에 사이버사령부를 창설하고 군사 네트워크 방어 및 관리 등을 전담토록 하였고 국토안보부 국가사이버안보・통신통합센터(NCCIC)가 민간부문을 담당토록 하는 국가 사이버안보 수행체계를 구축했다. 이 같은 부문별 정부기관들의 사이버안보 업무 분장이 초기부터 현재까지 큰 변화 없이 추진되고 있다.

미국의 정부부처들은 국토안보법 등 관련법에 근거를 두고 사이버안보 업무를 수행하고 있다. 그리고 신호정보 등을 수집하는 국가안보국(NSA) 국장이 사이버사령관을 겸직하는 등 조직구성이 특이한 구조를 갖추고 있다. 미국은 국토안보부가 국가 기간망을 책임지도록 규정하고 있음에도 사이버사령부도 국가기간망을 담당하는 조직을 신설해 국가 기간망 보호활동도 전개하고 있다.

이처럼 국가안보국장이 사이버사령부 수장을 겸직함으로써 신호정보, 영상정보 및 정세동향정보 등을 종합적이고 효과적으로 활용하면서 국가 사이버안보 업무에서 사실상 실무총괄 역할을 수행하는 특이한 시스템을 갖추고 있는 것이다.

한편 우리나라는 사이버안보 업무의 총괄은 청와대, 민간부문은 미래창조과학부, 국방부문은 국방부 및 실무총괄은 국정원이 담당하는 사이버안보 수행체계를 갖추고 있다. 그럼에도 불구하고 원전정보 유출사고 등이 잇따라 발생하면서 일각에서 사이버안보 수행체계를 수정・보완해야 한다는 주장이 제기되고 있다.

이러한 상황에서 우리로서는 백악관의 사이버안보국, 국방부의 사이버사령부 및 국토안보부의 국가사이버안보・통신통합센터 등 미국의 국가 사이버안보 수행체계의 조직, 기능 및 역할 등의 특징을 분석하고 우리나라의 사이버안보 수행체계에 주는 시사점을 도출하는 것이 중요하고 필요하다 하겠다. 본 논문은 미국의 사이버안보 수행체계의 특징을 분석하고 이로부터 시사점을 도출하며 향후 우리가 사이버안보 수행체계를 보완해 나가는데 고려해야할 점을 제시한다.

| 키워드 | 사이버안보국, 사이버사령부, 국가사이버안보・통신통합센터, 국가안보국, 사이버안보 수행체계, 사이버테러, 디도스

1. 서론

2003년 1월 우리사회에 인터넷 대란 이후 현재까지 청와대 등 정부기관 등에 대해 북한의 소행으로 추정되는 사이버공격이 수만 건에 달하고 있다. [표 1]에 나타난 바와 같이 최근 들어 북한의 사이버공격이 우리사회에 큰 피해를 주고 있다. 2009년 7월 청와대・백악관 등에 대한 디도스(DDoS) 공격, 2011년 4월 농협 전산망 해킹, 2013년 6월 청와대 등 67개 기관들에 대한 디도스(DDoS) 공격 등이 대표적이다. 이에 정부는 "국가 사이버위기 종합대책[1]", "국가 사이버안보 마스터플랜[2]" 및 "국가 사이버안보 종합대책[3]" 등 연속해서 대응책을 내놓았다. 정부는 북한의 사이버공격이 다양해지면서 국가 사이버안보[4] 수행체계 구축에 주력해왔다.

2009년 7월 정부는 처음으로 국가 사이버안보 수행체계로 "국가 사이버위기 종합대책"을 마련하면서 민간부문은 방송통신위원회, 국방부문은 국방부 및 공공부문과 국가 사이버안보 업무 총괄은 국정원이 담당토록 하는 국가 사이버안보 수행체계를 구축했다. 그리고 2011년 4월 북한의 농협전산망 해킹을 계기로 민간부문은 방송통신위원회, 금융부문은 금융위원회, 국방부문은 국방부, 정부전산센터는 행자부 및 평시・전시 모두 국정원이 사이버안보 업무를 총괄하는 방향으로 국가 사이버안보 수행체계를 변경했다.

---

1) 7.7 DDoS 공격, http://ko.wikipedia.org/wiki 및 "국가사이버안전 전략회의"의 발표내용(2009.9.13).

2) "3.4 디도스 공격, 7.7 대란의 업그레이드판,"『안철수연구소』, 2011.3.7., "검찰, "농협해킹, 북 정찰총국이 7개월간 준비","『동아일보』, 2011. 5. 4. 및 "정부, 사이버안보 마스터플랜 무엇을 담았나,"『전자신문』, 2011. 8. 8.

3) "정부, 국가사이버안보 종합대책 수립," 미래창조과학부 보도자료, 2013.7.8. 및 "KBS 등 전산망에 악성코드 침투!, 북한소행,"『뉴데일리』, 2013. 3. 20.

4) 사이버공간의 개념에 대해서 국제적으로도 논란이 되고 있지만 사이버안보란 사이버공간에서의 해킹, 사이버테러, 사이버범죄 등 사이버위협으로부터 국민생활과 국가안위 등을 안정적으로 유지 방어하기 위한 수단들을 총칭함.

[표 1] 최근 북한의 주요 사이버공격 및 정부의 대응책 사례

시기	북한의 주요 사이버공격 및 정부의 대응책 사례
2009.7	7.7 청와대·백악관 등 韓美 주요기관들을 대상으로 DDoS 공격해 1,500여대의 PC를 파괴 ⇒ 국가 사이버위기 종합대책
2011.3	3.4 청와대·국정원 등 40개 사이트에 대해 DDoS 공격해 800여대의 PC 하드디스크를 삭제하는 피해 야기
2011.4	4.12 농협내부 전산망 해킹해 서버파괴 및 금융업무 전면중단 야기 ⇒ 국가 사이버안보 마스터플랜, 국가사이버안전관리규정
2013.3	3.20 악성코드를 유포시켜 KBS·MBC·YTN 등 언론사 및 농협·신한은행 등 금융기관의 전산장비 48,000여대를 파괴
2013.6	6.25 청와대 등 국내 67개 기관 및 기업들을 대상으로 DDoS 공격해 서버파괴·사이트 변조 등의 피해를 초래 ⇒ 국가 사이버안보 종합대책
2014.12	한국수력원자력의 내부망에 침투해 원전도면 등 자료를 절취하고 원전가동 중단 등을 협박

북한의 사이버공격이 계속되고 국내 피해가 확대되자 2013년 6월 청와대 등 67개 기관들에 대한 디도스(DDoS) 공격을 계기로 국가 사이버안보 업무의 총괄은 청와대, 민간부문은 미래창조과학부, 국방부문은 국방부 및 실무총괄은 국정원이 담당토록 하는 방향으로 기존 사이버안보 수행체계를 보완해 현재까지 유지하고 있다.

그럼에도 불구하고 2014년 11월 원전정보 유출사고 등이 잇따라 발생하면서 전문가 및 사회단체 등 일각에서 사이버안보 수행체계를 수정·보완해야 한다는 주장이 제기되고 있는 상황이다.

사이버안보업무 수행을 위한 관련법 제정, 청와대의 컨트롤타워로서의 역할 재정립, 국방부의 대북 사이버전 수행을 위한 관련법 개정 및 국정원의 과도한 권한 집중 해소 등을 예로 들 수 있을 것이다.

한편 미국은 2000년대 들어 국가 사이버안보 업무를 두고 일부 부처간 알력이 조성되기도 했으나 2009년 백악관이 국가 사이버안보 업무를 총괄함으로써 부처간 기능과 역할 등이 정착되었다. 부문별 정부기관들의 사이버안보 업무 분장이 초기부터 현재까지 큰 변화 없이 추진되고 있다.

이에 전 세계에서 가장 먼저 국가 사이버안보 수행체계를 갖추고 효율적인 시스템을 구축하고 있는 것으로 알려진 미국의 사이버안보 수행체계의 조직, 기능 및 역할 등을 면밀히 살펴보고 우리의 사이버안보 수행체계와 비교([표 2] 참조)해 보는 것이 매우 필요하다 하겠다.

[표 2] 한미의 사이버안보 수행체계 비교

국가	총괄	민간부문	군사부문	실무총괄
미국	백악관	국토안보부	국방부	
	사이버안보국	NCCIC	사이버사령부	
한국	청와대	미래창조과학부	국방부	국정원
	국가안보실	사이버침해대응과	사이버사령부	사이버국

미국은 오바마대통령 시절인 2009년 12월 처음으로 사이버안보조정관을 임명하고 백악관 내 사이버안보국을 신설해 국가 사이버안보정책을 총괄, 지휘하는 역할을 부여하였다.[5] 그리고 2010년 5월 국방부내에 사이버사령부를 창설하고 군사 네트워크 방어 및 관리 등을 전담토록 하였고 국토안보부 국가사이버안보·통신통합센터(NCCIC)가 민간부문을 담당토록 하는 국가 사이버안보 수행체계를 구축했다.

미국의 사이버안보 수행기관들을 살펴보면 국가 사이버안보 업무를 담당하고 있는 정부부처들은 국토안보법 등 관련법에 근거를 두고 사이버안보 업무를 수행하고 있다.[6] 그리고 신호정보를 수집하는 국가안보국(NSA) 국장이 사이버사령관을 겸직하는 등 조직구성이 독특한 구조를 갖추고 있다.[7] 국토안보부가 국가기간망 보호·관리를 책임지도록 규정하고 있음에도 사이버사령부도 국가기간망을 담당하는 조직을 신설해 국가 기간망 보호활동도 전개하고 있는 것으로 나타

5) "사이버안보 최우선 인식...적국 시스템도 참고해야,"『정보보안뉴스』, 2013. 7. 4.
6) 이연수 외, "주요국의 사이버안전관련 법·조직체계 비교 및 발전방안 연구",『국가정보연구』, 제1권 2호(2008), pp.64-72.
7) NSA(National Security Agency : 국가안보국), CSS(Central Security Service: 중앙안보원) 및 사이버사령부 등의 수장이 동일 인물로 임명돼 사이버안보 업무 등을 수행하고 있음, https://en.wikipedia.org/Central_Security_Service

나고 있다.[8] 사이버사령관이 국가안보국장을 겸직함으로써 정보기관의 장점을 최대한 활용하는 동시에 국가 사이버안보 업무에서 사실상 실무총괄 역할을 수행하는 특이한 시스템을 갖추고 있는 것이다.

동 연구에서는 백악관의 사이버안보국, 국방부의 사이버사령부 및 국토안보부의 국가사이버안보·통신통합센터 등 미국의 사이버안보를 수행주체들에 대해 조직창설 경위, 현황, 기능 및 활동 등을 살펴보고 미국의 국가 사이버안보 수행체계의 특징을 분석한다. 이로부터 미국과 유사한 수행체계를 갖추고 있는 우리나라의 사이버안보 수행체계에 주는 시사점을 도출한다.

본 논문의 구성은 2장에서 백악관 사이버안보국, 국방부 사이버사령부 및 국토안보부 국가사이버안보·통신통합센터 등이 담당하고 있는 사이버안보 업무를 분석, 평가하고 3장에서는 이들 사이버안보 수행체계의 사이버안보 업무 특징 및 시사점을 도출한다. 마지막으로 4장에서는 앞으로 우리나라가 사이버안보 수행체계를 보완해 나가는데 고려해야할 점 등을 제시한다.

2. 미국의 사이버안보 수행체계 고찰

가. 백악관 사이버안보국

(1) 신설경위 및 조직 현황

9.11 테러가 발생하자 미국은 2003년 3월 국토안보부를 신설하고 국토안보부 내에 사이버안보체제를 구축하기 시작했다. 이어 2005년 12월 국방부가 사이버공간에 대한 작전개념을 정립하고 이와 관련한 구체적인 조치들을 단행하고 있는 가운데 2008년 3월 국토안보부는 장관직속 기관으로 국가사이버안보센터(NCSC:

8) 2013.3 NSA 키이스 알렉산더(Keith Alexander) 국장이 상원 법사위원회에서 사이버사령부는 기간산업의 보호를 위해 13개 사이버공격팀을 신설하고 각 13개 팀이 사이버상에서 공격력을 갖춰 별도임무를 수행하는 사이버부대를 창설할 계획이라고 밝힘, "오바마 대통령도 중국 해킹 비판," 『디지털타임스』, 2013. 3.14

National Cyber Security Center)를 설치하고 범정부 차원에서 사이버안보 업무를 총괄하고 있었다.[9)]

이즈음 국토안보부 국가사이버안보센터(NCSC)와 국방부 NSA간 국가 사이버안보업무 주도권을 두고 알력[10)]이 노정되기도 했다. 초대 국가사이버안보센터 수장이 국가안보국 국장과 사이버안보 업무와 관련한 의견대립으로 6개월 만에 사퇴하는 사건이 발생한데다 미국이 중・러 등 적대국들로부터 해킹 및 사이버공격 등이 날로 격화되면서 백악관은 국가 사이버안보 업무의 조정・통제 필요성을 절감하게 되었다.

이에 2009년 들어 오바마 정부는 사이버안보정책을 정부정책의 최우선과제로 선정하고 이전 정부들이 추진해온 사이버정보보호 기조[11)]를 계승, 확대해 국가 사이버안보 업무를 주도하기 시작했다. 2009년 12월 오바마 대통령은 사이버안보 조정관을 임명하고 국가 안전보장회의(NSC : National Security Council) 내에 사이버안보국을 신설해 국가 사이버안보정책 추진을 총괄, 지휘하는 사령탑 역할을 부여했다.([표 3] 참조)

[표 3] 백악관의 사이버안보 수행체제

조직	기능 및 역할	주요 활동
NSC내 사이버안보국 사이버안보조정관	사이버안보정책 총괄	부처・정보기관 지휘 사이버안보예산 관리 보안교육・인력 육성 등

(2) 주요 기능 및 역할

사이버안보국은 설치 이후 정부부처, 군 및 정보기관 등은 물론 전 국민을 대상

9) “주요국의 사이버테러 대응실태 고찰,” www.bluetoday.net, 2016.3.30

10) 이는 2010.3 백악관이 발표한 “The Comprehensive National Cybersecurity Initiative”(미국 사이버안보 종합계획)을 국토안보부와 NSA가 공동 주관하여 작성하는 요인이 되기도 함.

11) 2000년 미국은 국가 주요기반시설에 대한 사이버위협에 대응하기 위해 정보시스템 보호를 위한 국가계획을 마련함, 민경식 외, “미국의 사이버보안 정책과 R&D 전략에 관한 분석,” 『Internet & Security Focus』, 통권 제1호(2013.1), pp.45-62.

으로한 미국의 사이버안보정책을 총괄 지휘하고 있다. 이와 함께 사이버안보국은 전 국민들을 대상으로 사이버보안 교육프로그램을 비롯하여 국민 인식 캠페인 및 연방 보안인력 육성정책 등도 주도하고 있다.[12] 또한 효과적인 사이버안보정책 추진을 위해 정부부처가 사이버보안 조치의무를 이행하지 않을 경우 연방정보보안관리법(FISMA: Federal Information Security Management Act)에 의거해 예산을 감액하는 정책 또한 집행하고 있다.[13]

나. 국방부 사이버사령부

(1) 창설경위 및 조직 현황

2006년 10월 공군이 사이버사령부를 창설할 계획임을 밝힌 후 2006년 11월 먼저 공군 내에 사이버사령부를 창설하였다가 2009년 6월 국방장관이 전략사령관에게 통합 사이버사령부 창설을 지시했다. 이에 2010년 2월 미 국방부는 국방검토보고서(QDR: Quadrennial Defense Review)[14]에서 사이버공간을 육, 해, 공, 우주에 이어 제 5의 전장으로 분류한데 이어 작전영역으로 규정한 후 2010년 5월 전략사령부[15] 산하에 각 군의 작전능력을 통합해 사이버사령부(USCYBERCOM: United States Cyber Command)를 창설했다.

이로 인해 사이버사령부 조직은 육군사이버사령부, 해군사이버사령부, 공군사이버사령부 및해병대스페이스사령부 및 예하부대 등으로 구성하고 있고 사이버사령부의 인원은 전자전 전문병력 5,000명을 포함해 88,000여명의 IT전문가들을 중심으로 구성되어 있다.

---

12) "사이버안보 최우선 인식...적국 시스템도 참고해야", 『정보보안뉴스』, 2013. 7. 4.
13) 오일석 외, "미국 연방정보보안관리법 소개", 『한국인터넷정보학회 2004 추계학술발표대회 논문집』, 제5권 제2회(2004.11), pp.135-138.
14) 미 국방부가 4년마다 발간하는 보고서로서 주로 美국방부의 군사전략을수록 (http://www.defense.gov/qdr, 미 국방부 홈페이지).
15) 전략사령부는 정보전과 같은 정보작전 등을 담당하는데 컴퓨터 네트워크 공격 및 방어와 관련된 군의 활동을 총괄조정, 통제하고 있고 사이버 지휘부대 창설 및 사이버전쟁 모의훈련 등을 실시하여 사이버공격에 대응하고 있음 (https://en.wikipedia.org/wiki/united_states_strategic_command, 미국 전략사령부).

그리고 각 부대에는 ①미군 전산망 보호임무를 담당하는 사이버보호부대(CPF : Cyber Protection Forces), ②전력망, 발전소 등 국가의 주요 인프라 전산망 방어 임무를 담당하는 국가임무부대(NMF: National Mission Forces) 및 ③적대세력에 대한 공세적 사이버작전을 펼치는 전투임무부대(CMF: Combat Mission Forces) 등을 두고 있다.[16]

게다가 국가안보국[17](NSA: National Security Agency, 총인원 38,000여명) 및 중앙안보원[18](CSS: Central Security Service, 총인원 25,000여명) 수장이 사이버사령관을 겸직하고 있다.

[표 4] 미국 사이버사령부의 사이버안보 조직, 인력 및 수행체계

국가	조직	인력	지원 및 수행주체	
미국	육・해・공・해병대 사이버사령부 (사이버보호, 국가임무, 전투 임무부대형태)	육・해・공・해병대 사이버사령부 등 총 88,000여명	국방부	
			NSA(NRO), CSS, 전략사령부	사이버사령부

※ NRO는 영상정보를 NSA에 제공하고 있고 신호정보를 수집하는 NSA와 CSS・사이버사령부 수장이 동일인물이며 전략사령부는 사이버사령부 상급조직임

(2) 주요 기능 및 역할

사이버사령부[19] 관련 공개 자료는 미국 사이버사령부의 주요 기능 및 역할을

16) "미 vs 북 본격 사이버전쟁땐 누가 이길까?," 『나우뉴스』, 2014.12. 3.

17) 1952년 창설된 NSA는 암호개발은 물론 각종 수단을 활용해서 통신정보와 전자정보 등 신호정보를 수집하고 정리하는 업무를 담당하는 미국 국방부 산하에 있는 비밀 정보기관이다. 도청 및 감청기술을 보유하고 있는 NSA는 에셜론 프로젝트를 운용하고 있으며 국민들의 인터넷 사용을 감시하고 있는 기관으로도 알려져 있다. NSA가 CIA의 전화까지 도청했다는 루머까지 있는 실정이다. 2013.6 스노든에 의해 NSA가 관리해 온 영장없이 감시하는 PRISM 프로그램의 실체가 공개되기도 하였다. 미국 정보공동체의 핵심부이고 미 정보기관 중 가장 큰 규모와 막강한 정보수집력을 보유하고 있다. 법적으로는 NSA의 첩보수집은 해외 통신에만 국한되었지만 국내 통신도 수집하고 있음이 스노든에 의해 폭로된바 있다(http://www.nsa.gov).

18) 중앙안보원은 NSA 및 사이버사령부 등과 같이 메릴랜드에 소재하고 있으면서 여러 개의 사이버전 수행팀을 운용하고 있는 것으로 알려지고 있고 국방부산하 비밀정보기관으로 여타기관에 암호 해독술을 전파해 주는 기능도 담당하고 있음 (https://en.wikipedia.org/Central_Security_Service).

19) https://en.wikipedia.org/united_states_cyber_command

사이버 자원과 사이버공간 작전을 통합관리하고 국방부가 운용하고 있는 15,000개 이상의 군사 네트워크 방어를 담당하고 있다고 서술하고 있다. 그리고 주로 전 지구 네트워크전 합동군(JTF-GNO) 및 합동 네트워크전 구성사령부(JFCC-NW)[20] 등과 협력하여 컴퓨터 네트워크 방어 및 사이버공격 등을 수행하고 있는 것으로 기술하고 있다.

그러나 국방부관계자의 의회보고 및 국방부 보고서 등을 통해 사이버사령부의 주요 기능 및 역할 등을 면밀히 살펴보면 미 사이버안보 수행체계에서 국토안보부가 담당하고 있는 기간망 보호활동 등 여러 가지 활동을 수행하고 있는 것으로 나타나고 있다. 2013년 3월 국가안보국 키이스 알렉산더(Keith Alexander) 국장이 상원 법사위원회에서 사이버사령부는 기간산업의 보호를 위해 13개 사이버공격팀을 신설하고 각 13개 팀이 사이버 상에서 공격력을 갖춰 별도임무를 수행하는 사이버부대를 창설할 계획이라고 언급한 점[21]을 감안하면 군 네트워크 관리와 보호임무를 비롯하여 정부부처 및 국가기간산업 전산망 보호활동 그리고 적에 대해 공세적 사이버작전[22] 등을 전개하고 있는 것이다. 2011년 7월 국방부가 발표한 5개의 전략적 이니셔티브[23]로 구성된 "사이버공간에서의 국방작전전략"(Defence Strategy for Operating in Cyber-Space)[24]에서 선언한 내용 등을 고려하면 국방부가 정부부처, 공공기관 및 민간영역[25]과 협력강화를 통한 "국가사이버안보전략"을 추진하고 있는데 대해 전략사령부 산하에서 중추적인 역할을

---

20) JJF-GNO와 JFCC-NW는 사이버사령부가 창설되기 전 전략사령부 예하에서 사이버 관련 임무를 수행하던 조직으로 후에 공군 사이버사령부로 발전하였다.

21) "오바마대통령도 중국 해킹 비판," 『디지털타임스』, 2013. 3.14

22) 2014.7 소니픽쳐스사를 해킹했던 북한 인터넷 사이트에 대한 DDoS 공격은 사이버사령부 CMF가 담당했던 것으로 알려짐, "미 vs 북 본격 사이버전쟁땐 누가 이길까?," 『나우뉴스』, 2014.12. 3.

23) 5개 이니셔티브란 1)사이버공간을 작전영역으로 정의하고 담당조직을 설립하며 훈련과 무장추진 2)국방부 네트워크 및 시스템 보호를 위한 새로운 방어전략 도입 3)정부부처, 공공기관 및 민간영역과 협력강화를 통한 국가기반의 사이버안보전략 실행 4)동맹국들과 사이버안보의 국제공조 강화 5) 사이버안보관련 우수 인력 확보와 기술혁신 등을 말한다.

24) 『국가 사이버안보전략 참고자료』, 국가보안기술연구소(2012. 5), pp.VIII-1～VIII-16.

25) NSA는 메릴랜드대학 등 4개 대학에 사이버보안관련 연구비 지원을 확대하였다. "미 국가안보국, 사이버보안 연구를 위한 대학지원 확대," 『KISTI 미리안 글로벌동향브리핑』, 201.5. 5.14.

담당하고 있는 것이다.[26] 사이버사령관이 국가안보국장과 중앙안보원장 등을 겸직하고 있어 국가안보국(NSA)가 수집한 감청정보, 통신정보 및 전자정보 등 신호정보와 함께 국가정찰국(NRO)[27]이 수집한 영상정보 등을 제공받는 동시에 국가안보국 및 CSS 등이 요구하거나 필요로 하는 사이버무기 개발, 해킹 및 사이버공격 등도 지원하고 있는 것으로 관측된다. 이와 함께 사이버사령부는 인간정보를 수집하는 CIA와 해외 정세·동향정보 등을 수집하는 국방정보국(DIA, Defence Intelligence Agency) 등으로부터 관련정보 지원을 받아 활용하고 있다.

[표 5] 미국 국방부의 사이버안보 수행체제

조직	기능 및 역할	주요 활동
육군·해군·공군·해병대통합 사이버사령부	군 네트워크 보호관리 기간망 보호·관리	공세적 사이버전 전개 사실상 실무총괄 국가 사이버안보전략

다. 국토안보부 국가사이버안보·통신통합센터(NCCIC)

(1) 통합경위 및 조직 현황

2002년 미국은 국토안보 업무를 총괄하기 위해 주요기반보장국(CIAO: Critical Infrastructure Assurance Office) 및 비밀검찰국(Secret Service) 등 22개 기관을 통합해 국토안보부[28]를 신설하면서 각 정부기관에 산재해 있던 정보보호와 관련된 조직을 통폐합했다.

---

26) 2015.1 사이버사령관은 네트워크 방어는 공공부문 책임과 민간부문 책임으로 구분할 수 있는 양자택일의 문제가 아니어서 정부와 기업이 모두 긴밀히 협력해야 함을 강조하였다(www.armyrecognition.com, 2015. 1.14.).

27) 에셜론프로젝트 발각이후 NSA는 정찰기능을 떼어 NRO를 설립한바 NRO는 수집한 모든 영상정보를 NSA에 제공하고 있음, “세계의 정보기관 미국편, NSA·NRO·DIA, CIA보다 은밀한 미국의 눈,”『이투데이』, 2012. 4. 5.

28) 2002.11 신설된 후 국토안보부는 사이버안보 업무 총괄기관을 창설해 사이버테러 및 정보전에 대한 범국가적 대응활동을 조정, 통제하고 있으며 매년 사이버전쟁 모의훈련을 실시하고 산하에 사이버보안 및 통신실을 설치하여 사이버위협 위험분석, 취약점 보안, 사이버위협 경고전파, 사이버공격 대응활동 조정 등을 실시하고 있다.

준비국(Directorate for Preparedness) 및 과학기술국(Science and Technology Directorate) 등 2개의 국으로 통합하고 준비국 산하에 국가사이버안보처(NCSD: National Cyber Security Division)를 신설했다.

국가사이버안보처(NCSD)는 사이버침해사고 대응팀(US-CERT)을 운영, 정보발령 및 연방정부 정보통신망에 대한 취약성을 평가하고 CIIMG(Cyber Interagency Incident Management Group) 보안포탈 사이트를 통해 국방부, CIA 및 법무부 등과 실시간 정보공유 체제를 유지하고 있다. 그리고 NCSD는 "사이버 스톰"과 같은 전국적인 사이버전 모의훈련[29]을 실시해 국민과 민간기업들의 인식제고를 위한 사이버안보전략 수립과 민관협력을 주관하고 있다. 또한 NCSD는 APEC, OECD 및 G8 등 다자간 국제기구 등과 협력 체제를 유지하고 있다.

이후 2008년 3월 국토안보부는 장관직속의 국가사이버안보센터(NCSC: National Cyber Security Center)를 설치하여 범정부 차원에서 사이버안보 업무를 총괄하기 시작했다.[30] 여기서 국가사이버안보센터(NCSC)는 FBI, NSA 및 국방부 등과 협력하여 연방 정부기관의 컴퓨터 시스템에 침입하는 사이버테러를 감시하고 해킹 취약정보를 감사하는 등 모든 연방정부기관의 컴퓨터시스템과 인터넷 보안을 총괄하는 범부처 기구로 운영하기 시작했다.

2009년 11월에 국토안보부는 미국을 상대로 한 각종 사이버테러 대응 및 IT 인프라 보호 등을 위해 미국 정부부처들 산하에 산재해 있던 사이버안보 기능들을 통합하여 국가사이버안보·통신통합센터(NCCIC: National Cybersecurity and Communications Integration Center)[31]을 신설, 출범시켰다. 국가사이버안보·통

---

29) 사이버전 모의훈련으로는 국토안보부 산하 국가사이버보안처(NCSD)가 주관하는 "사이버 스톰"(Cyber Storm)이 있는데 사이버 스톰(Cyber Storm) 훈련은 2006년부터 미국의 민·관·군이 참여해 격년제로 실시하는 사이버공격 모의 대응훈련으로 2008년 실시한 "사이버 스톰" 훈련에는 호주, 캐나다, 뉴질랜드 및 영국 등도 참가했고 우리는 2010년 훈련에 참가를 검토하다가 불참했으나 2012년 실시한 훈련에는 기무사를 중심으로 일본과 함께 참가한 바 있다.

30) 이연수 외, "주요국의 사이버안전관련 법·조직체계 비교 및 발전방안 연구," 『국가정보연구』, 제1권 2호(2008), pp.64-72.

31) 2009년 11월 국가사이버안보 및 통신통합센터(NCCIC)는 국가를 상대로 한 각종 사이버테러 대응 및 IT 인프라보호를 위해 미 정부기관들의 사이버안보 기능을 통합하여 설립하면서 국토안보부 산하 조직인 컴퓨터위기대응팀(US-CERT), 국가텔레커뮤니케이션

신통합센터(NCCIC)는 국가사이버안보센터(NCSC)보다 역할을 확대하는 동시에 연방정부, 지방정부 및 민간 협력체들이 함께 참여해 유연하고 통합된 시스템의 필요성이 제기되어 창설됐다.

(2) 주요 기능 및 역할

2002년 미국은 "국토안보국가전략"(National Strategy for Homeland Security)에서 주요기반시설과 자산보호 등을 위한 프로젝트에 국토안보부가 주요기반시설 보호업무를 총괄하도록 업무를 조정했다. 미국의 전체 국가기반을 보호하기 위해 2002년 11월 제정한 법률인 국토안보법(Homeland Security Act of 2002)은 국토안보부가 미국의 주요기반시설의 보호와 사이버공격에 대한 대응활동을 총괄 조정한다고 규정하고 있다.[32] 이에 따라 국토안보부 산하 국가사이버안보·통신통합센터(NCCIC)는 미국을 상대로 한 각종 사이버테러 대응 및 IT 인프라 보호활동 등을 담당하고 있다.

[표 6] 미국 국토안보부의 사이버안보 수행체제

조직	기능 및 역할	주요 활동
국가사이버안보·통신 통합센터(NCCIC)	국가기간망 보호관리 IT 인프라 보호관리	사이버테러 모의훈련 사이버분야 국제협력 사이버공격 대응활동

한편 2011년 5월 국토안보부는 국무부, 국방부 및 재무부 등과 함께 사이버공간에 대한 국가전략인 "사이버공간에 대한 국제전략 : 네트워크 세계에서의 번영, 안보 및 공개성" 제하 보고서를 통해 미국의 사이버안보전략의 원칙 및 방향을 제시했다.[33]

조정센터(NCC) 및 국가사이버보안센터(NCSC) 등을 통합, 흡수하였다. "미"사이버안보 총사령부 "NCCIC 문 열어," 『연합뉴스』, 2009.11. 1.

32) 이연수 외, "주요국의 사이버안전관련 법·조직체계 비교 및 발전방안 연구," 『국가정보연구』, 제1권 2호(2008), pp.64-72.

33) 『국가 사이버안보전략 참고자료』, 국가보안기술연구소(2012.5), pp.VII-1~VII-25.

미국의 사이버안보전략의 원칙으로는 사이버공간이 가지고 있는 특성과 기존 자유에 관한 권리를 존중하고 이에 따라 사이버공간도 전통적인 규범의 적용을 받아야 함을 강조하고 있다. 미국의 사이버안보전략의 방향으로는 ①사이버공간에 대한 접근과 이용에 경제적 또는 기술적 제약이 없도록 하기위해 미국은 개방적이고 상호운용이 가능토록하며 ②안전하고 신뢰할만한 정보와 통신기초시설을 증진시키기 위해 국제적으로 노력하고 ③사이버안보는 일국의 능력으로 대처할 수 없기 때문에 집단안보를 강화하기 위해서 동맹국 및 협력국가들과 사이버공간에서의 협력을 확대해 나갈 것 등을 밝히고 있다.

사이버안보분야에서 국토안보부 국가사이버안보·통신통합센터(NCCIC)의 주요 기능 및 역할은 국가기간망 보호와 관리 등 민간부문을 담당하고 있는 것이다.

3. 미국의 사이버안보 수행체계 특징 및 시사점

2장에서 살펴본 바와 같이 미국의 사이버안보 수행체계는 미국 사이버안보정책을 총괄하며 컨트롤타워 역할을 담당하고 있는 백악관의 사이버안보국, 민간부문 등을 담당하고 있는 국토안보부의 국가사이버안보·통신통합센터(NCCIC) 및 군사부문 등을 전담하고 있는 국방부의 사이버사령부 등으로 구성되어 있다.

미국의 사이버안보 수행체계는 우리나라와 달리 사이버공간의 문제점이 노정되거나 보호 및 관리 필요성이 부각되면서 주관부처는 변경된바 없으나 부처 내에서 초기 조직들이 변화 및 수정과정을 거쳐 현재의 체계로 정착되었다.

백악관 사이버안보국은 연방정보보안관리법(FISMA)에 근거해 각 부처가 사이버안보 업무를 소홀히 할 경우 예산삭감 등을 통해 강력하게 추진하며 부문별 주무부처간 부처이기주의에 따른 정보 사각지대 최소화 및 업무효율성 제고를 유도하고 있다. 국토안보부는 국토안보법에 미국이 사이버공격을 받을 시 국토안보부가 주요기반시설 보호활동을 담당한다고 규정하고 연방정부, 주정부 및 기업들간

협력강화를 위해 정부부처들 산하에 산재해 있던 사이버안보관련 조직들을 통폐합하여 국가사이버안보·통신통합센터(NCCIC)를 창설해 업무효율화를 도모하고 있다. 국방부 사이버사령부는 국가정찰국(NRO)으로부터 해외 영상정보를 제공받고 있는 동시에 적의 감청정보, 통신정보, 전자정보 등 신호정보를 수집하는 국가안보국(NSA) 및 사이버전 수행팀을 운용하고 있는 것으로 알려진 중앙안보원(CSS) 등과 동일한 부처에 소속되어 있고 한 사람이 3개 기관의 수장직을 겸직하며 운영되고 있다. 게다가 인간정보 등을 수집하는 CIA와 해외 정세·동향정보 등을 수집하는 국방정보국(DIA, Defence Intelligence Agency) 등으로부터 정보지원을 받고 있어 적의 신호정보,[34] 영상정보 및 인간정보와 정세·동향정보 등을 종합적으로 활용해 사이버 업무를 추진할 수 있는 사이버안보 수행체계를 갖추고 있는 것이다.

이처럼 미국의 사이버사령부는 자국을 공격하는 사이버테러 등의 주체를 정확히 파악하고 강력하게 대응하기 위해 신호정보 및 영상정보는 물론 사이버전 수행팀을 운영하고 있는 기관들을 한 사람이 운영하고 있다는 점이 주목된다. 사이버공간 특성[35]을 감안해 신호정보에다 인간정보, 정세동향정보 등을 종합적이고 효과적으로 분석하기 위해 CIA 및 국방정보국(DIA) 등 기관들과 정보교류 협력체계가 원활하게 운영되고 있다는 점이다.

또한 군 네트워크 관리와 보호 등 기본업무 외에 국가사이버안보·통신통합센터(NCCIC)가 담당하고 있는 정부부처 및 기간망 등의 관리와 보호활동을 지원하기 위해 국가사이버안보·통신통합센터와 정보를 공유하며 국가임무부대(NMF)

34) 미국의 경우 주로 신호정보(통신 및 전자정보 등)는 NSA, 영상정보는 NRO, 인간정보는 CIA가 수집한다.

35) 사이버공간은 흔적을 남기지 않는 은밀성, 접속매체 등에 감염을 확산시키는 감염성 그리고 일정한 조건이 충족되기를 기다려 공격하는 잠복성 등을 포지하고 있고 시간적으로나 공간적으로도 제약이 없는 특성을 갖는다. 그리고 사이버위협은 날로 지능화되고 있어 사전탐지가 어렵고 병원균과 같이 외부화 되었을 때가 되어야만 인식하게 된다. 게다가 사이버위협은 인터넷을 매체로 정보통신기반시설에 잠복하거나 PC에 잠복하여 일정한 기간 또는 조건이 되었을 때 활동하는 경우가 대부분이어서 공격자의 원점을 타격하기가 매우 어려운 상황이다. 정준현, "북한의 사이버테러에 대한 우리의 대응전략과 과제,"『북한 사이버테러 위협과 대응전략』, 국가안보전략연구원·국가보안기술연구소 공동학술회의자료집(2015.3.31.), pp.67-96.

및 전투임무부대(CMF) 등을 별도로 구축, 운용하고 있는 점도 주목된다. 미국은 국가기간산업이 사이버공격을 받을 경우 국가경제 등에 미치는 피해가 지대한 점을 감안해 이를 국토안보부가 1차적으로 전담하게 하면서도 사이버사령부도 별도 조직을 구성해 기간망 보호활동도 전개하고 있는 것이다. 그리고 전략사령부가 상급부서로 정보전 및 사이버 모의훈련 등 사이버사령부의 업무를 지원하는 조직 체계를 갖추고 있다.

[표 7] 한미 사이버사령부의 사이버안보 조직, 인력 및 수행체계 비교

국가	조직	인력	지원
미국	육・해・공・해병대 사이버사령부(사이버보호, 국가임무, 전투 임무부대형태)	육・해・공・해병대 사이버사령부등 총 88,000여명	NSA, CSS, 전략사령부
한국	연구개발단, 사이버전단, 대북심리전단, 교육훈련단	육군으로만 구성된 1,000여명	국방정보본부

이러한 특성으로 인해 국방부 사이버사령부는 민・관・군 협력체제를 구축하며 사실상 미국의 사이버안보 수행체계에서 실무총괄에 버금가는 중추적 역할을 담당하고 있다는 점이다. 이와 함께 국방부는 미국에 대한 사이버공격을 전쟁행위로 간주하고 사이버공간에서의 자위권을 강조하며 무력 대응할 것임을 천명하면서 무력충돌법 등을 사이버공간에도 동일하게 적용해 나갈 것이라고 주장하고 있다.[36] 그러면서도 사이버사령부는 현재까지 사이버공격에 대해 무력충돌법 등을 내세워 적국에 무력으로 대응한 바 없고 사이버공격으로만 대응하고 있으며 사이버공간 특성을 감안해 동맹국 및 우방국들과의 협력을 강조하고 있는 점도 주목된다.

36) http://www.ajunews.com.view/20150113094601498

4. 맺음말

우리나라의 사이버안보 수행체계는 [표 2]에서 보는 바와 같이 청와대 국가안보실이 컨트롤타워 역할을 하고 있고 국방부 사이버사령부가 군의 네트워크 관리·보호 활동과 사이버전을 담당하고 있으며 미래창조과학부가 민간부문을 전담하고 있다. 그리고 미국과 달리 국정원이 실무총괄을 담당하고 있는 것으로 구성되어 있다.

우리 각 기관들은 미국의 정부부처들과 달리 근거법령 없이 대통령훈령인 "국가사이버안전관리규정"에 의존해 사이버안보 업무를 수행하고 있는 실정이다. 조속한 시일 내에 대통령 훈령만이 아닌 법률에 근거해 활동할 수 있도록 사이버테러방지법 등 관련법 제정이 시급하다. 그리고 우리 국가안보실에 사이버안보정책 전문가가 적고 집행력이 미약한 실정인바 전문성이 있는 사이버안보보좌관 임명 등 사이버안보정책 전문가들의 확대 또한 필요한 것으로 판단된다.

최근 우리 국방부 사이버사령부는 대북 사이버전 수행을 위해 관련법 개정과 업무확대 등을 추진하고 있는 것으로 알려져 있다. 그러나 한미 국방부 사이버사령부의 조직, 인력 및 체계 등을 비교([표 7] 참조)해 보면 사이버사령부는 관련법 개정 등을 통한 업무확대 추진에 앞서 우선 역량확충이 시급한 것으로 나타나고 있다. 육군으로만 구성되어 있고 1,000여명에 불과해 사이버사령부의 인력 확충이 필요하다. 국방부 내 사이버사령부는 신호정보를 수집하는 777부대, 인간정보, 영상정보 및 정세정보 등을 수집하는 정보사령부와 이원화되어 있어 정보교류 등 부족한 점이 있다면 원활하게 정보가 공유될 수 있도록 수행체계 역시 보완이 필요하다. 또한 사이버사령부를 장관직속으로 두고 있어 지원부서가 없는 상황으로 내몰리고 있는 것은 않은지 점검해 볼 필요가 있다.

미국은 사이버사령관이 국가안보국(NSA) 국장을 겸직하면서 각 분야의 첩보와 정보를 종합해 활용하고 있다. 그만큼 사이버테러 등 사이버공격을 방어하고 공격하는 데는 다각적이고 종합적인 첩보 및 정보가 필요함을 방증하고 있다. 현

재의 사이버안보 수행체계가 구축되기 이전에는 국토안보부 국가사이버안보센터(NCSC)가 주도하다가 구축 이후에는 NSA 국장이 주도하는 사이버사령부가 실무총괄 역할을 하고 있다.

일각에서 국정원이 실무총괄 업무를 담당하고 있는 것에 대해 과도한 권한 집중이라고 지적하고 있는데 미국의 사이버사령부의 업무 수행체계를 보면 설득력을 잃게 된다. 국정원은 미국의 국가안보국과 사이버사령부 관계처럼 북한 등 해외의 통신정보, 감청정보 및 전자정보 등을 수집하는 부서 그리고 인간정보와 영상정보 및 정세·동향정보를 수집하는 부서들을 모두 갖추고 있기 때문이다.

미국 사이버사령부는 국가 기간망 등이 공격을 받을 경우 경제에 막대한 피해가 야기될 것을 우려해 국토안보부가 전담하면서도 사이버사령부가 실무총괄 업무를 담당하듯이 이중으로 보호활동을 전개하고 있다. 우리의 경우 국정원이 실무총괄을 담당하고 있는 점을 감안해 볼 때 이 또한 유사한 체제를 갖추고 있다고 볼 수 있다. 민간부문은 미래창조과학부, 인터넷침해대응센터, 한국인터넷진흥원 및 경찰청 사이버안전국 등이 분야별로 나눠 수행하고 있다. 미국의 국토안보부는 연방정부, 주정부 및 기업들간 협력강화를 위해 정부부처들 산하에 산재해 있던 사이버안보관련 조직들을 통폐합하여 국가사이버안보·통신통합센터(NCCIC)를 창설해 업무효율화를 도모하고 있다는 점을 감안해 우리도 유사기능들을 통합하는 방안 검토가 필요할 것으로 보인다.

참고문헌

국가보안기술연구소,『국가사이버안보전략 워크샵』, 국가보안기술연구소 자료집(2012. 6.20.).

_____,『국가 사이버안보전략 참고자료』, 2012.5, p.VIII-1~VIII-16.

국가안보전략연구원・국가보안기술연구소.『북한 사이버테러 위협과 대응전략』, 국가안보전략연구원・국가보안기술연구소 공동학술회의 자료집(2015. 3.31).

김소정 외. “미국 국토안보부 사이버보안 연구개발 동향 소개.”『한국통신학회』, 한국통신학회 학술대회 및 강연회(2005.12), pp.100-104.

미 국방부.『미국 국방검토보고서(QDR: Quadrennial Defense Review)』(2010. 2).

민경식 외. “미국의 사이버보안 정책과 R&D 전략에 관한 분석.”『Internet & Security Focus』, 통권 제 1호(2013. 1), pp.45-62.

오일석 외. “미국 연방정보보안관리법 소개.”『한국인터넷정보학회 2004 추계학술발표대회 논문집』, 제5권 제2회(2004.11), pp.135-138.

유동열.『사이버공간과 국가안보』, 서울 : 북앤피플, 2012.

이연수 외. “주요국의 사이버안전관련 법・조직체계 비교 및 발전방안 연구.”『국가정보연구』, 제1권 2호(2008), pp.64-72.

정완. “한미 사이버보안 법제 동향에 관한 고찰.”『경희법학』, 제48권 제3호(2013), pp.213-242.

정준현. “북한의 사이버테러에 대한 우리의 대응전략과 과제.”『북한 사이버테러 위협과 대응전략』, 국가안보전략연구원・국가보안기술연구소 공동학술회의자료집(2015.3.31), pp.67-96.

조성렬. “북한의 사이버전 능력과 대남 사이버위협 평가: 한국의 사이버안보를 위한 정책적 함의.”『북한연구학회보』, 제17권, 제2호(2013), pp.119-147.

채재병. “안보환경의 변화와 사이버안보.”『정치・정보연구』, 제16권, 제2호 (2013.12.31), pp.171-193.
한국과학기술정보연구원. “미 국가안보국, 사이버보안 연구를 위한 대학지원 확대.”『KISTI 미리안 글로벌동향브리핑』(2015. 5.14).
한희. “사이버공간과 국가안보.”『사이버공간과 국가안보』, 국가안보전략연구원 학술회의 자료집(2014. 4.17), pp.3-18.
“3.4 디도스 공격, 7.7 대란의 업그레이드판.”『안철수연구소』, 2011. 3. 7.
“KBS 등 전산망에 악성코드 침투!, 북한소행.”『뉴데일리』, 2013. 3.20.
“검찰, 농협해킹, 북 정찰총국이 7개월간 준비.”『동아일보』, 2011. 5. 4.
“국가사이버안전 전략회의”의 발표내용, 2009. 9.13.
“미, 사이버안보 총사령부 NCCIC 문 열어.”『연합뉴스』, 2009.11. 1.
“미 vs 북 본격 사이버전쟁땐 누가 이길까?.”『나우뉴스』, 2014.12. 3.
“미래부・국방부・국정원, 사이버보안 R&D 연구개발 협력강화.”『서울경제』, 2015.12.21.
“베일에 싸인 미국의 비밀 정보조직 : 국가안보국.”『NewDaily』, 2015. 2.31.
“사이버안보 최우선 인식...적국 시스템도 참고해야.”『정보보안뉴스』, 2013. 7. 4.
“세계의 정보기관 미국편, NSA・NRO・DIA, CIA보다 은밀한 미국의 눈.”『이투데이』, 2012. 4. 5.
“오바마 대통령도 중국 해킹 비판.”『디지털타임스』, 2013. 3.14.
“정부, 국가 사이버위기 종합대책 확정발표.”『보안뉴스』, 2009. 9.14.
“정부, 국가사이버안보 종합대책 수립.”『미래창조과학부 보도자료』, 2013. 7. 8.
“정부, 사이버안보 마스터플랜 무엇을 담았나.”『전자신문』, 2011. 8. 8.
“주요국의 사이버테러 대응실태 고찰.” www.bluetoday.net(검색일 : 2016. 3.30)
“한미 사이버보안 공조강화...해킹정보 공유.”『머니투데이』, 2016. 3. 6.
Presidential Policy Directive(PPD-20) (TOP SECRET/NOFORN), pp.1-18.
http://ko.wikipedia.org/wiki 및 https://en.wikipedia.org/United_States_Cyber_Command, 미국 사이버사령부.

http://ko.wikipedia.org/wiki, 7.7 DDoS 공격.
http://ko.wikipedia.org/wiki, 미국 국토안보부.
http://ko.wikipedia.org/wiki, 및 http://www.nsa.gov, 미국 국가안보국 홈페이지.
http://www.ajunews.com.view/20150113094601498, 2015.1.13.
http://www.defense.gov/qdr, 미국 국방부 홈페이지.
https://en.wikipedia.org/Central_Security_Service, 미국 중앙안보원
https://en.wikipedia.org/wiki/united_states_strategic_command, 미국 전략사령부.
www.armyrecognition.com, 2015.1.14.

Abstract

Characteristics and Its Implication of the US Cyber Security Governance System

Wan Joo, Jeon (Institute for National Security Strategy)

In the US cyber security governance system, White House is in charge of controlling national cyber security. In December of 2009, president appointed Cyber security Coordinator and also established Office of Cyber Security and Information Assurance to lead national cyber security policy. In May of 2010, Department of Defence established US Cyber Command which is to protect and manage military network, while Department of Homeland Security's National Cyber Security and Communications Integration Center are in charge of cyber security in the private sector.

Functions of government institutions which deal with cyber security are introduced by Homeland Security Act. It has unusual structure that a head of NSA with a mission of collecting signal intelligence is also the head of US Cyber Command. Although DHS should bear all the responsibility to operate national network, US Cyber Command keeps its own organization separated from DHS to control security of national network.

As a head of the US Cyber Command holds his position as a head of NSA concurrently, he can use signal intelligence, imagery intelligence and international state of affairs intelligence to take care of national cyber security issues.

In Korea, cyber security governance system under the control of Blue House is made up of Ministry of Science, ICT and Future Planning for the private sector and Ministry of National Defense for the defence sector. National Intelligence Service is in charge

of directing working-level of cyber security.

As frequent accidents of leaking information about nuclear facility have occurred recently, there is a growing concerns that national cyber security governance system has to be modified and improved.

In this situation, now we need to examine organizations' functions and roles of US national cyber security governance system, expecially, Office of Cyber Security and Information Assurance of the White house, US Cyber Command of Department of Defense and National Cybersecurity and Communications Integration Center of DHS. It is important that we take lessons from the US case to improve the Korean cyber security governance system.

Key Words: Office of Cyber Security and Information Assurance, US Cyber Command, NCCIC, NSA, National cyber security governance system, Cyber terrorism, DDoS

투고일 : 2016.10.20. 심사일 : 2016.11.20. 게재확정일 : 2016.12.10.

III

중국의 사이버 안보법제와 우리의 대응: 중국 『사이버안전법』(Cyber Security Law)을 중심으로

윤봉한 (국가안보전략연구원)

Summary

중국은 2016년 11월 7일 「사이버안전법」을 제정하여 사이버공간에서의 국가주권 개념을 확립하는 한편, 자국내 인터넷 기업과 개인 사용자에 대한 관리 통제를 강화하였다. 「신 국가안전법」 「테러방지법」과 함께 중국은 사이버안보 정책을 규율하는 법률체계를 완성하게 된 것이다.

중국의 사이버안보 정책은 시진핑 주석이 조장으로 있는 「중앙인터넷안전정보화영도소조」를 중심으로 이루어진다. 시진핑의 '총체적 국가안보관'을 반영하고 있는 사이버안보 정책은 '사이버상 국가주권과 안보, 공공의 이익 확립'과 '대내안정을 위한 네트워크 통제강화'가 핵심 내용이다. '시'주석은 조직의 리더로 전례없이 인터넷 안보와 정보관리를 정책의 우선순위에 두고 있다. 중국은 이제 자국의 인터넷 기반시설 보안을 확충하면서 대외적으로 인터넷 대체기구를 만들려고 할 것으로 보인다.

「사이버테러방지법」이나 독자적인 사이버 감독기관이 없는 우리나라는 국가안보와 국민안전을 위해 정보기간자산과 네트워크 안정을 확보하기 위한 법제를 신속히 정비하여야 한다. 북한이 노리는 국가 및 기밀정보 보호 수준을 높여가면서, 사이버보안 관련 국제활동에 적극 동참하여 협력관계를 증진해 나가야 하겠다.

| 키워드 | 사이버안보(전), 사이버주권, 정보기간자산, 사이버정책, 사이버 감시

1. 서론

오늘날 사회는 네트워크 공간에서 생성되는 정보가 인간의 생활을 주도하는 정보지배사회가 되었다. 사물인터넷(IoT), 클라우드 컴퓨팅, 빅 데이터 등 신기술의 등장으로 IT와 ICT 기술이 국가 경쟁력을 선도하고 있으며, 국가 고유의 경제와 안보문제에 있어 새로운 과제로 부각되고 있다. 사이버공간과 물리적 공간이 융합된 시대가 되면서 국제사회의 사이버 및 네트워크 환경에 대한 의존도가 심화되고 사이버안보와 보안문제가 국가안보의 가장 큰 도전 요소로 등장하였다. 사이버공격은 세계경제포럼이 2016년 발표한 'Global Risk Report 2016'에서 테러를 능가하는 글로벌 위험요인으로 선정되기도 하였다. 발생가능성(likelyhood)과 파급력(Impact)이라는 두 요인을 반영하여 선정된 29개의 주요 글로벌 리스크 요인에 기후적응실패, 수자원 위기 등과 함께 '주요 정보인프라 파괴', '데이터 사기 및 절취' 와 같은 대규모 사이버공격이 핵심 위험요인으로 선정된 것이다.[1] 국가가 사이버공간에 대한 지휘통제시스템과 통신능력을 보전하지 못하면 국가안보와 국민의 안전에 돌이킬 수 없는 결과를 초래할 수가 있다.[2] 사이버 공격이 본격적으로 국가안보위협 문제로 대두된 것은 2007년 에스토니아 정부가 디도스(DDoS) 공격을 받아 3주 동안 국가 마비사태를 겪었던 경험에서 비롯된다. 최근에는 국가 산업기반시설에 대한 집중 원격감시 제어(SCADA : Supervisory Control And Data Acquisition)나 산업제어시스템(ICS : Industrial Control System)을 공격하여 국가전략시설이나 지휘 통제망을 무력화시켜 심각한 안전문제를 야기하거나 국민들의 생명과 재산상 손실을 가져오기도 한다. 이와 같이 오늘날 사이버 영역에서 제기되는 안보위협은 사회 안정과 국가안보를 위협하는 수준까지 위험 요인화되고 있다.

중국은 2016년 11월 7일 제12차 인민대표대회 상무회의에서 그동안 미루어 오

1) *World Economic for global Risk Report 2016* 참조.
2) 우리 정부는 2016.11.18. 구글 측의 정밀지도(1:1000) 제공요청을 "국가안보상의 이유 등"을 들어 거절한 바 있다.(biz.chosun.com/svc/news/ 참조, 검색일: 2016.11.18.)

던 「중화인민공화국사이버안전법」(이하 「사이버안전법」으로 약칭)을 통과시켜 시행에 들어갔다. 지난 2015년 1월 「신 국가안전법」을 시행한데 이어 사이버상에서 공격과 범죄, 유해정보 확산 위협으로부터 국가 주권과 안보, 공공이익을 확보하기 위한 법제적 근거를 완성한 것이다. 중국은 사이버 공간을 '국가간 경쟁의 새로운 고지'이며 상대 국가의 군사적 우위를 상쇄할 수 있는 '비대칭 전력의 한 분야'로 인식하고 있다. 2015년도 국방백서인 『China's Military Strategy(戰略學)』에서 '사이버 군사력 개발 촉진'을 천명하며 "사이버·미사일 등 비대칭 전력 강화에 주력할 것"이라고 밝히고,[3] "적극 방어" 개념과 함께 "정보화한 지역전쟁에서의 승리"를 강조하고 있다.[4] 이 백서를 통해 중국이 사이버공간에서의 활동에 대한 중요성을 깊이 인식하고 공격적인 사이버 활동을 전개해 나가겠다는 입장에 있다는 것을 알 수 있다.

아래에서는 최근 중국 정부의 「사이버안전법」제정을 계기로 관심을 불러일으키고 있는 중국의 사이버안보와 관련한 법제와 정책을 살펴보기로 한다. 중국은 「사이버안전법」제정 등을 계기로 내부적으로 사이버 공간을 보다 효율적으로 통제함으로써 국가안보를 확고히 보장하면서, 외부적으로는 다양한 정책과 제도를 정비하여 미국 등 서방세계가 주도하는 세계 네트워크 질서로부터 자율성 확립을 추구하고 있다. 시진핑 정부는 사이버공간을 사회전반의 통합과 국가안보를 확보하기 위해 체계적으로 관리하고 통제해야 할 핵심 영역으로 인식하고 대내외로 사이버 영역에 대한 영향력을 현저히 확대시켜 나가고 있다. 본 연구는 주로 중국 정부에서 발표한 각종 사이버정책과 공개된 법률체계 등과 같은 문헌자료를 기초로 하였다. 따라서 복잡한 권력·행정 구조를 가진 중국 정부의 내밀한 정책을 구체적으로 살펴보는데 어느 정도 한계가 있을 수 밖에 없었다. 하지만, 중국은 정치·경제·문화적인 분야에서 뿐 아니라 사이버 공간에서도 우리와 밀접하게 교류를 하고 있다는 점에서 중국의 사이버안보 법제 강화가 우리에게 제기하는 시사점이

3) 이상호, "새로운 도전: 국가 사이버 위협 및 사이버," 『신안보연구』, 제1권, 1호(2016 여름), p.39.
4) Elsa Kania, "China: Active Defense in the Cyber Domain," *The Diplomat*, 2015. 6.12.

무엇인지를 살펴보는 것은 의미가 있다고 본다. 이러한 관점에서 본 논문은 중국의 사이버 관련 정책과 법제에 대한 전반적이고 일반적인 이해를 통해 우리나라가 사이버공간에서 국가안보를 확립하는데 필요한 정책적 대안을 제시하는 것을 목적으로 하고 있다.

본 논문은 1장에서 사이버안보 개념의 등장, 국제사회와 중국정부의 대응 자세를 살펴보고, 2장에서는 중국 정부의 사이버안보 정책의 도입과 진화, 특성에 대해 기술한 다음, 3장과 4장에서 정책의 근간이 되는 안보법제 내용 및 평가를 거쳐 제5장에서 정책적 대안을 검토해 보는 것으로 구성하였다.

다만, 중국은 「신 국가안전법」·「사이버안전법」등에서 살펴 볼 수 있는 바와 같이 '안보' 또는 '보안' 개념을 '안전'으로 통칭하고 있는 것으로 파악되었다. 이는 「신 국가안전법」의 내용이 우리의 「국가보안법」내용과 매우 유사하다는데서 읽을 수 있다. 따라서 본 논문에서는 기술상 법 명칭을 제외한 나머지는 '사이버안보'로 통일하기로 한다.

2. 중국의 사이버안보 정책

가. 중국의 사이버안보 개념의 태동과 발전

(1) 사이버안보 개념의 태동

전 세계적으로 인터넷 공간이 국제사회 질서에서 국가안보 영역의 주요 개념으로 등장한 것은 그리 오랜 일이 아니다. 2013년 UN의 '국가전문가그룹'(United Nation's Group of Governmental Experts)에서 사이버공간에서 개별 국가의 행위를 규제할 수 있는 헌장과 국제법 제정이 필요하다는 합의를 도출한 것을 계기로 사이버공간에서의 국가주권 개념이 국제사회의 핵심쟁점으로 부각되었다.[5]

5) Mikk Raud, *China and Cyber: Attitudes, Strategies, Organization,* Nato Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia(2016), p.7.

사이버 안보는 전통적인 안보의 개념에서 확장된 개념으로, 사이버공간의 국제화, 세계화와 더불어 대두된 국가안보, 국민안전 등에 대한 위협에 대한 대응활동을 의미하는 비전통적 안보영역이라고 할 수 있다.

중국에서 국가안보에 대한 개념은 덩샤오핑[6]이 정권을 장악하고 있던 1990년대 이전 시기와 그 이후시기로 구분해서 살펴 볼 수 있다. 덩샤오핑 이전 시기가 군사안보에 초점을 맞춘 전통적 안보관에 초점을 두고 있었다면, 그 이후는 개혁개방을 통해 중국 정부가 세계 질서에 편입되기 시작한 시기로 비전통 안보영역까지 포함하는 신안보관이 자리매김하고 있다.[7] 시진핑 주석이 주장하는 '총체적 국가안보관'도 신안보관의 연장선에서 파악하여야 한다. 이러한 중국 안보관의 변화는 세계질서 속에서 중국의 위상과 역할이 증대된 사실과도 깊은 연관이 있는 것으로 보인다. 냉전시기 중국의 안보관은 '생존'을 위한 안보, 즉 군사안보에 초점을 맞춘 전통적 안보관이었으며, 1980년대 개혁개방 이후 경제안보 등 종합안보 차원의 비전통 영역과 국제협력분야까지 확대된 신안보개념이 자리잡게 된 것이다.[8] 1980년부터 시작된 '도광양회(韜光養晦)'[9]의 기조가 유지되는 가운데 2003년에는 '평화굴기(和平崛起)'[10]가 강조되었다. 이는 장쩌민(江澤民)과 후진타오(胡錦濤) 집권 시기에 중국에서 강조되었던 '신안보관'을 상징하고 있다. 이어 시진핑 등장과 함께 주동작위(主動作爲)[11]를 외치며 새로운 시대에 부합하는 '총체적 안보관'으로 진전시키게 된다.

중국이 사이버공간에서 주권 개념을 공개적으로 주장하고 나선 것은 2011년

---

6) 덩 샤오핑은 1978~1989년간 중국인민정치협상회의 주석, 중화인민공화국 중앙군사위원회 주석 등을 역임한 소위 중국 공산당 2세대를 이끌었던 인물이다(위키백과 참조)
7) 김순수, "중국의 '중앙국가안전위원회' 설립에 관한 연구," 『민족연구』, 63호(2015. 10.) p.5.
8) 김순수, 위의 글. p.8.
9) 도광양회(韜光養晦)는 '자신의 재능이나 명성을 드러내지 않고 참고 기다린다'는 내용으로 덩 샤오핑이 권력을 잡고 있던 1980년대 중국의 대외정책을 일컫는 말. (m.blog.naver.com 참조)
10) 평화굴기(和平崛起)는 '평화롭게 우뚝 선다'는 의미로, 2003년 당시 중국 주선 후진타오(胡錦濤)가 군사적 위험없이 평화를 추구해 나간다는 것을 천명한 외교노선. (m.blog.naver.com 참조)
11) 주동작위(主動作爲)는 '대외정책에서 해야 할 일을 주도적으로 한다'는 의미로 시진핑 정권의 대외정책의 기조를 나타내는 말.(m.blog.naver.com 참조)

UN 총회에서 중국 주도로 러시아 및 중앙아시아 국가들로 구성된 '상하이 협력기구'(Shanghai Cooperation Organization)를 통해 국제 인터넷주소관리기구(ICANN)에 대한 대안체제를 주장하고 나서면서 공식화 되었다고 볼 수 있다.[12] 당시 중국의 주장은 한 국가의 내부 인터넷을 사용하는 내국인은 물론 외국인도 주재국의 정책과 법률을 준수하도록 하여야 하며, 사이버공간에서 제3국의 간섭을 받지 않는 국가주권 확립이 필요하다는 것이었다. 이러한 중국의 사이버공간 주권확보에 대한 공고한 입장은 사이버공간에 대한 자국내 인터넷 사용 통제강화와 세계질서 속에서의 국가안보 확립의 차원으로 발전하였다. 2014년 3월 프랑스를 방문한 시진핑이 "사자는 이미 깨어났다"라고 공언[13]한 것은 첨단 과학문명 시대의 특징과 추세에 바탕한 중국의 대외 자신감에 비롯된 국제사회에서의 위상을 확보하고자 하는 의지를 반영한 것이라고 볼 수 있다.

이러한 신안보관을 배경으로 중국 정부가 이번에 「사이버안전법」을 제정한 것으로 판단된다. 2015년도에 「신 국가안전법」제정에 이어 「사이버안전법」을 제정함으로써 중국 정부가 '사이버안보'의 개념을 신안보 개념의 일부로 인식하고 있음을 명확하게 보여주고 있다.

(2) 사이버안보 개념의 진화

중국의 인터넷 관련 연구는 일찍이 1988년경 중국 컴퓨터과학기술인터넷(CANET) 사업이 시작되어 대학과 연구센터 컴퓨터를 세계 인터넷 망과 접속하게 된 것이 출발점이다. 1993년 12월 국무회의 의결로 국가경제정보화연석회의(國家經濟信識化連席會議)가 상설기구로 등장하였으며, 이듬해인 1994년 2월에 '컴퓨터 정보시스템 안전보호 조례'(국무원령 제147호)를 제정 시행하였다. 이 조례는 그 명칭에서 볼 수 있듯이 컴퓨터 정보시스템의 안전을 보호하기 위한 것이었다. 1996년 8월 「국가정보화영도소조」가 설치되고 당시 중앙정치국 상무위원이

12) Mikk Raud, 앞의 글, p.7.
13) 이지훈, "중국의 새로운 방공식별구역 정책과 한국의 대응전략 : 법률전의 전개", 『신안보연구』, 제1권, 1호(2016 여름), p.83.

자 국무원 총리인 주룽지가 조장을 맡으면서 국가와 사회의 정보화 사업이 중국 정부의 최우선 과업의 하나로 추진되게 되었다. 2005년 11월 국무원에서 '국가정보화발전전략 2006-2020'을 통과시켜 정보보안과 관련한 각종 법규와 제도를 정비하여 왔다.[14]

인터넷 공간에 대한 국가적 인식은 2011년 5월 출범한 「국가인터넷정보판공실」이 설립된 것에서 비롯된다. 이 기구의 목적은 인터넷 구축 및 발전과 관리를 강화하고 가상 사이버 공간에 대한 관리수준을 향상시키는 것으로, 국가 차원에서 사이버를 더욱 중시하는 계기가 되었다. 이후 2013년 11월 중국 공산당 제18기 회의에서 "법에 의거하여 인터넷에 대한 관리를 강화하고, 국가인터넷과 정보안전을 확보하여 국가안전과 사회안정을 수호하도록 한다"는 결의를 채택하였다. 2014년 2월 「중앙인터넷안전과 정보화영도소조」를 설립하고 시진핑 총서기가 조장에 취임함으로써 "인터넷 안전수호"가 국가적 과제로 등장하게 되었으며, 2016년 11월 「사이버안전법」을 제정함으로써 '사이버안전'(사이버안보)이 국가안보와 사회안전을 확보하는 신안보 개념의 일부로 법제화되기에 이르렀다.

나. 중국 정부의 사이버안보 정책 기조

(1) 중앙정부 주도의 사이버안보 정책

중국의 사이버 정책은 2016년 6월 현재 총 인구의 49%에 해당하는 7억1천여만 명(전세계 인터넷 사용자의 21%)이 인터넷을 사용하고 있고,[15] 연 평균 30%식 성장하는 정보통신산업 고도화와 밀접한 관련을 갖고 추진되었다.[16] 또한 2015년 기준으로 1000만대 이상의 컴퓨터가 디도스(DDoS) 공격과 관련된 좀비 PC로 이용되는 등 매년 사이버공격으로 인한 물적 피해가 80%씩 급증하고 있는데 따른 정보환경의 개선을 목적으로 이루어지고 있다. 중국 정부는 2015년 기준으로 트

14) 김한균, "동북아 사이버범죄 및 보안 지역협력방안," 『형사정책연구』(2015.12) pp.55-58.
15) Mikk Raud, 앞의 글, p.5.
16) IGCC, "China and Cybersecurity: Political, Economic, and Strategic Dimensions," *SITC* (2013.4.) p.5.

로이목마 바이러스(Trojans), 봇넷 등 공격의 40% 이상이 해외에 위치한 IP에서 출발하는 것으로 파악하고 있다.[17]

앞에서 살펴본 바와 같이 중국 정부의 사이버 정책은 2014년 「중앙인터넷안전정보화영도소조」를 설치한 것을 전후하여 결정적인 변화를 맞게 된다. 그 이전까지 정보정책은 「국가정보화영도소조」를 중심으로 운영되어 오다가 2014년 2월에 당・정・군으로 나뉘어진 정보기술 발전과 관리체계를 일원화하고, 부처간 유기성을 강화하여 기술발전과 인터넷 사용확대에 따른 정책 집행의 효율성을 높이고자 공산당 정치국 상무위원회 산하로 「중앙인터넷안전정보화영도소조」를 내오게 된 것이다. 시진핑 주석이 직접 조장을 맡아 국가 정보기반시설 확충과 제도개발을 진행시키고 있다.

2015년 광대역 인터넷 네트워크 보급을 시작하면서 '인터넷 경제발전' 개념을 처음으로 도입하였고, 과학기술 진보와 혁신을 바탕으로 하는 경제구조 조정을 서두르고 있다. 안정적 인터넷 경제 발전을 위한 인터넷 보안과 네트워크 안전을 강화하는 정책을 적극적으로 추진하고 있다. 「중앙인터넷안전정보화영도소조」의 출범은 중국 지도부가 국가안보 차원에서 인터넷과 네트워크의 보안에 대한 중요성을 인식하고 사이버안보 강화를 위해 적극적으로 활동하기 시작했음을 국내・외에 알리는 출발점이 되었다. 또한, 시진핑 주석이 직접 이 조직의 조장을 맡아 지도하고 있다는 점에서 중국정부가 얼마나 심각하게 사이버안보의 중요성을 인식하고 있는지를 단적으로 보여주고 있다.

(2) 중국 사이버안보 정책 내용

중국의 사이버안보 정책은 국방과 군사영역에서의 정보화 과정을 통해 살펴 볼 수 있다. 이것은 사이버안보 정책이 중국 인민해방군(PLA)을 중심으로 진행되어 왔기 때문이다. 국방기술 발전과 군사전략 다변화를 통해 국내・외로부터 제기되는 위협으로부터 네트워크와 인터넷을 보호함으로써 사회안전을 유지하고 국가

17) 정종필, "사이버안보의 주변 4망(網)과 한반도, 중국의 사이버 안보 전략," 네크워크세계정치 세미나 자료집(2016.4.25.), pp.34-35.

안보와 국민경제를 보장받고자 하는 것이다. 군에 대한 정보화는 2010년경부터 군내 IT 전문 인력을 충원하고 차세대 위성 네트워크를 구축하는 등 정보 인프라를 강화하게 되었으며, 재래식 무기 운영을 원활하기 하기 위한 소프트웨어 및 군 지휘 전용 프로그램을 개발하게 되었다. 2013년 미국을 비롯한 외부의 사이버 침해가 격심해 지기 시작하고, 특히 미 국가보안국(NSA) 직원 스노든이 "미국이 전 세계 정부와 언론을 대상으로 도청과 해킹을 하였다"고 폭로한 것을 계기로 사이버공간을 중요한 안보영역으로 받아들이고 중앙정부 차원에서 과학기술교육을 지원하게 되었다. IT기술 전문가를 본격적으로 육성하고 국내 인터넷과 IT기술에 대한 보호전략을 수립하였으며, 군 전용 인트라넷을 구성하고 군 지휘통제 시스템을 보호하기 위한 모의훈련을 실시하는 등 정보전에 대비한 군사훈련 실시하였다.

이러한 중국의 사이버안보 전략은 2015년부터 적극적인 방어 방식을 적용하여 국가안보와 사회안정을 위한 컨트롤 타워를 중앙군사위원회로 일원화하게 된다. 사이버전에 대비하여 중앙군사위원회에 정보전을 담당하는 부처(3부처와 4부처)를 신설하고 네트워크 전쟁에 대비하여 사이버공간에서 적의 시스템을 파괴함으로써 보안능력을 약화시키는 전략을 수립하였다.[18]

한편, 중국의 사이버정책은 대내적인 측면과 대외적인 측면에서 나누어 생각해 볼 수 있다. 중국 정부의 대내 사이버정책은 네트워크와 데이터를 보호하기 위해 접근해오는 대상을 모니터링하고 차단하기 위한 대책을 내오는 한편, 대외적으로는 자국의 정보 탈취를 시도하는 적의적 행위에 대해 대상 시스템을 적극 공격하는 전략을 수립하게 되었다. 이를 위해 중국은 미국 주도의 사이버세계를 벗어나서 국가주권을 보장하는 새로운 국제규범(Global Governance)을 만들기 위해 상하이협력기구(Shanghai Coopertion Organization: SCO)와 아세안지역안보포럼(ARF) 활동을 강화하면서, 러시아를 포함한 아시아・태평양지역 국가들과 협력을 확대해 나가고 있다.[19]

---

18) 2013년 중앙군사위원회 3부처 소속 61398부대 해킹요원 Sun Kailang 등 5명이 미국의 경제 및 무역기밀을 해킹한 혐의로 FBI의 수배를 받고 미 연방법원에 기소된 사건이 있었다.

19) 정종필, 앞의 글. pp.36-37.

(3) 중국 사이버안보 정책의 주요 특징

(가) 국제사회에서의 '사이버주권' 확보

중국의 대외 사이버안보전략 정책이나 전략에 대한 내용은 거의 알려지지 않고 있어 정확한 내용을 파악하기는 힘들지만, 미국, 러시아와 함께 가장 강한 사이버 역량을 구비하고 있는 사이버 강국이라는 사실은 잘 알려져 있다. 중국은 사이버 공격에 대한 역량을 '국제사회에서 경쟁의 새로운 고지'이며, '적들의 군사적 우위를 상쇄할 수 있는 새로운 무기'로 인식하고 있다. 사이버공간을 국가주권 차원에서 안보전장의 하나로 간주하고 있는 것이다. 사이버공간에서의 안전확보가 국가주권, 안보 및 경제적 이익에 결정적인 역할을 할 것으로 보고, 국내는 물론 해외에서 인지되는 사이버위협으로부터 안전을 보장하기 위해 '사이버주권'을 확보하고 신장시켜 나가려고 노력하는 것이다. 러시아 등과 협력하여 미국의 지배적 구조 하에 있는 사이버 공간을 이탈하여 독자적인 사이버 국가 주권을 확보하고 행사해 나가겠다는 의도를 노골적으로 내보이고 있다. 이는 사이버 영역에 대한 지배를 확고히 하여 사회안정을 확립하면서 군사적으로 강력한 역량을 구축하여 중국 공산당의 지배적 위상을 확립하겠다는 목적을 가지고 있다. 중국에서 활동하는 외국 계열의 ICT 관련 업체에 대해 새로운 규칙과 제재를 부과하고, 국가안보 및 대테러 정책을 강화해 나가겠다는 것이다.

인터넷 주권에 대한 중국의 강한 욕망은 시진핑 주석의 발언 내용에서도 읽어낼 수 있다. 그는 "현대의 인터넷 공간이 다양한 이해관계를 효과적으로 반영하지 못하고 있다"며, "인터넷 주권은 국가적 차원에서 가져야 할 '당연한 권리'로서 국내에서 적절한 규제권한에 대한 내용까지 확대되어야 한다"고 강조하였다. "주권이 없는 사이버공간은 의미가 없다"며, '세계 인터넷규칙'에 사이버 주권을 명기하자는 것이다.[20] 미국이 국제 인터넷주소자원 관리기구(ICANN: International Cooperation for Assigned Names and Numbers)를 관리하고 있어 과도한 영향력을 피할 수 없으며, 이는 미국이 슈퍼파워로서의 한 원동력이 되고 있다는 것이다.

20) 최진홍, "중국의 인터넷 주권 화두, 위선과 위선의 대결," 『이코노믹리뷰』, 2015.12.20.

이러한 중국의 인식은 애플, 구글, 페이스북, 마이크로소프트 등 세계 유수의 인터넷 기업들에 대한 규제 태도에서도 나타나고 있다. 즉 중국은 이들 기업들을 대상으로 ① 중국의 국가안보를 해치지 말아야 하고 ② 중국인 사용자들의 자료는 중국내에 보관하여야 하며 ③ 중국정부의 사회전역에 대한 감시를 수용해야 한다는 내용의 서약서에 서명하도록 하고 있다.

「사이버안전법」발효를 계기로 중국은 대정부 비판가, 망명자 및 외국계 회사 등으로부터 제기되는 사이버 주권에 대한 위협을 감지해내면서, 방화벽 '만리장성(Great Firewall)'으로 구축한 "사이버국경"을 현실화 시키기 위해 으로 더욱 공세적이고 적극적으로 사이버주권 정립 주장을 하고 나설 것으로 보인다.

(나) 사이버전 대응 역량 구축 노력

자국을 대상으로 한 사이버공격에 대해 '비례적 대응'을 공개적으로 천명하고 있는 미국을 제외하고 세계 어느 나라도 사이버공격에 대응한 응징이나 보복을 적극적으로 주장하는 국가는 없다. 중국도 마찬가지로 사이버공격에 대응한 대응방침을 명문화하고 있지는 않다. 하지만, 중국이 사이버공간에서 직면하고 있는 안보위협을 심각한 상황으로 받아들이고 전략적 경쟁에서 우위를 확보하기 위해 노력하고 있다는 사실은 명백해 보인다. 미래전쟁이 네트워크전으로 진화할 것이라는 예상에 따라 사이버전력 강화를 촉진하고, 사이버 위협 감지와 방어능력 향상을 위한 다양한 대책들을 내오고 있는 것이다. 국외로부터 제기되는 지속적인 사이버 침해로 중국 국가안보와 국민경제가 피해를 입고 있다는 판단에 따른 것이다.

중국은 1997년 4월 인민해방군 소속 중앙군사위원회 주도로 컴퓨터 바이러스 부대를 창설하였다. "컴퓨터 바이러스를 침투시키는 것이 원자탄을 사용하는 것보다 더 효율적"이라는 판단에 따라 창설되었다고 한다.[21] 이어 2000년 2월 '인터넷 기초총부'로 불리는 사이버전 부대(Net-Force)를 창설하였고, 각 군구별 사이

21) 김필재, "中 인민해방군 '제4군' 사이버 전담부대 분석," 『조갑제닷컴』, 2015. 1.11.

버군대를 구성하고 있다. 한편, 인터넷 검열시스템인 '만리장성'(Great Firewall of China)을 구축하고 모든 기업과 국민들의 인터넷 활동을 감시하고 있다. 중국의 사이버공간에서의 국가안보에 관한 인식은 2013년 12월 중국 '군사전략학'(SMS; The Science of Military Strategy, 이하 '전략학')에 잘 나타나고 있다. 거기에는 "국가의 주요 정보 및 정보네트워크의 안전에 대한 방어대책 수립" 전략이 실려 있다. 핵심내용은 "방어에 중점을 두되, 공격과 방어를 동시에 고려"(以防爲主, 兼慮進攻)한다는 것이다. 이를 위한 사이버군을 사이버전특수군(軍隊專業網戰略戰力量), 인민해방군대응역량(授權力量), 민간역량(民間力量) 등 3가지 형태로 구분하고 있다.[22] 2015년 발간된 전략학에서는 사이버국경보호, 사이버주권 및 국가안보 확립(守護網絡邊疆, 擔保網絡主權和國家安全)이라는 보다 향상된 사이버안보 전략을 설명하고 있다. 여기서는 "적극방어, 미래전쟁 승리(積極防禦, 葛制幷打 및 未來戰爭)와 정보우위 확보(爭取網絡制權)를 강조하고 있다. 여기서 주장하는 사이버공간 방어의 개념은 ① 중국의 사이버주권(網絡主權)과 사이버국경(網絡邊疆) 방어, ② 사이버군지휘구조확립(網絡空間力量領導體制) 내용으로 하고 있다.[23]

사이버공격과 관련해서 중국은 1990년대 중반부터 군사력으로는 상대가 되지 않는 미국을 상대로 비대칭전력을 핵심으로 하는 '점혈(点穴, 급소)' 전략을 구사하고 있는 것으로 알려졌다. 점혈전략(点穴戰略)'이란 약한 것으로 강한 것을 대적하며 실한 것은 피하고 허한 것을 공격한다는 전략이다. 대규모 첨단전력으로 구성된 미군의 급소를 공격해 마비시킨 뒤 전세를 역전시킨다는 것이다. 중국 국방대학은 97년 사이버전과 관련한 '점혈전략' 개념을 도입하고 "전자(사이버) 공격의 우선순위는 상대방이 가진 전자 시스템의 약점과 급소부위를 핵심 대상으로, 그 혈을 눌러 전체를 마비시킴으로써 최대의 작전 효과를 추구한다"고 밝히고 있다.[24]

---

22) Elsa Kania, "China Brief: the Latest Indication of the PLA's Network Warfare Strategy," The JamesTown Foundation, *China Brief Volume,* 15(24)(2015.6.)

23) Simon Elegant, "Cyberwarfare: the Issue China Won't Tuch," *Time Megazine*, 2009.11.18.

(다) 네트워크에 대한 강력한 통제

중국의 사이버공간 규제는 서구 국가로부터 표현의 자유를 통제하고 인권을 침해하고 있다는 비난을 받을 정도로 심각한 상황으로 알려지고 있다. 인터넷을 포함한 미디어 전반에 대해 엄격한 규제를 가하고 있기 때문이다. 국제엠네스티 동아시아사무소 조사국장 로젠 라이프는 "중국 정보는 온라인상 규칙을 새로 규정함으로써 검열과 감시가 만연한 환경을 만들려고 하고 있다"며, "이는 인터넷에 대한 전면적인 공격이다"라고 비난한다.[25] 전체 국제 광대역의 80%를 점유하는 ChinaNet과 China169이라는 2大 네트워크를 모두 중국 정부가 관리하고 있기 때문에 거대한 국가 인트라넷(National Intranet)의 형태를 가지고 있어 통제와 규제가 용이한 것이다.[26]

중국에서 인터넷 규제가 본격화한 것은 정보화 수준의 정도와 궤를 같이 하고 있다. 2000년 '전국 인민대표회의 상무위원회 인터넷 보안에 관한 결정'에서는 인터넷상의 유언비어 유포나 유해정보 게시, 체제에 위협되는 정보유통의 통제를 규정하였다. 2010년에는 '국가비밀보호법'을 개정하여 인터넷 및 통신회사가 검열을 받도록 하는 규정을 도입하였다. 특히 중국의 인터넷에 대한 감시강화는 2011년 튀니지 혁명과 2014년 미 국가보안국 직원 스노든이 '미국의 중국 인터넷 검열' 사실을 폭로한 것을 계기로 급격한 변화의 계기를 맞는다. 튀지니 혁명을 기점으로 중동과 아프리카 국가에서 일어난 민주화 시위과정에서 소셜미디어 활동이 커다란 역할을 한 사실을 지각한 중국 정부는 '시나 웨이보(微博, Sina Weibo)를 비롯한 중국내 소셜미디어에서의 정치적 표현을 통제하기 시작했다. 인터넷 가입시 실명등록을 의무화하고 반정부적 표현을 차단하거나 금지시키게 되었다. 2015년 7월 1일 「신 국가안전법」을 제정한데 이어 2016년 11월 7일에는 「사이버안전법」 체계를 출범시킴으로써 개별 인터넷 사용자인 기업과 개인에 대한 온라인 검열도

24) 김민석, "북한 사이버전법은 중국의 '점혈전쟁술' 모방한 것," 2009.7.10.(news.joins.com, 검색일: 2016.10.18.)
25) 최남규, "중국: IT기업들은 중국의 억압적인 인터넷 규제 거부해야,"『국제인권뉴스』, 2015.12.16.
26) 이연수, 이수연, 윤석구, 전재성, "주요국의 사이버안전관련 법·조직체계 비교 및 발전방안 연구,"『국가정보연구』, 제1권, 2호(2008), pp.65-66.

심각한 수준에서 진행할 수 있게 되었다.

중국이 사이버 보안을 강화하고 인터넷에 대한 규제를 강화하는 두드러지는 이유로는 첫째, 전 세계를 연결하는 인터넷을 통해 얻을 수 있는 정보의 흐름이 커지면서 정보가 국력의 크기를 결정할 정도로 영향력을 가지게 되었기 때문이다. 둘째, 중국 내부의 반정부・비판세력, 해외와 연대한 민주세력 들이 인터넷으로 연대결집하고 있어 국가안보에 영향을 미칠 수 있는 수준으로 위협이 되고 있다고 판단하여 사전 정지작업이 필요하다고 보고 있는 것이다. 젊은 층들이 인터넷을 통해 서구의 다양한 문명을 접할 수 있게 되었고 민주적 가치관을 형성하게 되어 반국가 의식을 키우고 있다는 우려가 생긴 때문으로 보인다. 셋째, 미국 등 서구국가로부터 비롯되는 사이버안보 침해가 위험한 수준에 이르고 있어 이에 대항할만한 적정한 무기가 필요하다고 보기 때문이다.

중국의 인터넷 감시와 관련해서 특히 (해외)기업이 제공하는 제품이나 서비스의 안전 여부를 검증하기 위해 중국 정부의 사회 전반에 걸친 모든 검열과 감시를 받아 들이도록 강요하고 있다는 점이 우려가 되고 있다. 중국 정부가 (해외) 인터넷 서비스 기업의 시스템에 직접 접속하여 서비스를 검열하고 영업정보를 비롯한 회사운영 전반에 감시할 수 있도록 한 것이다. 2010년 3월 중국정부의 검열 방침에 반발하여 철수했던 구글이 3개월만에 '중국법을 준수하고 위해(危害) 콘텐츠를 서비스하지 않겠다'는 서약을 하고 중국사업을 재개한 사실에서 사이버 공간에서 갖는 중국의 영향력이 매우 크다는 것을 알 수 있다.

(라) 인터넷 오지 북한의 대외 사이버 창구

북한은 세계에서 유일하게 공개 인터넷과 연결되지 않는 폐쇄체제를 유지하고 있어 사이버안보와 관련한 기구와 활동 능력 등에 대해 알려진 내용이 거의 없다. 중국과 북한 간에 긴밀한 연대관계를 가지고 있을 것이라는 주장은 많이 있지만, 양 집단 간의 구체적인 지원・협력관계에 대해 연구된 논문도 거의 찾아 볼 수가 없다. 하지만, 미국과 함께 사이버공간에서 명실상부한 글로벌 리더로 자리매김하고 있는 중국이 북한의 사이버역량 개척과 발전에 커다란 영향을 주고 있는 것은

분명한 것으로 보인다. 미국 정부는 2014년 소니사 해킹사건 당시 배후에 중국이 모종의 역할을 한 것이 아닌가 하고 의심하였다.[27] 북한이 소프트웨어와 하드웨어를 모두 중국에 의존하고 있으면서, 공격진원지로 중국 지역 IP가 등장하여 중국의 역할을 의심하지 않을 수 없다는 것이 그 이유였다.

중국이 북한의 사이버공격의 배후로 의심받는 이유를 살펴보면 아래와 같이 정리할 수 있다.

첫째, 북한이 대외망으로 중국통신망을 사용하고 있다는 점이다. 체제불안을 이유로 인터넷 대외공개를 꺼리고 있는 북한이 사용하는 인터넷 프로토콜 주소(IP address)는 불과 1000개 남짓에 불과한데, 그것마저 중국 차이나 컴(China Com)을 통해 확보한 4개의 인터넷 회선에서 유발되는 회선이다.[28]

둘째, 중국은 북한 사이버전사들의 양성을 지원하고 있다. 중국 후단대학, 북경대학 등에는 연간 북한 과학 영재 50-60명이 유학을 하고 있으며, 유학을 마친 후 정찰총국 등에서 사이버전 요원으로 활동을 하고 있다.[29] 북한은 중국으로부터 핵심기술을 전수받고 컴퓨터 영재들을 중국으로 유학시키고 있으며, 중국의 IP를 임대하거나 절취하여 사이버공격을 감행하고 있다.

셋째, 중국이 북한의 사이버공격 거점을 제공하고 있다. 인터넷 기반시설이 부족한 북한이 수천 명의 사이버 전사들을 보다 정보화되고 네트워크가 잘 형성되어 있는 중국으로 파견하여 공격활동을 하도록 하고 있다. 북한의 사이버 전사들은 중국에서 안전한 거점을 확보하고 사이버공격을 감행하고 있는 것은 지금까지 우리나라에서 발생한 다수의 북한 대남 사이버테러 공격에서도 밝혀진 바 있다. 2014년 12월 발생한 한국 수력원자력 발전소 해킹사건도 북한 체신청이 사용하고 있는 중국 랴오닝성에 할당된 IP주소로 확인되었다. 2014년 11월 소니픽쳐스 해킹사건이 발생하자 미 국무부장관 존 케리는 중국 왕이 외교부장에게 "해킹이 중국을 출발한 뒤 볼리비아・싱가포르・태국에 있는 서버를 경유해서 수행된 것으

27) "China a Likely in North Korea Cyber Prowess: Experts," *AFP,* 2014.12.26.
28) AFP,앞의 글.
29) 한상미, "북한, 과학영재 50-60명씩 유학 보내 사이버 요원 양성," *VOA*, 2016. 6.14. (www.voakorea.com/a/3375411.html, 검색일: 2016. 11.8.)

로 확인됐다"면서 "중국이 북한의 해킹행위를 차단하는데 협조해 줄 것을 요청"[30]하였으나, 중국은 "그러한 제재가 북한 인민들의 삶의 질을 높이지도 않고 효과적이지도 않다"면서 분명하게 거부한 사실[31]이 있었다고 알려졌다. 중국 보안전문가들에 따르면 중국 동북부지방에서 수 많은 북한 해커들이 거점을 마련하고 활동하고 있다고 한다.[32]

넷째, 북한이 구사하는 사이버공간 전술은 모두 중국의 전략을 모방하고 있다는 것이다. 북한의 사이버 전술은 3가지 형태로 나타나는데 첫째, 대남 도발전 악성코드를 우리나라의 컴퓨터에 잠복-은폐시키는 방법, 둘째, 컴퓨터 인터페이스를 통해 악성코드 침투 후 전체 시스템으로 확산시키는 방법, 셋째, 공장에서 컴퓨터를 생산할 때 발생하는 자기장을 활용해 악성코드를 심거나 또는 간접 자장을 만들어 컴퓨터에 장애를 일으키는 방법 등이다.[33] 이는 바로 중국이 구사하는 사이버전술인 전궤잠복법(前饋潛伏法 - 전쟁 발발전 고체 바이러스를 敵 컴퓨터나 무기에 장착), 간접공격법(間接攻擊法- 바이러스를 전원・출력・온도제어시스템 등 보조시스템에 침투), 접구수입법(接口輸入法- 컴퓨터 인터페이스를 통해 바이러스 침투후 본 시스템으로 확산), 탐측공격법(探測攻擊法- 공장에서 컴퓨터를 생산할 때 발생하는 자기장을 활용해 바이러스를 침투시키거나 또는 간접 자장을 만들어 컴퓨터를 혼란케 함) 등과 구체적으로 일치한다는 것이다.

---

30) 디펜스 21, "사이버위기 직면한 한반도 정세(하), 2014.12.26.(2korea.hani.co.kr/?act, 검색일: 2016.11.18.)

31) Taylor Brooks, "why China Needs to Rein in North Korea's Hackers," *Christian Science Monitor*, 2016.2.5.

32) 김경애, "북한의 사이버위협 대응, 중국 역할 매우 커,"『보안뉴스』, 2015. 9.11. (www.boannews.com, 검색일: 2015.11.17.)

33) 김필제, "북한의 '사이버테러' 전략: 점혈전략,"『조갑제 닷컴』(www.chogabje.com, 검색일:2009.7.11.)

3. 중국의 사이버안보 법제

가. 중국의 사이버안보 법률

(1) 「신 국가안전법」제정과 내용

중국은 2010년 이후 자국을 대상으로 하는 사이버 침해사고가 급증하는 상황에서 2013년 미국 국가안보국(NSA) 전 직원 에드워드 스노든이 미국의 대외 국가들을 대상으로한 통신・인터넷 감청을 무차별적으로 감청하고 있다고 폭로한 것이 「신 국가안전법」을 제정하는 강한 계기가 되었던 것으로 보인다. 스노든의 폭로에서 미 국가안보국이 중국의 주요 지도자와 기업들을 대상으로 첩보활동을 해온 사실이 드러났던 것이다. 이때부터 중국 정부는 사이버공간에서 비롯되는 위협으로부터 국가안전과 국민경제를 보장하기 위한 보안관련 정책을 최우선시 하는 정책을 전개하게 되었다. 강력한 국가안전보장 체계를 구축하기 위해 법 정비를 추진하였다. 1993년 제정되어 첨단 현대 통신사회의 현실을 반영하지 못하고 있는 구 「국가안전법」을 폐지하고 2015년 7월 1일 시진핑의 '종합안보관'을 반영한 「신 국가보안법」을 내오게 되었다.

「신 국가보안법」은 제1조에서 법안 제정의 목적을 "국가안전을 유지하고 인민민주주의 전제 정권 및 중국 특색을 갖춘 사회주의제도를 확립하며 인민의 근본적인 이익을 보호하고 중화민족의 부흥을 실현시키기 위해 본 법을 제정한다."고 밝히고 있다. 나아가 제2조에서 '국가 안전'을 "국가의 주권, 통일 및 영토보전, 인민의 복지, 경제사회의 지속가능한 발전 및 기타 국가의 중대한 이익과 관련하여 상대적인 위기 없이 내외에서 위협을 받지않는 상태"를 의미하고, "그 안전한 상태를 유지하는 능력을 보장하는 것"이라고 매우 포괄적으로 정의[34]하고 있다. 이는 2014년 1월 창설한 「중앙국가안전위원회」활동 근거가 되며, 정치, 경제, 군사 및 사회 등 전 분야에 걸친 전통적 안보와 더불어 우주, 심해, 극지방에서의 중국

34) 신국가안전법 제2조.

의 이익을 수호하겠다는 의지를 담고 있다.

특히 이 법이 '인터넷 주권' 개념을 제시하고 사이버공간에 대한 감독강화를 명문화하고 있다는 사실에 주목하여야 한다. 법 제25조에는 온라인 범죄행위에 대해 통제 관리를 위한 국가의 사이버 공간주권을 수호한다는 내용을 담고 있다.[35] 중국 정부는 사이버 국가안보와 관련해서 국가와 개인간에 법익이 충돌할 경우 그 판단에 대한 법적 기준을 마련한 것이라는 평가[36]하였다.

또한, 중국 정부가 앞으로 인터넷 공간에서 강도 높은 인터넷 검열과 통제를 할 수 있는 근거를 규정하고 있다는 것이다. 내부적으로는 국가체제의 안전성을 확보하는 한편, 중국에 진출해 있는 해외 IT기업들을 통제하려는 의도도 있어 보인다. 중국정부가 이 법을 통해 기도하는 것은 강력한 검열과 높은 수준의 통제로 국가안보의 위협 요인을 조기에 제거하고 사회안정을 기하겠다는 것으로 보인다 중국 정법대(政法大) 마화이더 부총장은 "「신 국가안전법」은 인터넷상 국가의 주권을 확보하는 것으로 국가 안보를 위한 의미 있는 조치"라며, "향후 구체적인 내용의 사이버 관련법을 제정할 수 있는 기틀을 마련하였다"고 하였다.[37]

이와관련 중국주재 한국대사관에서 2015년 7월 "중국 「신 국가안전법」 개정·시행에 따른 교민 유의안내"를 게시한 바 있는데, 중국 주재 각국 정부가 이 법을 얼마나 심각하게 받아들이는지를 단적으로 보여준다. 그 내용을 보면 "「신 국가안전법」은 국가경제안전, 사회주의 핵심가치관 및 중화문화에 대한 안전, 사이버 공간 안전 등을 확보하기 위한 종합적이고 기초적인 성격의 법률인 바, 이 법의 시행과정 중, 유관집행기관에 더욱 많은 재량이 부여될 것"이라며 "확인되지 않은 정보의 온라인상 유포(SNS 포함), 의심스러운 메일의 열람, 미허가 종교집회 개최 및 참석, 타인의 화물 대리운반, 은행업무 대리 등 오해의 소지가 있는 행위에

35) 신국가안전법 제25조 "국가는 사이버와 정보안전 보장체계를 구축하며, 사이버와 정보안전 보호역량을 향상시키고 사이버와 정보기술의 창조연구와 개발응용을 강화하여 사이버와 정보핵심기술, 관건이 되는 기초시설과 중요한 분야의 정보 및 데이터가 안전하고 통제 가능하도록 한다. 사이버에 대한 관리를 강화하고, 사이버공격, 사이버 침입, 사이버 비밀정보, 불법 그리고 유해한 정보의 살포 등 사이버 불법행위를 예방하고 제지하며, 법에따라 처벌하고 국가의 사이버 공간주권, 안전과 발전이익을 수호한다"

36) 문혜정, 앞의 글.

37) 문혜정, 앞의 글.

연루되지 않도록 하라"는 내용[38]이었다.

(2) 「사이버안전법」(Cyber Security Law)

중국 인민대표대회상무위원회는 2015년 7월 고시하였던 「사이버안전법」을 조야의 반대에도 불구하고 2016년 11월 7일 통과시켰다. 이 법은 이미 광범위하게 이루어지고 있는 검열과 인터넷 감시를 법의 이름을 빌려 합법성을 보장받자는 중국 정부의 의지를 법제화 한 것이다. 국가의 인터넷 주권을 지키기 위해 인터넷 서비스 제공자들로 하여금 중국 내에서 인터넷을 이용하는 모든 개인들의 정보를 중국내 설비에 보관하도록 규정하고 있으며, 영장이나 법원의 명령이 없어도 중국정부의 요구가 있을 경우 자료를 제공하도록 명문화한 "사이버 감시법"이라고 할 수 있다.

이미 시행중인 「신 국가안전법」으로도 중국내 인터넷활동을 규제하고 특히 해외 IT기업들의 활동을 충분히 관리 통제할 수 있는 상황에서 새롭게 「사이버안전법」을 제정한 것은 사이버공간에 대한 규제를 더욱 강화하여 사이버테러나 사이버전과 같이 국가적으로 막대한 피해를 야기할 수 있는 예측할 수 없는 안보위협에 적극 대응해 나가겠다는 것이다. 중국 정부는 이 법안은 "사이버 상에서의 공격과 범죄, 유해정보 확산 위협으로부터 사이버공간 주권과 국가안보, 사회 공공이익을 지키기 위한 것"이라고 설명한다. 나아가 "공민・법인・기타 조직의 합법권익을 보호하고 경제사회 정보화의 건전한 발전을 촉진"한다는 것을 제정취지로 하고 있다.[39] 네트워크 보안의 강화와 개인정보보호를 그 목적으로 하고 있다는 것이다. 구체적으로 그 내용은 크게 IT사업자의 사이버 안전 의무, 개인정보, 불법정보로 나누어 살펴 볼 수 있다.

첫째, IT사업자의 사이버안전 의무와 책임을 현저하게 강조하고 있다. 인터넷 네트워크 구축 및 운영 또는 인터넷 네트워크를 통해 서비스를 제공하는 사업자는 반드시 ① 법률 및 행정법규 규정과 국가표준의 요구사항을 따르고, ② 기술적

38) chn.mofa.go.kr/webmodule/common/download.jsp?boardid=13350(검색일: 2016.11.18.)
39) 「사이버안전법」(초안) 제1조

조치와 기타 필요한 조치를 취하여야 하며, ③ 사이버 안전을 보장하면서 사이버 안전과 관련된 사건에 대해 효과적으로 대응하도록 하여야 하고, ④ 법률을 위반하는 범죄활동을 방지하고, ⑤ 인터넷 데이터의 완전성과 기밀성 및 가용성을 유지하여야 한다.[40] 그리고 인터넷 쇼핑몰이나 APP쇼핑몰 개발할 때는 최소한 ① 사이버공격을 예방할 수 있는 시스템, ② 사용자 정보의 안전을 위한 보안유지 장치, ③ 제3자의 전자서명과 전자계약서에 대한 안전저장 등을 구축할 것을 주문하고 있다.[41] 이와 함께 사업자는 인터넷사업일지를 6개월 이상 기록유지를 하도록 하고 있다.

둘째, 국가 핵심정보인프라와 관련해서는 "공공통신과 정보 서비스, 에너지・교통・수리・금융・공공서비스, 전자 정무 등 주요 산업과 분야"와 "또한 기타 파괴로 인해 기능이 상실되거나 데이터가 유출되어 국가 안전, 국가 경제와 민생, 공공이익에 심각한 위험을 초래할 수 있는 핵심 정보인프라"로 설명하고, "사이버 보안 등급 보호제도를 바탕으로 중점적으로 보호한다"[42]고 규정하였다. 그러면서 "핵심 정보인프라의 구체적인 범위 및 보안보호 방법은 국무원에서 제정한다"[43]고 하여 초안단계에서 법안에 포함시켰던 핵심정보인프라에 대한 정의를 삭제하고, 새롭게 국무원에서 그 범위를 결정하도록 하고 있다. 이는 정보통신기술의 진화에 따라 새롭게 등장하는 사이버보안 영역에 탄력적으로 대처하기 위한 것으로 판단된다. 이 법은 국가 핵심정보인프라사업장에 대해 국가의 평가와 심사, 규제를 받도록 하고 있으며, 네트워크 핵심장비와 보안 전용 제품에 대해서도 안전 인증 및 안전검사에 합격하여야 운용이 가능하도록 하고 있다.[44]

셋째, 개인정보보호의 국외유출 방지책을 강화하였다. 인터넷 사업자는 사용자 가입시 온라인 실명제를 실시(제20조)하고, 통신망에 대한 실제 이용자의 신분정보를 제공받도록 하고 있다. 사업자가 개인정보를 수집 및 생산시 반드시 중국 국

40) 「사이버안전법」 제10조.
41) 「사이버안전법」 제21조 등.
42) 김유향, "중국의 네트워크 안전법과 온라인 규제동향," 『KISO저널』, 제20호(2015.10. 1).
43) 「사이버안전법」 제31조.
44) 「사이버안전법」 제37조.

경 내에 저장하도록 하고, 부득이 국경 밖으로 제공할 때에는 사이버정보 주관 부처 및 국무원 유관부처가 정한 방법에 따라 '보안심사'를 받도록 규정하였다.[45] 이 법에 따르면 모든 IT서비스 사업자는 서버를 반드시 중국 국경 내에 두어야 하며, 데이터를 국경 밖으로 이전하는 경우 보안평가를 강제하고 있다. 이는 중국 정부가 '사이버주권'을 행사하겠다는 것이다. 어떠한 분야를 막론하고 데이터를 국외이전 시키려면 국가의 안전평가를 받아야 한다. 구글의 인터넷 지도 요청과 인터넷 택시 '우버'의 서버를 중국 국경 내에 두도록 한 전례도 사이버주권 확보차원에서 벌어진 일이다.

넷째, 국가 사이버안보 활동과 관련된 개별 IT 사업자의 의무를 강화하고 있다. 개별 사업자는 운영과정에서 불법정보를 발견시 전송중단, 제거, 확산방지, 기록보관 등의 조치를 하여야 하고 유관기관에 보고하도록 하였다. 나아가 수사기관에 대한 협조(제23조) 규정을 두고있고, 국가기관은 국가안전과 사회질서 유지 등을 위하여 사업자에게 그 사용을 제한하는 임시조치를 내릴 수 있도록 하고 있다(제50조).

(3) 테러방지법(원명 : 『反恐怖主義法』)

중국 정부는 2015년 12월 27일 『테러방지법』을 통과시켜서 2016년 1월 1일부터 시행하고 있다. 이 법안은 중국에서 통신, 인터넷 서비스를 제공하는 기업들은 테러사건 발생 또는 발생 우려가 있을 경우 중국 정부가 데이터에 접속할 수 있는 장치를 마련하고 암호키를 제공하도록 하고 있으며, 테러정보 관련 언론과 소셜미디어를 통제하는 내용을 담고 있다. 구체적으로 새로운 반테러 기구 및 정보센터를 설립하고, 전문적인 반테러 군대를 창설하도록 하고 있다. 이에 통신 및 인터넷 회사는 '암호해독을 포함한 기술적 지원을 정부측에 제공'해야 하며, 극단주의 테러세력에 대한 '정보유포를 방지'하는 것을 규정하고 있다. 경찰은 총칼을 소지한 상대가 공격해 오는 '긴급상황'에서는 바로 무기를 사용할 수 있으며, 군은 반

45) 『사이버안전법』 제37조.

테러 활동을 위해 해외로 나가 활동을 할 수 있도록 하고 있다. 또한 테러리스트 활동과 관련된 정보를 유포가 금지되며, 발생하지 않은 테러사건을 조작하는 등 정보조작행위도 금지하고 있다. 나아가, 사전에 승인된 미디어 매체를 제외하고는 테러공격이나 정부 당국의 입장에 대해 온・오프라인에서 보도하는 것을 허용하지 않는 것을 내용으로 하고 있다.[46]

나. '사이버안보' 관련 개별 범죄 규제 법규

상기한 내용 이외 사이버공간에서의 발생하는 국가안보 침해행위에 대해서는 형법 각 조항에 내용을 규정하고 있다. 중국의 사이버범죄는 그 대상에 따라 4가지 부류로 나누어 볼 수 있다.

첫째, 사이버 운행 안전을 침해하는 행위는 형법 제285조(컴퓨터정보시스템 불법침입죄 등), 제286조(컴퓨터정보시스템 파괴죄)에서 규정하고 각각의 행위에 대해 유기징역 또는 단기징역과 벌금형을 병행 부과하도록 하고 있다.

둘째, 사이버를 이용하여 국가안전과 사회안정을 침해하는 행위로 유언비어 날조, 비방, 유해정보 전파, 국가전복 선동, 사회주의제도 전복, 국가분열 선동, 국가통일 방해 등 죄를 국가정권전복죄와 국가정권전복을 선동한 죄로 보아 형법 제105조에 규정하고 단기징역에서 무기징역까지 벌을 부과하도록 하고 있다. 이와 함께 사이버를 이용하여 국가비밀, 정보 또는 군사비밀을 절취, 누설한 죄는 형법 제398조, 민족원한, 민족단결을 파괴한 행위는 형법 제249조에서 규율하고 있다.

셋째, 사이버를 이용하여 사회주의 시장경제질서와 사회질서를 파괴하는 행위는 형법 제140조(위조상품 생산 및 판매), 제221조(상업신용 훼손죄), 제21조(지적재산권 침해), 제180조(금융시장 교란), 제 363조(음란사이트 개설죄) 등에 개별 규정을 두고 있다.

넷째, 사이버를 이용하여 개인, 법인 및 기타 조직의 인신, 재산 등 합법적 권리

46) 이에 대한 위반이 있을 경우 벌칙은 최고 5년 이상의 유기징역과 벌금형을 부과 또는 재산을 몰수하도록 하고 있다.

를 침해하는 행위에 해당하는 범죄는 형법 제246조(타인을 모독 또는 비방), 제253조(통신비밀의 침해), 제264조(절도, 사기, 협박)로 규정하고 있다.

다. 사이버안보와 관련한 법률체계의 문제점

지금까지 중국의 사이버안보와 관련한 법률체계를 살펴보았다. 중국은 사이버안보에 대한 관리 강화를 목적으로 하는 주요 3개의 법률을 2015년 이후 줄곧 제정해 온 사실을 알 수 있다. 중국 정부와 각 개별법규 제정취지를 통해 나타나는 법령 제정 목적은 각기 다르다. 먼저 「신 국가안전법」은 "국가안전을 유지하고 인민 민주주의 전제 정권 및 중국 특색을 갖춘 사회주의제도를 확립하며 인민의 근본적인 이익을 보호하고 중흥을 실현시키기 위해" 제정된 것으로 온·오프라인에서의 중국 국가의 안전 확보에 중점을 두고 있다. 「사이버안전법」은 "사이버 상에서의 공격과 범죄, 유해정보 확산 위협으로부터 사이버공간 주권과 국가안보, 사회 공공이익을 지키기 위한 것"으로, 네트워크 운용과 활용의 공간에서 제기될 수 있는 각종 안보저해 행위에 대한 감시·검열 기능을 담아내고 있다. 국가핵심정보인프라가 사회전반의 신경계통으로 작동하고 있는 현 시점에서 이들 핵심 정보시스템에 대한 안전을 보장함으로써 경제안전 뿐 아니라 사회 및 공공안전, 나아가 국가안전을 보장하는 것이 목적이다. 이에 반해 「사이버테러법」은 중국에서 통신, 인터넷 서비스를 제공하는 기업들은 테러사건 발생 또는 발생 우려가 있을 경우 중국 정부가 데이터에 접속할 수 있는 장치를 마련하고 암호키를 제공토록 함으로서 「신 국가안전법」이나 「사이버안전법」에서 규정하고 있는 사태가 발행하였을 시 인터넷 기업들의 국가에 대한 의무사항을 규정하고 있다. 따라서 이 3개의 법안은 형법에 개별적으로 규정된 네트워크 불법침해 등 범죄와 함께 사이버공간의 안전을 확보하기 위한 주요 기재로 작동하고 있다. 이와 더불어 중앙인터넷관리기관의 장을 국가 주석이 겸하도록 하고 있는 것은 사이버 안보 위협에 대한 심각성에 대해 중국 정부가 충분히 인식을 하고 국가 최고 수준에서 이에 대비해 가고 있다는 것을 알 수 있다. 사이버안보의 주체와 관련하여 중국은 정부,

인터넷 사업자 및 개인으로 세분하여 책임을 규정하고 있으며, 사이버안보에 대한 예방과 경고 및 비상대처조치를 제도화 하고 있다. 「신 국가안전법」을 통하여 중국의 인터넷 주권과 인터넷 사업자에 대한 통제권한을 명문화 하였다. 2016년 11월 제정한 「사이버안전법」에서는 사이버안전에 대한 정의와 함께 중국 국내에서 사이버안전에 대한 검열과 통제 권한을 명시하여 사이버주권 원칙을 분명히 보여주고 있다. 다만, 「신 국가안전법」을 비롯하여 사이버안보와 관련한 법령을 통일적으로 내오지 못하고 개별 법이나 형법에 산입하여 규정함으로써 법 적용에 있어 통일성을 기하기 어렵고, 개인과 기업과 같은 이해 당사자들에게 명확한 법규내용 이해를 기대하기 어려울 것으로 보인다.

중국이 사이버공간에서의 범죄의 확산과 국가안보에 대한 위협을 심각하게 인식하면서도 유럽연합의 <유럽사이버범죄협약>에 참여하지 못하는 이유가 사이버범죄의 관할권에 대한 이견과 함께 사이버범죄와 관련된 중국 국내법 정비가 부실한 것도 이유가 되었었다. 그러나 앞에서 살펴 본 바와 같이 중국은 최근 사이버공간의 안보확보를 목적으로 3개의 법안을 순차적으로 제정하여 시행함으로써 강력한 사이버안보 정책을 전개할 수 있게 되었다. 이는 중국이 주장하는 사이버안보 주권의 확립차원에서도 효과를 거둘 수 있도록 하고 있을 뿐 아니라, 사이버 안전의 보장이 사이버산업 발전을 위한 보증임과 동시에 국가안보를 확립하는 정책이 병행 진행할 수 있도록 해주고 있다. 한편, 이들 법률에 대한 서방국가들의 시각은 매우 비판적이다. 일례로 2016년 8월 미국, 유럽, 일본, 영국, 호주, 멕시코 등 국가를 대표하는 46개 상공단체가 중국 리커창(李克强) 총리에게 이들 법의 주요 내용이 “외국과 중국 기업 모두의 진입장벽을 높이는 결과를 초래할 뿐”이라며 “오히려 중국의 경제성장을 저해하고 고립을 촉구할 것”이라는 항의 서한을 보내기도 하였다.[47]

47) 임근호, “중국 ‘네트워크 안전법’이 뭐길래...,” 「한국경제」2016. 8.15 (www.hankyung.com/news/app/newsview.php?type)

4. 중국의 사이버안보 법제 강화의 의미

가. 국외로부터 사이버침해(테러) 방지를 위한 예방법

중국은 사회주의 전제국가로서 구체적인 관련 법을 구비하지 않더라도 국가권력의 힘으로 사회시스템을 충분히 통제해 나갈 수 있는 체제라고 할 수 있다. 중국은 미국과 함께 사이버공간에서도 명실상부한 글로벌 리더이다. 2013년 이후 미-중 정상회담에서 양국간 해킹문제가 가장 중요한 이슈로 논의될 만큼 사이버공간에서 미국에 필적할 수 있는 유일한 세력이다. 그럼에도 불구하고 「사이버안전법」을 비롯한 관련법을 정비하고 나서는 것은 글로벌시대 국제사회의 일원으로서 위상을 확고히 하고자 하는 것으로 판단된다. 「사이버안전법」은 중국 정부가 사이버공간을 '국가주권확보'의 대상으로 처음 규정한 법률이다. 앞으로 중국 정부는 「신 국가안전법」과 「사이버안전법」을 토대로 사이버공간에서 국가주권을 확보하기 위한 보안전략을 적극 추진해 나갈 것이다. 사회영역과 군사적인 측면에서 사이버 능력 수준을 제고하고 인터넷 안전보호를 강화하는 것이 사이버주권의 일부를 확보하는 것이라고 보는 것이다. 또한, 사이버공간에서는 주권을 확보하는데 있어 컴퓨터 바이러스 침투활동이 원자폭탄보다 효율적이라고 인식하고 있는 것이다. 이와함께 「반테러법」제정으로 해외에서도 반테러작전을 수행하고, 정보기관이 온라인 개인정보를 감청할 수 있도록 허용하고 있다. 인터넷서비스 업체들은 암호해독을 기술적으로 지원해야 하고, 온라인 공간에서 극단주의가 유포되는 것을 원천적으로 막아 중동지역에서 불어온 오렌지혁명의 단초를 아예 차단하려고 하고 있다.

보이지 않는 사이버라는 영토에서 사이버공간에 대한 침해와 위협을 제거하여 사이버주권을 확보하기 위한 노력은 비단 중국 뿐 아니라 미국, 일본, 유럽 국가들도 전력을 다하고 있다. 미국은 에드워드 스노든의 폭로에 따른 조야의 저항이 거세지면서 기존의 「애국법」을 2015년 6월 2일 폐지하였으나 사라진 「애국법」의 자리에 「미국자유법」(The USA Freedom Act)을 새롭게 제정하여 과거보다 합법성

을 확보하는 가운데 정보수사기관이 민간기업에 국가안보서신(NSL)을 통해 개인정보를 수집할 수 있는 권한을 부여하고 있다. 영국은 2016년 6월 일명 스파이헌장(Snooper's Charter)으로 불리는 「사이버테러 방지법」을 제정하였다.[48] 이 법은 수사기관이 개인의 모든 인터넷과 통신활동에 대한 접근권과 감청권을 부여하고 있다. 정부 발의로 제정된 이 법은 MI5, MI6, GCHQ 등 정보기관과 경찰 등 수사기관이 모든 유·무선 통신과 이와 관련된 데이터를 수사과정에서 확보할 수 있도록 허용하고 있는 것이다. 아울러 애플·구글과 같은 IT회사들이 영국에서 서비스를 하려면 사용자들의 인터넷 접속 및 사용기록을 최소 1년간 보존하여야 하고, 수사기관 요청이 있을 경우 관련 데이터를 제공하도록 하고 있다. 호주는 2014년 10월에 이미 정보기관인 호주 안보정보기구(ASIO)에 대테러작전과 관련해서 국내외에서 제기되는 위협을 제압하기 위해 필요하다고 생각되는 컴퓨터 네트워크를 감시할 수 있는 권한을 부여하는 초강력 「대테러법개정안」(Counter-Terrorism Legislation Amendment Bill 2014)을 제정하였다.[49] 스페인도 2004년 마드리드 열차테러사건을 겪은 후 테러범들의 구금기간을 연장하고 테러조직에 가담하는 것만으로도 처벌이 가능하며 통신비밀을 제한할 수 있도록 하는 법안을 만들었다. 캐나다는 2015년 6월 테러를 선동하는 매체, 캐나다에 서버를 둔 선동적 웹사이트를 압수·폐쇄할 수 있도록 하는 「반테러법」을 제정하였다.[50] 프랑스는 2015년 11월 동시다발로 발생한 파리테러를 겪은 후 올랑드 정부가 수사기관들이 영장없이 테러리스트의 통신을 감청하고 체포할 수 있도록 허용하는 프랑스판 애국법 제정을 시도하였으나 부결되었다.[51][52]

우리나라도 2016년 3월 2일 10년간 논란이 되어오던 「국민보호와 공공안전을

48) 이지용, "영 '스파이헌장' 논란 사이버테러방지법 통과," 『MBN』, 2016. 6. 8.
49) The parliament of the Commonwealth of Australia, *Counter-Terrorism Amendment Bill* (2014.9.23.) (www.attorneygeneral.gov.au, 검색일: 2016.11.15.)
50) 이인숙, "테러방지법 만든 국가들," 『경향신문』, 2016. 2.23. (wwww.khan.co.kr, 검색일: 2016.11.8.)
51) 문재연, "파리테러 당사국 프랑스, 테러방지법 부결," 『헤럴드』, 2016. 3. 4. (biz.heraldcorp.com/)
52) 동 법안은 2016년 5월 프랑스 하원에서 압도적 다수의 찬성으로 통과되었으나 같은 해 6월 상원에서 '지나친 사생활 침해'를 이유로 부결되었다.

위한 테러방지법」(이하 「테러방지법」)이 통과되어 국정원이 “테러위험인물에 대한 출입국·금융거래 정지 요청 및 통신이용 관련 정보 수집”을 할 수 있도록 하고 있다. 하지만 이 법에는 사이버공간에서의 테러행위는 규정을 하지 않고 있다. 이에 정부(국정원) 법안으로 제20대 국회 첫회기에 제안되었으나, 사생활 침해 우려 등을 이유로 통과하지 못했으며,[53] 2016년 9월 정기국회에 「국가 사이버안보 기본법(안)」으로 재차 상정되어 심사대기 중에 있다.

나. 국내 인터넷사용 감시·통제 강화로 사회안전 확보

중국 「사이버안전법」은 국가핵심정보인프라가 사회전반의 신경계통이 되어 이제는 핵심 정보시스템에 대한 안전을 보장하는 것이 경제안전 뿐 아니라 사회 및 공공안전, 나아가 국가안전을 보호하기 위해 제정된 법이다. 이 법은 중국의 핵심 정보 인프라를 보호하고, 사이버안전사고 등 중대한 도발사건 발생시 국가안전과 사회공공질서 유지를 위해 인터넷 통신 등에 대한 관제 활동, 인터넷 실명제 실시, 개인정보보호를 주요 내용으로 하고 있다. 중국 정부가 사이버상에서의 공격과 범죄, 유해정보 확산으로부터 사이버공간 주권과 국가안보, 사회 공공이익을 지키기 위한 조치라는 것이 중국 정부의 법 제정 배경이다. 중국은 세계에서 인터넷 검열을 가장 심하게 하는 나라로 알려졌으며. 이러한 검열 기술을 짐바브웨를 비롯한 다른 국가들에게 노하우로 전수하고 있는 것으로 알려졌다.[54] 인권단체와 야당, 대만과 티베트 독립운동, 파룬궁 등과 관련된 사이트 및 일부 국제뉴스사이트까지 검열하고 있다고 한다. 「사이버안전법」제정은 이러한 불법적인 검열과 감시 행태를 합법공간으로 유도한 것이라고 할 수 있다.

세계 모든 국가는 자국의 안보확보, 국민안전을 위한 범죄수사 및 국익을 위한 정보수집 차원에서 인터넷 서비스 제공자의 시스템과 개인들의 네트워크 활동을

53) 최우석, “20대 국회에 바란다 - 반드시 처리해야 할 안보법안은 무엇인가,” 『월간조선』, 2016. 7.

54) KH Moon, “인터넷 검열 확산.. 전세계 20여개국서 실시,” *The Science Times*, 2016.11.23. (www.sciencetimes.co.kr, 검색일 2016.11.23.)

들여다 보고 있다. 사이버공간에서 발생하는 위협은 다양한 출처와 형태를 가지고 있다. 웜, 바이러스 등 악성코드를 통하여 감염된 좀비 PC, 스팸메일의 범람,. 봇넷 등을 이용한 디도스(DDoS) 공격, 해킹으로 군사 기밀정보를 절취하고, 금융정보, 건강정보를 획득하고, 시스템 장애를 유발하는 사건을 예방할 필요 때문이다. 집중원격감시제어시스템(SCADA)이나 산업제어시스템(ICS)을 공격하여 사회 핵심기반시설을 무력화 또는 파괴할 수도 있다. 따라서 이러한 반국가적・반사회적 테러행위나 범죄행위는 사전에 이를 적발하여 예방하는 것이 국가적・사회적 피해를 최소화하는 수단이 된다. 이러한 경우 불가피하게 이를 모니터링하여 차단하거나 접근을 제한할 수 밖에 없는 것이다. 2014년 12월 9일 우리나라에서 발생한 한수원 사이버테러를 적시에 제지하지 못했다면 아주 끔찍한 결과가 나타났을 수도 있다. 2007년 4월 에스토니아에서 발생한 국가마비 사태[55]는 사이버테러의 위력을 극명하게 보여준 사건이다.

다. 사이버정보 공유를 위한 국제협력 증진

사이버공간은 특성상 국경의 한계를 가지지 않으며 시공의 제한을 받지도 않는다. 네트워크는 1년 365일 밤낮을 가리지 않고 가동되면서 인류에게 편익을 주는 한편, 악의적인 범죄자들의 범행 지원수단으로 이용이 되고 있다. 중국은 전술한 바와 같이 <유럽사이버안보협약>에 가입하지 않고 있었던 것은 이 협약이 개별국가의 주권을 침해할 소지가 있다는 이유와 함께 자국 내 법제 미비도 이유가 되었던 점도 하나의 이유가 되었던 것으로 보인다. 이제 「사이버안전법」을 제정함으로써 자국 내 데이터 확보 및 공유에 대한 법적기반이 조성되었다는 점에서 사이버범죄(테러) 정보의 국제공유와 수사공조 등 국제 교류여건이 조성되었다고

55) 2007.4월 에스토니아 대통령궁을 비롯해 의회・정부,은행・언론사 등 주요기관의 홈페이지와 전산망이 디도스(DDoS) 공격을 받아 국가 기간망이 1주일 이상 마비되었다. '사이버진주만' 사건으로 불리는 이 사건을 계기로 사이버공격을 전쟁으로 간주하여 사이버공격에 국제법을 적용하기 위한 '탈린메뉴얼'이 제작되고, 독일・이탈리아・라트비아・리투아니아・슬로바티아・스페인・에스토니아 등 NATO 7개국이 "사이버테러방어센터"를 발족시키게 되었다.

할 수 있다. 그러나 이러한 중국의 국제 사이버협력 증진은 미국과 EU를 중심으로 이루어진 현행 사이버지배 질서에 결합하기 보다는 러시아 등과 연대한 새로운 사이버지배 기구를 만드는 방향으로 노력할 것으로 전망된다. 중국은 사이버안보와 관련해서 미국 주도의 사이버세계를 벗어나서 국가주권을 보장하는 새로운 국제규범(Global Governance)을 만들기 위해 상하이협력기구(Shanghai Cooperation Organization: SCO)와 아세안지역안보포럼(ARF) 활동을 강화하면서, 러시아를 포함한 아시아·태평양지역 국가들과 협력을 확대해 나가고 있다. 2015년 5월 중국 시진핑 주석이 방미시 오바마 미 대통령과 정상회담에서도 사이버안보와 관련한 이슈들에 대해 협의하여, 상호 첩보행위 중지와 사이버공간에서의 위협행위에 대한 수사공조와 정보공유를 합의한 바 있다.[56]

이웃 일본의 경우 2004년 <유럽사이버안보협약>에 업서버 국가로 가입하였다. 2015년 4월 「미-일방위협력지침」에 사이버공간을 추가하여 양국이 사이버공간에서 국제안보와 안전성을 지키기 위해 협력할 것을 선언하였다. 일본이 미국의 사이버 방위능력을 활용할 수 있는 실질적인 협력체계를 구축하였음을 의미하며, 언론에서는 일본이 미국의 '사이버우산'의 보호를 받게 되었다고 보도하였다.[57]

우리나라는 국내 「통신비밀보호법」규정의 미비와 법체제의 상이 등으로 <유럽사이버안보협약>에 가입하지 못하고 있으며, 미국 등과의 사이버테러 정보 공유 및 수사공조 체제 등도 아직 일본의 수준에 훨씬 못 미치는 '합의단계' 수준에 머물러 있다.

5. 결론

지금까지 중국의 사이버안보 정책과 법제 현황에 대해 살펴보았다. 중국은 자국내 사이버안전을 강화하면서 국외로부터의 사이버공격(테러) 행위를 적극 방어

56) 이용성, "[G2정상회담] 오바마·시진핑 '사이버 산업스파이 근절' 합의," 『Biz Korea』, 2015.9.26. (biz.chosun.com, 검색일 2016.11.8.)
57) Tim Kelly, "U.S. to bring Japan under its cyber defense umbrella," *REUTERS*, 2015. 5.30.

하여 국가안보와 경제안정을 돈독히 하고 공산당 지배체제를 공고하자는데 정책의 중점을 두고 있다. 이를 위하여 2015년 이후 「신 국가안전법」 「사이버안전법」을 제정하여 사이버안보를 확보하기 위한 법적 기반을 마련하였다. 그리고 「테러방지법」과 형법 각 규정에 네트워크 불법접속, 정보절취, 국가안보저해 행위 및 테러선동 등과 관련한 개별 규정을 두어 엄중하게 집행을 하고 있는 것도 살펴보았다. 시진핑 주석은 2014년 2월 네트워크와 사이버공간에서 안정을 목적으로 「중앙인터넷안전과정보화영도소조」를 설립하고 조장으로 취임하는 등 지도부가 사이버보안의 국가적 중요성을 인식하여 노력하고 있다. 이와 함께 미국이 강한 영향력을 가지고 있는 인터넷 네트워크에 대한 주권을 확보하기 위해 러시아 및 동남아 국가들과 협력하고 있으며, 「사이버안전법」을 제정한 것도 외국 또는 외국 기업에 대해 중국 네트워크에 대한 제한적 접근과 중국법 준용 등 한계를 가하는 것은 인터넷 주권 확보방법의 일환이다. 나아가 자국 내에서 사업하고 있는 IT 기업들과 개인 사용자들을 통제 관리하고 규제하는 것은 사회안정을 도모하고 국익을 확보하기 위한 것으로 보인다. 「신 국가안전법」 「사이버안전법」등 일련의 사이버 활동에 대한 법률 구비가 사이버테러 정보의 공유와 수사의 공조 등 국제협력을 도모하기 위한 것이다. 이와 같은 연구결과를 바탕으로 우리의 당면하고 있는 사이버정책적 과제가 무엇인지 정리해 보자.

첫째, 보이지도 않고 감지할 수도 없는 사이버공격에 만반의 대응태세를 갖추기 위해서는 하루라도 빨리 「사이버테러방지법」이 제정되어야 한다. 지금까지 살펴 본 바와 같이 중국은 물론, 세계 각국은 자국의 안보와 국민의 안전을 확보하기 위해 사이버테러에 대해 강력하게 대응할 수 있는 법제를 구비해 나가고 있다. 우리나라는 세계 최고의 인터넷 환경을 가지고 있지만 '스팸공화국' '해커들의 운동장' '최고의 사이버공격 경유지' 등의 오명도 함께 가지고 있다. 이는 곧 우리의 네트워크 환경이 사이버공격에 노출될 가능성이 높다는 것이다. 이와함께 북한의 대남 사이버위협은 갈수록 지능화 첨단화되고 있어 사회핵심시설에 대한 근본적인 사이버테러 대응방안을 강구할 필요가 있다는 것이다. 비대칭 전력으로서 사이버공간에서 한반도는 세계 최고 사이버역량을 가진 미・중・러시아와 함께 가

장 악의적 적대세력인 북한과 마주하고 있다.

둘째, 「사이버테러방지법」 제정과 함께 국가의 사이버 안전 활동을 규율하는 근본법 제정과 '국가컨트롤타워' 구축이 시급하다. 현재 국정원에서 사이버공격 대응활동 조정역할을 하고 있으나 근거법이 없고 기능이 기관별로 분산되어 있어 수준높은 협력 업무를 기대하기 어렵다.[58] 국가 컨트롤 타워 기능은 국정원에 부여하는 것이 사이버대응 기술과 정보수집, 긴밀한 수사대응 등 측면에서 바람직하다. 국가기관으로의 권력집중이나 개인의 권리 침해 등이 염려가 있다면 정보기관의 활동을 감시 통제할 수 있는 기구(예를 들어 사이버테러활동 감찰위원회)를 함께 도입하는 방법도 고려해 볼 수 있다.

셋째, 강한 국가안보를 확보하고 국가이익과 국민의 안정된 생활을 유지할 수 있도록 관련 법규에 대한 손질이 필요하다. 그 중에서도 인터넷, 스마트폰, 사물인터넷(IoT), 클라우드, Big data 등 급변하는 환경에 적용 가능하도록 통신비밀보호법을 개정하여야 한다. 사실상 '식물법' 상태에 이른 통비법을 모바일과 무선환경에 대해 적용이 가능하고, 인터넷・통신사업자의 협조를 받아 적정한 Data 수집이 가능하도록 개정하여야 한다. 현행 통비법은 첨단 미디어나 매체에 대한 구체적인 감청 등 절차가 결여되어 있고, 원할한 수사활동 지원에 관한 절차의 부재, 원격감시 수단의 부재, SMS 추출제한 등 많은 문제점을 가지고 있다.

넷째, 사이버공격 대응 전문가 양성과 기술을 개발하여야 한다. 우리나라의 사이버공격에 대한 대응은 철저하게 방어와 보호라는 수동적 방식으로 접근하고 있다. 고도화되고 증폭되는 사이버위협을 수동적 방어체제로 감당해내기 어렵다. 사이버 위협대응기술과 함께 사이버 공격에 대한 역추적, 핵심기반시설 공격에 대한 방호기술, 공격원점 추적을 위한 기술개발, 임박한 공격을 예방하기 위한 능동적 방어기술 또는 억제기술을 확보하는 것이 중요하다.

마지막으로, 정보공유와 공동 대응을 위한 국제협력을 강화하여야 한다. 국경의 한계를 받지 않는 인터넷 공간에서 효과적으로 사이버공격에 대응하기 위해서 사

58) Martin C. Libicki, "Brandishing Cyberattack Capabilities," *RAND*(2013.) p.10.

이버 국제협력이 필수이다. 우리나라는 세계 사이버스페이스 총회 개최(2013년), UN GGE 가담 등 활동을 전개하고 있으나, 아직 사이버 종주국이자 최고 동맹국인 미국과 「사이버안보협약」을 맺지 못하고 있으며, <유럽사이버범죄협약>에도 수차 검토한 바 있으나 우리의 여건이 부합되지 않아 가담하지 못하고 있는 실정이다. 하루라도 빨리 국제 사이버대응 기준과 절차에 부합하도록 법제를 정비하고 동맹관계를 강화하여야 한다. 특히, 살펴 본 바와 같이 북한의 대남 사이버 공격의 매개가 되는 중국정부를 설득하여 북한이 중국 IP를 사용해서 공격해 오는 일을 없도록 설득하고 협조하여야 한다. 이렇게 할 때 북한은 '인터넷 질식'과 '정보의 부재 심각성' 등으로 자연스럽게 세계인터넷에 가담하는 계기가 될 것이며, 대외 개방의 유인요소로 작용할 것이다. 지금까지 중국의 사이버안보 정책과 법제의 주요 내용을 살펴보고, 그것이 우리에게 주는 의미와 정책적 대안을 정리해 보았다. 북한과 마찬가지로 중국의 사이버역량에 대해 공개된 자료를 찾아보기 어렵고, 중국 내부의 사이버안보 실행체제에 대해서도 그나마 신빙성이 있다고 할 만한 데이터는 부족하였다. 주어진 짧은 기간에 부족한 데이터를 가지고 연구한 내용에 많은 부실함이 있을 것으로 본다.

참고문헌

김경애. “북한의 사이버위협 대응, 중국 역할 매우 커.”『보안뉴스』, 2015. 9.11.

김민석. “북한 사이버전법은 중국의 ‘점혈전쟁술’ 모방한 것.”『조인스닷컴(News.joins.com)』, 2009. 7.10.

김순수. “중국의 ‘중앙국가안전위원회’ 설립에 관한 연구.”『민족연구』, 63호(2015. 10)

김유향. “중국의 네트워크 안전법과 온라인 규제동향.”『KISO저널』, 제20호(2015.10.1.).

김필제. “북한의 ‘사이버테러’ 전략: 점혈전략.”『조갑제 닷컴』, 2009. 7.11.

_____. “中 인민해방군 ‘제4군’ 사이버 전담부대 분석.”『조갑제닷컴』, 2015. 1.11.

김한균. “동북아 사이버범죄 및 보안 지역협력방안.”『한국형사정책연구원』, 2015.12.

디펜스 21. “사이버위기 직면한 한반도 정세(하), 2014.12.26.

문재연. “파리테러 당사국 프랑스, 테러방지법 부결.”『헤럴드』, 2016.3.4.

이상호. “새로운 도전: 국가 사이버 위협 및 사이버.”『신안보연구』, 제1권, 1호(2016 여름).

이연수・이수연・윤석구・전재성. “주요국의 사이버안전관련 법・조직체계 비고 및 발전방안 연구.”『국가정보연구』, 제1권, 2호(2008).

이용성. “[G2정상회담] 오바마・시진핑 ‘사이버 산업스파이 근절’ 합의.”『Biz Korea』, 2015. 9.26.

이인숙. “테러방지법 만든 국가들.”『경향신문』, 2016. 2.23.

이지용. “영 ‘스파이헌장’ 논란 사이버테러방지법 통과.”『MBN』, 2016.6.8.

이지훈. “중국의 새로운 방공식별구역 정책과 한국의 대응전략 : 법률전의 전개.”『신안보연구』, 제1권, 1호(2016 여름).

임근호. “중국 ‘네트워크 안전법’이 뭐길래... .”『한국경제』, 2016.8.15.

정종필. “사이버안보의 주변 4망(網)과 한반도, 중국의 사이버 안보 전략.” 네트워크세계정치 세미나 자료집(2016.4.25.).

최남규. “중국: IT기업들은 중국의 억압적인 인터넷 규제 거부해야.”『국제인권뉴스』, 2015.12.16.

최우석. “20대 국회에 바란다 – 반드시 처리해야 할 안보법안은 무엇인가.”『월간조선』, 2016.7.

최진홍. “중국의 인터넷 주권 화두, 위선과 위선의 대결.”『이코노믹리뷰』, 2015.12.20.

한상미. “북한, 과학영대 50-60명씩 유학 보내 사이버 요원 양성.” *VOA*, 2016.6.14.

Elsa Kania. “China: Active Defense in the Cyber Domain.” *The Diplomat*. 2015.12.

_____. “China Brief: the Latest Indication of the PLA’s Network Warfare Strategy.” The JamesTown Foundation, *China Brief Volume* 15(24).

IGCC. “China and Cybersecurity: Political, Economic, and Strategic Dimensions.” *SITC*. 2013.4.

KH Moon. “인터넷 검열 확산.. 전세계 20여개국서 실시.” *The Science Times*, 2016.11.23.

Martin C. Libicki. “Brandishing Cyberattack Capabilities.” *RAND*, 2013.

Taylor Brooks. “why China Needs to Rein in North Korea’s Hackers.” *Christian Science Monitor*, 2016.2.5.

The parliament of the Commonwealth of Australia. *Counter-Terrorism Amendment Bill* (014.9.23).

Tim Kelly. “U.S. to bring Japan under its cyber defense umbrella.” *REUTERS*, 2015.5.30.

World Economic for global Risk Report 2016.

“China a Likely in North Korea Cyber Prowess: Experts.” *AFP*. 2014.12.26.

chn.mofa.go.kr/webmodule/common/download.jsp?boardid=13350.

Abstract

A Study on China's Cyber Security Legislation and Policy: Implications of China's New Cyber Security Law and Our Responses

Youn Bonghan (Institute for National Security Strategy)

China set off new 'Cyber Security Law' on November 7, 2016. The main characteristic of this law is setting up the concept of network sovereignty(wangluo zhuquan) in cyberspace as well as establishing regulatory institutions and mechanisms to strengthen governance on IT company and individual users in China. With adoption of 'New National Security Law 2015' and 'Anti-Cyber Terrorism Law 2015', China's legal system for the regulation of cyber security policy has well equipped.

China's main cyber security concerns are based on the Small Leading Group for Internet Security and Informatisation being chaired by the President Xi Jinping. It's Cyber Security policy, backed up by the Xi's conception of General National Security, controls the national sovereignty, national security and public interests in cyber space, as well as is enforcing control over the networks in China. Xi leads the unit with taking unprecedented priority to both internet security and information management. China will stick to improving the security of the domestic internet infrastructure and promote an alternative attitude to create another global internet governance.

Conclusively, without any Anti-Cyber Terrorism Act and dominant Cyber Control Governance, Korea definitely need to bring laws and social bodies protecting its

critical information infrastructure and network security for its national and public safety. It also need to strengthen the governmental and classified information security systems, which are often attractive targets for North Korea's cyber operation. Finally, it should positively take part in global cyber security communities and develop a cooperative relations with them.

Key Words: cyber security, cyber sovereignty, information infrastructure, cyber policy, cyber monitering

투고일 : 2016.10.20. 심사일 : 2016.11.20. 게재확정일 : 2016.12.10.

Ⅳ

신안보 요소로서의 재난 개념의 변화와 법 제도적 함의

이창주 (성균관대학교)

Summary

과거 전통적인 국가안전보장의 개념은 외부로부터의 군사적 위협에 대응하는 군사적 부문에 한정하여 정의되었다. 그런데 냉전이 종식된 이후 국제질서의 변화, 경제·사회의 발전에 따라 군사적 부문은 물론 외교, 경제, 환경, 자원 등 전반적 분야를 포함하는 이른바 포괄적 안보개념이 일반화되었다. 또한 정보통신 기술의 발전, 교통수단의 발달 등으로 인하여 국경의 의미가 점차 약화되어 가고 있고 최근 스마트 사회로 진입하면서 국가안전보장의 개념은 변화를 거듭하여 신안보 개념이 등장하기에 이르렀다.

과거 재난관리의 문제는 주로 자연재난 문제 대응에 치중하여 국내 통치 및 민생 개념의 범주에 포함시키는 것이 일반적이었으며 국가안전보장 차원의 개념으로 정의되지는 않았다. 그런데 국내외 환경의 변화에 따라 재난의 양태가 자연재해뿐만 아니라 인적재난과 사회적재난, 복합재난, 해외재난 등 다양한 개념으로 분류되었고 대규모화, 국제화되면서 국가안보에 영향을 미치는 요인이 점차 커지게 되었다. 이에 따라 국가안보의 개념에 재난의 개념이 포함되는 것이 일반화되었으며 오늘날 재난의 개념은 테러, 사이버 보안 등 까지도 포함하는 광범위한 개념으로 자리 잡게 되었다.

우리나라 역시 국가안전보장의 범주에 확대된 재난 개념을 도입하여 법제도적으로 매우 광범위한 재난 개념 및 재난 유형을 적용하고 있으며 세월호 침몰 사고 수습과정에서 국민안전처를 창설하는 등 재난 개념 및 재난 대응체계를 대폭 개편하여 재난에 대응하고 있다. 그러나 국민안전처의 임무와 기능이 아직 재난 대응체계를 완전히 갖추지 못하여 최근 경주 지진, 태풍 등 재난 문제에 제대로 대응하지 못했다는 국민적 비판에 직면하는 등 개선 여지가 적지 않게 나타나고 있는 실정이다. 이러한 문제에 대하여 지속적인 재난 대응체계 개선과 법제도적 보완 등이 필요한 것으로 보인다.

| 키워드 | 국가안전보장, 신안보, 재난, 재난관리, 자연재난, 인적재난, 사회적 재난, 테러

1. 서론

우리 사회는 사회체제의 전반적인 발전에 따라 가치관・이념・제도 등 다양한 분야에서 변화를 겪고 있으며, 점차 가속화되고 있는 전자통신 수단의 발달 등 스마트사회 진입으로 인한 급격한 변화가 사회 모든 분야에 파급영향을 미치고 있는데 따라 국가안전보장의 개념도 계속 변화하고 있다. 전 세계적으로는 제2차 세계대전 이후 미국과 소련이 주도했던 동서 냉전체제 종식 이후 공산권 국가들의 몰락으로 인한 국제관계의 재편이 진행되면서 국가안전보장 환경의 변화가 이어져 왔다. 냉전시기를 포함한 과거의 국가안전보장 개념은 국가에 대한 외부로부터의 군사적 위협에 대응하는 국가의 군사력을 중심으로 하는 개념으로 정의되고 있었다.[1)]

그런데 동서냉전이 종식된 1990년대 초반 이후 세계적인 힘의 균형이 깨지면서 급속하게 재편되기 시작한 국제질서의 변화, 경제・사회의 발전에 따라 국가안전보장 개념은 군사적 부문에서만 정의되던 범위에서 벗어나 외교, 경제, 환경, 자원, 정치, 사회 등 전반적 분야로 확대되면서 이른바 포괄적 안보개념이 일반화되게 되었다. 또한 정보통신 기술 및 수단의 발전, 교통수단의 발달, 국경을 넘어서는 다국적기업 및 국제범죄조직의 활동 등으로 인하여 국경의 의미가 점차 약화되어 가고 있고 정보화사회를 지나 스마트사회로 진입해가는 과정에서 국가안전보장의 개념은 사회 전반의 발전 속도에 따라 변화를 거듭하여 근래에 이르러서는 신안보 개념이 등장하게 되었다.

국가안전보장의 개념이 군사적 부문뿐만 아니라 외교, 경제, 환경, 자원, 정치, 사회 등 전반적 분야로 확대되어 오고 신안보개념이 등장하여 그 개념 및 범위 등에 대한 논의가 전개되면서 테러, 재난 등 과거에는 독립적 요소로 논의되던 문제들도 신안보개념에 포함시키는 것이 국가안전보장 체계를 정립하는데 있어서 중요한 의미를 갖게 되었다.

---

1) 백종천・이민룡 공저, 『한반도 공동안보론』(서울: 일신사, 1993), pp.89-90.

재난관리의 문제를 살펴보면, 인류 역사가 시작된 이래 오랫동안 재난대응을 국내 통치권 확립을 위한 민생관리 개념의 범주에 포함시켜 자연재난 문제 대응에 치중하였던 것이 일반적이었으며 국가안전보장 차원의 개념으로 정의되지는 않았었다. 그런데 산업 및 기술의 발전, 사회구조의 복잡화, 이념 및 정치적 대립, 자연환경의 변화 등 국내외 환경의 변화에 따라 오늘날에 이르러서는 재난의 양태가 자연재해뿐만 아니라 인적 재난과 사회적 재난, 복합 재난, 해외 재난 등 다양한 개념으로 분류되고 있고 다양한 원인 및 발생·피해규모의 대규모화, 국제화되면서 국가안전보장에 영향을 미치는 요인이 점차 커지게 되었다.

이에 따라 확장된 국가안전보장의 개념, 즉 신안보 개념에는 확장된 재난의 개념이 포함되는 것이 일반화되었으며 오늘날 재난의 개념은 테러, 사이버 보안 등까지도 포함하는 광범위한 개념으로 확장되게 되었다. 그리하여 신안보 개념 요소 중의 하나로서 재난의 개념을 정립하는 것은 국가안전보장 체계의 발전을 위한 개념적 틀의 기초를 제공한다는 면에서 중요한 과제라 할 수 있다.

이러한 관점에서 본 연구는 확장된 재난의 개념이 신안보 개념의 범위에 포함되어 정의되는데 있어서 앞으로 개선해 나가야할 법제도적 과제를 제기하고 그 해소방안은 무엇인지를 밝히는데 중점을 두었다. 본 연구에서는 이를 위하여 오늘날 신안보 개념에 이르기까지 국가안전보장의 개념이 논의되어온 과정을 살펴보고, 재난의 개념 및 유형의 변화와 법제도적 변화 등을 살펴보는데 중점을 두었다. 한편, 재난관리에 관련된 많은 선행 연구결과를 이번 연구를 위하여 활용하였다. 본 연구에서는 그동안 본 논문의 주제와 관련되는 내용으로 이루어진 선행 연구의 결과인 각종 저술과 논문, 인터넷 자료 등을 참고하여 분석하고 인용하는 방법으로 연구를 수행하였다.

2. 국가안전보장 개념의 변화와 재난 개념의 확대

가. 국가안전보장 개념의 변화[2)]

전통적이고 고전적인 국가안전보장 개념은 '국가를 외부로부터의 침략이나 공격이 없는 상태로 유지하는 것, 또는 외부로부터의 위협에 대한 국가의 소극적 방어기능'으로 정의 되었다.[3)] 이러한 전통적이고 고전적인 국가안전보장 개념에 따르면 외부로부터의 위협인 군사적 위협으로부터 국가의 안전을 유지하기 위한 수단으로는 군사력이나 국방・외교 정책이 사용되는 것으로 정의할 수 있다.[4)]

또한 국가안전보장의 의미는 "일반적으로 국가의 책임으로써 국가 및 시민의 핵심적 가치가 대내외로부터 위협받는 상황을 방지하여 심리적으로 뿐만 아니라 물리적인 안정을 추구하는 것"으로 정의되기도 했다.[5)] 여기에서 '핵심적 가치'의 의미에 관해서는 다양한 해석이 가능하겠으나, 국민 개개인의 생명과 재산의 보호, 국가적 차원의 생존 및 번영, 국가적 위신 등이 해당될 수 있으며 주관적 해석도 적용될 수 있다.[6)]

국가안전보장이라는 개념이 최초로 법제화된 것은 제2차 세계대전이 끝난 뒤 미국이 소련 등 공산권 국가들과의 대립에서 유발된 동서 냉전체제에 대응하기 위하여 1947년 제정한 「국가안전보장법(National Security Act of 1947)」이었다. 미국에서의 「국가안전보장법(National Security Act of 1947)」 제정의 가장 큰 의의는 과거 오랫동안 국가안전보장 개념을 단지 국가의 존립보장을 의미해 오던 것에서 확대하여 국가존립 보장을 위하여 평상시와 전시(戰時) 양자를 포괄하는 전시(戰時)체제의 항상화를 의미하는 것으로 파악한 점이라 할 수 있다.

---

2) 이창주, "미국에서의 국가안전보장 관련정보 공개제한에 관한 연구", 한국외국어대학교 박사 학위 논문(2013.2.)」중 일부를 인용, 재구성.
3) 김승렬, "국가위기관리 법제에 관한 연구", 『법제』(서울: 법제처, 2007.11.), p.9.
4) David A. Baldwin, "The concept of security", Review of International Studies 23/1(1997), pp.5-26.
5) Robert Mandel, The Changing Face of National Security: A Conceptual Analysis (Westport, Connecticut: Greenwood Press, 1994), p.21.
6) 전 웅, 『현대국가정보학』(서울: 박영사, 2015.1.), p.514.

이렇게 제2차 세계대전 이후 형성된 동서 냉전기에 확립되어 확대되었던 전시체제의 항상화 경향에 대해 '국가안전보장의 국가화 현상'이라는 측면에서 비판을 제기하는 견해도 있었다.[7] 이와 같이 미국에 있어서 국가안전보장의 개념은 냉전구조 하에서 주로 군사적으로 대치하고 있는 적과의 생존을 위한 투쟁에서 승리하는 것을 가장 중요한 목적으로 하는 이데올로기적 개념으로 등장하여 그 개념이 확대되어 왔다.

그런데 이렇게 미국에서 확립되어 각국으로 확산된 전통적 국가안보 개념은 1970년대 발생한 에너지 위기와 국제교역 불균형 등 경제문제가 국가의 사활적 이익에 중대한 요소로 작용한다는 사실을 인식하게 되면서 새로운 내용으로 변화하게 되었다.

우리나라에서도 위와 같이 미국을 비롯한 각국에서 새로운 내용으로 변화되고 확립된 국가안전보장의 이념을 헌법에 수용하여 1972년 헌법 개정 시 제37조 제2항에 기본권 제한의 목적으로 '국가안전보장'을 추가하여 기본권을 제한하게 될 경우 '국가안전보장·질서유지·공공복리'를 위하여 필요한 경우에 한하여 허용된다고 규정하였다.[8] 이렇게 우리나라 헌법 제37조 제2항에 규정된 국가안전보장의 개념에 대하여 헌법재판소는 국가의 존립·헌법의 기본질서 유지 등을 포함하는 개념으로서 국가의 독립·영토의 보전·헌법과 법률의 기능·헌법에 의하여 설치된 국가기관의 유지 등의 의미를 가지는 것으로 해석하였다.[9]

미국에서는 1979년 7월 15일 카터(James E. Carter) 대통령이 당시 전세계적인 범위에서 발생하였던 석유에너지 위기를 극복하기 위하여 "에너지 안전보장(energy security)"이라는 새로운 국가안전보장 개념을 설정한 것이 새로운 안전보장 개념의 사례이다.[10]

이와 같이 70년대 이후의 국가안전보장에 대한 위협 양태의 다양화는 미국뿐

---

7) Harold Lasswell, "The Garrison State", *American Journal of Sociology* 46/4(1941), p.455.
8) 성낙인, 『헌법학(제9판)』(서울 : 법문사, 2009.2.), p.352.
9) 헌재 1992.2.25. 자89헌가104 결정.
10) Energy and the National Goals – A Crisis of Confidence, 15 July, 1979.

아니라 널리 서방 선진국 전체에서 나타난 현상이었다. 미국의 경우는 국가안전보장 개념이 카터 행정부에 의해 에너지자원 정책을 포함하는 것으로 확대된 데 이어, 그 후임으로 집권한 레이건(Ronald W. Reagan) 행정부 시대에는 경제정책, 대테러정책 등도 국가안전보장 정책으로 편입되기에 이르렀다.

레이건 대통령은 1988년 1월에 수립한 국가안전보장전략(National Security Strategy)에서 "국가안전보장은 전통적으로 외부로부터의 공격에 대한 방어로 인식되어 주로 군사적 위협에 대한 군사적 방위라는 개념이었으나 이것은 매우 좁은 개념이다. 국가의 안전보장은 오늘날 군사력의 준비와 그 적용 이외에도 훨씬 다수의 것, 즉 낮은 강도의 지역적인 분쟁, 핵보유국의 증가 가능성, 국제테러리즘, 마약거래, 과격한 정치 및 종교 활동 그리고 중요한 우방국이나 동맹국의 정국불안정, 정권 교체, 경제개발을 포함하고 있다."고 지적하였다.[11]

한편 클린턴(William J. Clinton) 행정부는 1989년 11월 베를린 장벽 붕괴, 1991년 12월 소련 연방의 해체로 상징되는 동서 냉전구조의 해소 상황에서 미국의 국가안전보장정책의 전반적인 전환을 도모하였다. 이러한 새로운 국가안전보장정책에서는 미국의 국익에 대한 위협 요인으로 글로벌 규모의 환경파괴, 에너지자원 문제, 제3세계의 인구폭발과 기아, 빈곤, 난민문제, 지역분쟁, 핵, 대량살상무기의 확산, 국제테러리즘, 국제적 마약밀수 등을 적시하였으며, 이에 따라 클린턴 대통령은 재임 중인 1995년 작성된 "관여와 확장의 국가안전보장전략(A National Security Strategy of Engagement and Enlargement)"에서 군사적·기술적 위협, 지역분쟁, 대량살상무기의 확산뿐만 아니라 테러리즘, 마약밀수, 세계 각국의 경제활동, 환경활동, 인도적 활동, 재해구조활동 등 매우 광범위한 국가정책의 영역이 국가안보의 영역임을 확인하였으며 재해구조활동 등을 최초로 국가안보 영역으로 편입시켰다.[12]

즉, 탈냉전기 이후 국가안전보장의 개념은 대외 안보환경의 변화, 민주화의 확

11) The White House, *National Security Strategy of the United States*, 1988.1.
12) The White House, *A National Security Strategy of Engagement and Enlargement*, 1995.2. [http://www.au.af.mil/au/awc/awcgate/nss/nss-95.pdf]

산 등에 따라 군사전략적 측면에서의 안보개념에 추가하여 경제, 자원・환경, 사회문제 등 비군사적 요소들을 포괄하는 개념으로 변화되었으며[13] 이는 곧 소위 '포괄적 안보' 개념으로의 변화를 초래하게 되었다.

2001년 9월 11일에 발생한 '9.11테러' 사건은 명맥을 유지해 오던 전통적 안보개념을 '포괄적 안보' 개념으로 전환시키는 강력한 계기가 되었다. 부시(George W. Bush) 대통령은 9.11 테러사건이 발생한 이후 다양한 입법을 포함하여 국내외에서 전방위적으로 국력을 결집한 복구 및 대응정책을 추진하면서 2002년 9월 미국의 새로운 국가안전보장전략을 발표하여 소련의 붕괴와 동서 냉전의 종결로 미국의 국가안전보장 환경이 크게 변화되었으며, 국제테러조직과 이란・이라크 등에 의한 대량살상무기의 개발・보유・사용능력의 획득이야 말로 미국의 국가안전보장에 가장 중요한 위협이라고 선언하였다.[14] 또한 부시 행정부가 발표한 새로운 국가안전보장전략에서는 국민의 생명과 재산을 보호하기 위한 구체적인 위기관리 정책을 추진토록 하였다. 이후 유럽의 주요 국가들도 미국의 영향으로 다양한 위협으로부터 국가의 안전과 국민의 안전을 보호하기위한 적극적인 노력을 기울이기 시작하면서 소위 '인간안보'를 포함하는 '포괄적 안보' 개념이 국제사회의 위기관리 개념으로 자리잡게 되었다. 소위 '포괄적 안보'는 영속적인 '인간안보'에 필수적이고 지속가능한 발전을 보다 인간적인 형식으로 연계시켜 주는 것이다.[15]

이상 살펴본 바와 같이 과거에는 전쟁 등 군사력 대립과 같은 전통적 안보위기만을 국가안전보장 위협요인으로 보았으나 탈냉전기 이후 확연히 달라진 국내외 환경과 여건에 따라 각국은 국민, 영토, 주권, 국가핵심기반 등의 안전을 위협하고 마비시킬 수 있는 재난이나 질병, 전염병, 실업, 파산까지도 국가안전보장을 위협하는 요인으로 규정하고 대응체계를 구축해 왔다. 또한 테러를 비롯하여 각종 사회 안정 위협요소, 국가의 안녕・질서를 위협하는 요소들도 모두 국가안전보장 위협요소로 다루고 있다.[16]

---

13) 전 웅, 앞의 책, p.518.
14) The White House, *The National Security Strategy of the United States of America*, 2002.9.
15) 이재은, 『위기관리학』(서울: 대영문화사, 2012.1.), p.75.
16) 이재은, 위의 책, p.72.

나. 재난 개념의 확대

재난은 단순히 어떤 원인으로 인하여 물리적인 결과만으로 나타나는 현상이 아니며 물리적 현상이자 동시에 막대한 사회적 영향을 발생시키는 복합적 결과이다. 재난의 개념은 사회 전체 또는 사회 내 일부 조직에 심대한 피해를 끼쳐 그 사회 구성원이나 물리적 시설의 손실로 인하여 사회구조가 교란되고 그 사회의 본질적인 기능 수행이 장애를 받게 되는 사건으로서 우연히 발생하거나 통제 불가능하며 동일한 시간과 공간에 집중적으로 나타나는 실제적이고 위협적인 사건으로 정의된다.[17]

또한 재난의 개념에 관하여 UN 산하 국제기구인 UN-ISDR(United Nation-International Strategy for Disaster Reduction : 재난 감소를 위한 국제전략)[18]은 "재난은 광범위한 인적, 물적, 경제적, 환경적 피해로 인하여 공동체 또는 사회 기능의 심각한 붕괴현상이 발생하는 것을 의미하며 이러한 피해는 공동체 또는 사회 내부의 자원만으로는 스스로 극복하기 힘든 상태"를 의미한다고 정의하였다.[19]

이러한 개념에 기초해 재난의 유형은 직접적 발생 원인에 따른 구분 방법과 법적・사회적・간접적 원인에 따른 방법 등으로 나누어 볼 수 있다. 전통적이고 일반적인 재난 유형의 분류 방법은 재난의 직접적 발생 원인에 따라 자연으로부터 발생하는 현상이 발생 원인이 되는 자연재난, 인간의 행위로 인하여 재난이 유발되는 인적재난으로 구분하는 방법이다.

자연재난으로 분류되는 자연 현상은 태풍, 홍수, 호우, 강풍, 폭설, 해일 및 쓰나미, 가뭄, 지진, 황사 및 미세먼지, 적조 및 녹조 등을 들 수 있으며 인간에 의한 인위적 원인으로 발생하는 인적재난에 해당되는 것은 테러, 화재, 붕괴, 폭발, 교통사고, 화생방사고, 환경오염 사건, 해상운송 사고 등을 들 수 있다. 자연재난은

17) 이종열・이종영・최진식・정지범 공저, 『재난관리론』(서울: 대영문화사, 2014.10.), p.12.
18) UN-ISDR(United Nation-International Strategy for Disaster Reduction)은 국제적 재난 감소를 위한 활동을 목적으로 1999년 12월 유엔 사무국 산하에 창설된 국제기구이다.
19) 이종열 등 공저, 앞의 책, p.12.

예측가능성을 기준으로 예측 가능한 자연재난과 예측 불가능한 자연재난으로 분류될 수 있으며 인적재난은 인간의 의도된 행위의 결과인 고의적 재난과 시설이나 설비의 노후, 고장, 오류, 착오, 기술 미숙, 시스템 미비 등으로 발생하는 비고의적 재난으로 분류할 수 있다.[20]

그런데 이러한 분류 방법에 따르면 재난의 개념은 현대에 이르러 인적재난 유형에 속하는 고의적 재난과 비고의적 재난의 개념 부분에서 많은 변화가 있음을 알 수 있다. 즉, 고의적 인적재난으로 분류할 수 있는 것은 테러, 폭동, 방화, 폭파, 환경오염 사고, 고의적 대규모 금융사고, 해킹 등 사이버 범죄 등을 들 수 있고 비고의성 인적재난에 해당되는 유형은 건조물 붕괴, 화재, 가스 등 폭발 사고, 육·해·공 대규모 교통사고 등을 들 수 있다.

이렇게 재난의 개념이 다양하게 변화되어 온 이유와 계기는 사회체제의 전반적 발전 및 가치관과 이념의 변화, 시설 및 장비의 대형화, 인터넷·IT 등 첨단 기술과 산업의 발전, 대규모 사건 사고 등이 직접적, 간접적 영향을 미친 결과이다.

재난 대응 체계에 있어서 선진국이라고 할 수 있는 미국의 경우를 보면 앞서 국가안전보장 개념의 변화에서 살펴본 바와 같이 국내외에서 발생한 환경과 여건을 반영하여 1970년대에 국가안전보장 개념을 경제 영역으로 확대한데 이어 1980년대에는 테러 문제를 국가안전보장 개념으로 편입하였으며 1990년대에는 재난 대응 및 구호 문제를 국가안전보장 개념으로 확대 적용하기 시작하였다. 이러한 국가안전보장 개념의 확대에 동조하여 재난의 개념과 범위도 변화와 확대의 과정을 거쳐 왔다. 즉, 재난 대응 및 구호 문제를 국가안전보장 개념으로 편입시킨 1990년대 이래 재난의 개념이 이른바 '포괄적 국가안전보장'의 개념 틀에 맞추어 바뀌어 오던 중 2001년 9월 11일 소위 '9.11 테러 사건'[21]이 발생하면서 재난 개념에도 적극적 확대가 이루어지는 강력한 계기를 맞이하게 되었다. 미국으로서는

20) 이종열 등 공저, 앞의 책, p.14.

21) '9.11 테러'는 2001년 9월 11일 알 카에다 소속 테러범 19명이 미국 민간항공기 4대를 납치하여 뉴욕의 세계무역센터, 국방부 건물 등에 충돌, 자폭하는 방식으로 저질러진 사상 초유의 테러 사건이었다. 이 사건으로 인하여 사망 2,749명, 부상 3,600명, 피해액 2,000억 달러라는 천문학적 피해가 발생하였다. 전 웅, 앞의 책, P.309.

건국 이래 최대 규모의 본토 대상 테러 공격을 당하고 이를 복구하는 과정에서 사상 최대 규모의 행정부 개편을 단행하게 되었으며 이때 창설된 국토안보부(DHS)[22]가 테러와 재난 등을 총괄하게 되면서 재난 개념의 적극 확대가 단행되었다.

미국 국토안보부의 주요 임무는 테러 예방 및 대응 활동 총괄, 국경경비, 재난대응 활동, 화생방 공격 대비 활동, 테러 및 재난정보 분석 등이다. 여기에서 주목할 점은 국토안보부(DHS)를 창설하면서 독립기관으로 존재하던 연방재난관리청(FEMA)[23]을 소속 기관으로 편입시켜 재난관리업무를 테러 대응 업무와 병행하는 국토안보부의 주요업무 분야 중 하나로 선정하였다는 점이다. 이에 따라서 미국 연방재난관리청은 재난 대응 과정인 예방, 대비, 대응, 복구의 과정에서 국토안보부에서 수행하는 테러와 재난 대응 관리 등을 수행하는 중심 기관으로서의 역할이 부여되었다.[24]

미국 연방재난관리청에 부여되어 있는 주요 임무는 모든 재난에 대비하여 종합적인 국가 재난관리 체계 구축, 신속하고 효과적인 재난 대응 및 복구 체계 구축, 주정부 및 지방정부의 재난관리 능력 강화, 연방정부・주정부・지방정부・자원봉사기관・기업체 등과의 재난관리 협력 강화 등이다.[25]

---

22) 국토안보부(DHS : Department of Homeland Security)는 본래 9.11 테러 사건을 계기로 각 부처에 분산되어 수행되고 있던 대테러 기능을 통합할 목적으로 2002년 11월 25일 제정된 국토안보법(Homeland Security Act of 2002)에 근거하여 2003년 1월 24일 창설되었다. 기존 22개 정부기관의 일부 및 전부(소속 직원 17만명)를 흡수한 대규모 부처로 출범하였다.

23) 미국 연방재난관리청(FEMA : Federal Emergency Management Agency)는 빈발하는 대규모 재난에 대응하고자 1950년 연방재난법(Federal Disaster Act)을 제정한 이후에도 100여개 기관이 제각기 수행하여 비능률적이던 연방 재난관리 업무를 효율적으로 집행하기 위하여 1979년 카터 대통령에 의하여 창설되었다.

24) 이종열 등 공저, 앞의 책, pp.76-82. 국방부 영역인 전쟁, 핵 공격 등은 임무에서 제외되었다.

25) 김인범・류상일・송윤석・양기근・이동규・이주호・홍영근 공저,『재난관리론』(서울 : 대영문화사, 2014.7.), p.173.

3. 우리나라에서의 재난 관련 법제도적 변화의 함의

가. 재난 관련 법제도적 변화

우리나라에서의 재난 개념은 건국 이후 장기간 인적재난, 자연재해, 민방위 분야로 구분되어 운영되어 왔다. 즉, 2004년 「재난 및 안전관리 기본법」이 제정되기 이전에는 「(구)재난관리법」에 의한 인적재난(화재・붕괴・폭발・교통사고・화생방사고・환경오염사고 등 국민의 생명과 재산에 피해를 줄 수 있는 사고로서 자연재해가 아닌 것), 「자연재해대책법」에 의한 자연재해(자연현상으로 인하여 발생하는 피해), 「민방위기본법」에 규정된 민방위사태(적의 침공이나 전국 또는 일부 지방의 안녕 질서를 위태롭게 하는 재난) 규정 내용에 따라 재난관리를 3원화하여 운영해 왔다.

2003년 2월 발생한 대구지하철 방화 사건을 계기로 2004년 정부는 재난관리를 총괄하는 법률로서 「재난 및 안전관리 기본법」을 제정하고 소방방재청을 창설하는 등 국가재난관리 체계를 전면 개편하면서 재난의 개념과 범위를 새로이 규정하고 용어를 통일하게 되었다. 즉, 과거 재해와 재난으로 이원화된 용어를 '재난'으로 통일하고 재난의 유형을 자연재난, 사회적재난, 해외재난으로 나누어 규정하였다.

「재난 및 안전관리 기본법」은 제정 당시 방화범에 의한 대구 지하철 화재로 인하여 막대한 인명피해가 발생한 사건[26]을 수습하는 과정에서 국가재난관리 체계의 분산과 비효율성 개선이 시급함을 인식하여 관련 법령을 정비하고 재난 및 안전관리와 관련된 기본법을 제정하여 국가재난관리 체계의 개념과 기준을 확립하기 위하여 제정된 것이다.

이 법이 제정되면서 새로이 국가차원의 재난 범주에 포함된 국가기반재난 및 보건재난은 이후 노무현 대통령 집권 당시 청와대 NSC 소속 위기관리센터에서

26) 2003년 2월 18일 대구 도시철도 1호선 중앙로역에서 방화로 일어난 화재이다. 이 사건으로 인해 2개 열차에 편성된 12량의 전동차가 모두 불타고 192명의 사망자와 21명의 실종자 그리고 151명의 부상자가 발생하였다.

주관하여 제정된 「국가위기관리지침」(대통령 훈령 제124호, 2004.7.12. 제정)과 「위기관리 표준매뉴얼」(2004.7.12. 제정)을 통하여 변화된 범위를 세부적으로 규정하였다.

이에 따르면 자연재난(풍수해, 지진), 인적재난(산불, 고속철도 대형사고, 해양·수질 등 대규모 환경오염, 유해물질 유출사고, 공동구 재난, 댐 붕괴, 지하철 대형화재사고, 다중 밀집시설 대형사고), 국가기반재난(사이버안전, 전력, 원유 수급, 원전 안전, 정보통신, 금융전산, 육상 화물수송, 식용수, 보건의료), 보건재난(감염병, 가축 질병), 전통적 안보(북핵 우발사태, 서해 NLL 우발사태, 독도 우발사태, 북한의 우리국민·물자 억류, 개성공단 돌발사태, 대통령 권한 공백, 테러, 재외국민 보호, 소요 폭동, 북한 방문단 집단 망명, 파병부대 우발사태, 비군사적 해상분쟁) 등이 재난의 범위로 규정되었다(「재난 및 안전관리기본법」 제3조).

위의 「국가위기관리지침」과 「위기관리 표준매뉴얼」에서 새로이 재난의 범위에 포함된 국가기반재난의 범위 및 내용을 보면, 국가기반재난의 개념은 "테러, 대규모 시위·파업, 폭동, 재난, 해킹 또는 컴퓨터 바이러스 등의 원인에 의하여 국가경제 및 국민생활, 정부 기능 유지에 중대한 영향을 미칠 수 있는 인적·물적·기능 체계 등이 마비되는 상황으로서 해당 분야로는 에너지, 식용수, 보건의료, 정보통신, 금융전산, 교통, 수송, 원자력, 주요 산업단지 및 정부 중요시설 등이 해당된다"고 정의하였으며 정부가 관리해야 할 유형으로 매뉴얼화된 분야는 사이버, 전력, 원유 수급, 원전 안전, 금융전산, 정보통신, 식용수, 육상 화물 운송, 보건의료 등 9개 분야를 지정하였다.[27] 이와 같이 노무현 대통령 정부 당시 전반적으로 재정비된 재난의 개념과 범위는 미국의 사례에서 살펴본 바와 마찬가지로 사회발전과 환경 및 여건의 변화를 반영하여 상당한 부분의 변화가 이루어졌다.

우리나라에서의 재난 개념 변화 과정을 보면 2004년 「재난 및 안전관리 기본법」이 제정되기 이전에도 '화재·붕괴·폭발·교통사고·화생방사고·환경오염사고 등 국민의 생명과 재산에 피해를 줄 수 있는 사고로서 자연재해가 아닌 것'을

27) 이종열 등 공저, 앞의 책, p.64.

인적재난의 개념을 설정하여 관리하고 있었으나 이러한 개념은 단순 사고의 개념, 즉 비고의적 인적재난의 개념을 적용하였던 것으로써 2004년 「재난 및 안전관리 기본법」이 제정된 이후에 재정비된 광범위한 재난의 개념과는 거리가 있는 것이었다.

2004년 법 제정 이후에는 세계적인 추세에 맞추어 테러, 사이버 안전, 금융전산, 정보통신 등을 포함한 '국가기반재난'의 개념을 도입하여 다른 어느 나라와 비교해도 크게 다르지 않은 다양한 유형의 재난을 재난의 개념에 포함하고 있다.

나. 법제도적 변화의 함의

2003년 2월 발생한 대구지하철 방화 사건을 계기로 정부는 「재난 및 안전관리 기본법」을 제정하여 건국 이후 오랫동안 유지되어 오던 재난 관리 체계(「(구)재난관리법」에 의한 인적재난, 「자연재해대책법」에 의한 자연재해, 「민방위기본법」에 의거한 민방위사태)를 통합, 조정하였다.

그런데 재난관리 기본법으로서의 기능과 이념을 가진 「재난 및 안전관리 기본법」은 재난의 개념과 범위를 일반적인 개념 수준에서 정의하였고 재난의 유형과 범위 등에 관한 세부사항은 규정하지 않았으며 그 구체적 개념 및 유형, 범위는 앞서 살펴본 바와 같이 「재난 및 안전관리 기본법」 제정과 같은 시기에 제정된 「국가위기관리지침」(대통령 훈령 제124호, 2004.7.12. 제정)과 「위기관리 표준매뉴얼」(2004.7.12. 제정)에서 규정하였다.

이렇게 재난관리 체계의 구체적 틀을 상위 법률에 규정하지 않고 하위 규정인 지침과 매뉴얼에 규정하는 법제도 방식을 취한 결과 단임제 대통령을 선출하게 되는 정권 교체기에 기존 정권과는 이념을 달리하는 정권이 집권하면 기존 행정체계를 대폭 개편하였던 상례가 재난관리 체계에도 그대로 적용되어 큰 변화를 맞게 되었다. 즉, 이명박 정부에서는 재난관리 체계를 대폭 개편하면서 전임 정부인 노무현 대통령 집권기에 규정하고 유지했던 재난 개념과 범위는 물론 재난관리 주무 부처 등 재난관리의 많은 부분을 상이하게 변화시키는 결과로 이어졌다.

이명박 정부는 노무현 정부에서 설정한 재난의 개념 및 범위를 대부분 그대로 유지한다는 정책 기조를 취하면서도 자율과 책임, 분권의 원리를 도입한다는 명분으로 노무현 정부 당시 재난관리를 총괄하던 NSC 사무처 소속 위기관리센터(비서관급)을 폐지하고 재난 및 위기관리 업무를 각 부처로 분산시켰다. 이렇게 분산된 국가 재난관리 총괄 기능은 개편된 행정안전부에 재난관리 업무분야를 강화하는 방식으로 임무를 부여하였다.

또한 재난의 개념과 범위를 확대하는 세계적인 추세를 반영하여 재난 개념을 확대한다는 명분으로 군사적 부문의 재난관리(비상대비 분야)와 비군사적 부문의 재난관리(재난안전 분야)를 통합하는 정책을 취하였다. 이러한 방식은 일반 국민 개인의 안전과 보호를 최우선하는 선진국의 재난관리 정책 방식을 수용하면서도 우리나라의 안보 현실을 반영하여 안보 영역을 재난 분야로 포괄하려는 새로운 시도로 평가되었다.[28]

이러한 재난관리 정책 방식은 후일 박근혜 대통령 집권초기의 재난관리 정책에도 이어졌다. 그러나 박근혜 정부는 2014년 4월 16일 발생한 세월호 침몰사고로 인하여 우리나라 국가 재난관리 체계의 총체적 부실과 부패, 무력함이 드러나자 국민안전처 창설, 청와대 위기관리센터 부활 등 우리나라 건국 이래 가장 큰 규모로 재난관리 체계를 개편하였다. 세월호 침몰사고로 촉발된 박근혜 정부의 재난관리 정책 변화는 일반적 재난으로부터 국민 개인의 안전과 보호를 최우선 할 수 있도록 국민안전처를 통하여 모든 국가적 재난관리 통합조정체계를 갖추는 정책으로 전환하는 체계를 갖추게 되었다.

우리나라에서의 재난 개념 변화와 관련하여 미국 등 다른 나라들과 유사한 점을 살펴보면, 재난의 개념 및 범위를 사회 체제의 전반적 발전 및 가치관과 이념의 변화, 시설 및 장비의 대형화, 인터넷・IT 등 첨단 기술과 산업의 발전, 대규모 사건 사고 발생에 따라 확대, 변화시켜 온 점이 같다고 할 수 있다. 또한 다른 나라들과 다른 점은, 우리나라는 다른 나라들과 달리 민방위 사태인 '적의 침공 및 재난'을 재난의 범위에 포함시켜 관리(민방위 기본법)하고 있다는 점이 매우 다른

28) 이종렬 등 공저, 앞의 책, p.66.

차이점 이라고 할 수 있다. 이러한 이유는 우리나라가 북한의 군사적 위협에 상시 노출되어 있는 지정학적 특성으로 인하여 언제 발생할지 모르는 민방위사태를 재난관리 체계에 반영한 것이라고 할 수 있다.

4. 결어 - 법 제도적 보완 필요성

어느 나라이든 재난의 개념과 유형에 대하여 정의하는 것은 현실 사회 현상을 반영한 결과로 나타난다. 중장기적 분석과 판단으로 미래지향적인 재난 대응 체계를 갖추는 것이 각국의 목표라는 점에서는 일치하나 재난에 대한 구체적 대응 체계는 언제나 다양한 재난의 유형이 발생한 이후에 갖추어지기 마련이다.

우리나라의 재난관리 체계에서 재난의 개념 및 범위에 대한 최근의 가장 큰 변화는 국민안전처 창설이라고 볼 수 있을 것이다. 국민안전처는 2014년 4월 16일 침몰된 세월호 사고에 대응하고 구조활동 등 사고를 수습하는 과정에서 국가 재난안전관리 체계의 비효율과 방만한 운영, 재난 업무분야 공무원 및 관계기관 등의 부패와 무사안일 등이 폭넓게 지적되어[29] 대통령 지시에 따라 2014년 11월 19일 창설되었다.

그런데 국민안전처는 창설 당시 국가재난안전업무를 총괄한다는 기능과 임무, 목적으로 창설되었음에도 불구하고 일부 기능이 미흡하거나 급조되어 제 역할을 하지 못하는 경우가 발생하고 있어 법제도적 개선 필요성이 제기되고 있다. 2016년 9월 12일 경주에서 발생한 지진에 대하여 경보 지연 전파 등 제대로 대응하지 못하여 국민적 비판에 직면하기도 하였으며,[30] 여름 혹서기의 폭염 예보 지연,[31] 태풍 피해 예보 및 경보에 실패[32] 등 자연재난에 제대로 대응하지 못하는 기능적

29) 대법원 2015.11.12.선고 2015도6809 전원합의체 판결 참고.
30) "경주 최강지진에 재난대처 총체적 무능 드러낸 국가의 위기관리", 『뉴스1』(2016.9.13.), "경주 지진이 발생하는 동안 안전은 어디에도 없었다", 『시사저널』(2016.9.17.)
31) "지진 긴급재난문자 늦은 안전처, 최근 3년간 폭염경보 문자도 '늑장'", 『경향신문』(2016.9.27.)
32) "안전처 또 '늑장 재난문자'…인명피해 집계도 혼선", 『매일경제신문』(2016.10.6.)

미흡함을 노출시킨 바 있다. 다른 한편으로 최근 국가안보 및 재난 관련 문제에서 중요한 이슈로 제기되고 있는 테러 대응 체계와 관련하여 「국민보호와 공공안전을 위한 테러방지법」 및 동 시행령 등에서 국민안전처는 모든 테러 대응 단계에 참여토록 규정하고 있다. 그러나 국민안전처 내부의 조직별 기능, 임무 등을 살펴보면 테러 대응 체계에 관한 임무분장을 명확하게 규정하지 않고 있다. 법제도적 미비점은 시급히 개선될 필요가 있다.[33]

이러한 내용은 미국의 국토안보부(DHS) 창설 당시에도 유사한 문제점으로 지적되었었다. 미국은 2001년 사상 처음으로 미국 본토가 공격당한 9.11 테러를 복구하고 대응 조치를 하는 과정에서 자국의 테러 대응 및 재난 대응 체계가 수많은 부처와 기관에 분산되어 있어 제 기능을 하지 못한다는 결론을 내렸다. 이에 테러와 재난 대응 관련 22개 부처를 흡수하여 미국 역사상 가장 큰 규모의 행정조직 개편을 단행하여 2003년 1월 24일 국토안보부가 창설되었다. 당초 국토안보부는 테러 대응을 총괄하는 부처로 창설되었으나 테러 대응의 핵심 기관이라고 할 수 있는 CIA와 FBI의 반발로 양 기관의 대테러 기능을 흡수하지는 못하였다. 대신에 국토안보부(DHS)는 창설 당시 독립 기관으로 역할을 수행하던 연방재난관리청(FEMA)을 산하기관으로 편입하여 테러 대응 기능을 포함한 국가 재난안전관리의 중심 역할을 부여함으로써 기능상 미흡함을 보완하였다. 즉, 미국의 연방재난관리청(FEMA)은 중앙에서 재난 대응의 지원과 조정 역할을 수행하는 컨트롤 타워로서 기능하며 재난 대응 현장에서는 지역 관할 경찰서장 또는 지역 자치단체장 등이 현장 컨트롤 타워가 되어 이중적 대응체계를 구성하고 있다.[34]

우리나라의 국민안전처도 세월호 침몰 사건이라는 대규모 재난 사고로 인하여 창설된 부처로서 중앙의 재난 대응 컨트롤 타워 역할이 부여되어 있고 각종 재난 및 테러 등에 대하여 중앙에서 현장까지 모든 과정을 통제하는 기능을 수행하도록 하고 있다. 그러나 세월호 침몰사건에서 지방자치단체 등 현장과 지역 수준의

33) 테러방지법 제3조 (국가테러대책위원회 구성), 테러방지법 시행령 제17조 (테러복구지원본부), 테러방지법 시행령 제19조 (테러대응구조대)

34) 윤민우, “최근 테러리즘의 동향 및 국내 대테러체계 구축방향”, 『신안보연구』, 제1권 제1호(2016년 여름, 국가안보전략연구원, 2016.8.2.), p.27.

컨트롤 타워가 제대로 작동하지 못했다는 평가가 있는 만큼 지역 레벨의 재난 현장 대응체계 구축은 우리의 과제로 남아있다.[35] 즉, 재난 및 테러 발생 시 중앙에서 작동하는 국민안전처 주도의 중앙컨트롤 타워와 경찰 및 자치단체 주도의 현장 컨트롤 타워 간에 이원적, 유기적 협력체계가 구축되어야 효율적인 재난 대응체계가 작동될 수 있을 것이다.[36]

또한 재난관리 문제가 신안보 개념의 요소로서 작동하기 위해서는 소위 '재난 거버넌스'의 체계가 적절한 방식으로 적용될 수 있도록 법제도적으로 보완될 필요가 있다. 지금까지 전통적이고 통상적인 방식으로 재난에 대응하는 것을 '재난관리'라고 해왔는데, 이는 정부와 기술적 전문가들에 의한 재난 대응 체계를 총칭하는 의미이다.

지금까지 발생한 대규모 재난에서 시민들이 참여하여 재난에 대응하였던 대표적 사례는 2005년 미국 뉴올리언즈에서 발생한 허리케인 카트리나 사례, 2007년 충남 만리포 해상에서 유조선 '허베이 스피릿'호가 좌초되어 원유가 유출된 사례 등에서 재난 대응 및 복구에 시민들이 참여하여 효과적으로 대응하였던 것으로 평가되었으며, 2014년 세월호 침몰 사고 당시에도 많은 자원봉사자들이 구조활동에 나섰었다. 이와 같이 재난 발생 시 시민들의 자원봉사 참여로 재난 대응 및 복구에 큰 효과를 본 사례는 많았으나 재난 발생 이전 단계인 예방 및 대비 단계에서 시민들이 참여하고 재난관리 정책에 참여하는 법적, 제도적 장치는 아직 미흡하다고 할 수 있다. 최근의 대표적 사례인 세월호 침몰 사건에서 사고의 주된 원인이 관계기관과 관계자들의 무능과 무사안일, 부패 등에서 비롯되었다는 사실이 재판과정에서 밝혀진 것을 보면 재난관리의 초기 단계부터 시민들이 참여하는 협력적 거버넌스(collaborative governance)로서의 '재난 거버넌스(disaster governance)'의 필요성이 제기된다.[37]

---

35) 이재은, "국가재난법제의 정비와 실효성 확보 방안", 『한국위기관리논집』, 제10권 제12호 (2014.12.), p.7.
36) 윤민우, 앞의 책, p.27.
37) 이영희, "재난관리, 재난 거버넌스, 재난 시티즌십", 『경제와 사회』(비판사회학회, 2014.12.), p.70.

‘재난 거버넌스’는 시민들이 재난관리의 초기 단계부터 참여하여 관료, 기술적 전문가, 담당기관 등과 함께 재난관리의 모든 과정에서 집단적 의제 선정 및 해결책 모색 등으로 안전하고 합리적인 재난정책을 마련하는 것을 말한다. 세월호 사건이 아직도 우리 사회에서 치유되지 않고 논란과 아픔으로 남아있는 현실을 보면 시민들이 참여하는 ‘재난 거버넌스’의 제도화가 합리적인 재난관리의 대안이라는 생각을 갖게 한다.

참고문헌

국가정보포럼.『국가정보학』. 서울 : 박영사, 2006.

김인범・류상일・송윤석・양기근・이동규・이주호・홍영근 공저.『재난관리론』. 서울 : 대영문화사, 2014.

문정인.『국가정보론』. 서울 : 박영사, 2009.

백종천・이민룡 공저.『한반도 공동안보론』. 서울 : 일신사, 1993.

성낙인.『헌법학(제9판)』. 서울 : 법문사, 2009.

이재은.『위기관리학』. 서울 : 대영문화사, 2012.

이종열・이종영・최진식・정지범 공저.『재난관리론』, 서울 : 대영문화사, 2014.

전 웅.『현대국가정보학』. 서울 : 박영사, 2015.

김승렬, "국가위기관리 법제에 관한 연구."『법제』(법제처, 2007)

윤민우. "최근 테러리즘의 동향 및 국내 대테러체계 구축방향."『신안보연구』, 제1권, 제1호(2016 여름)

이영희. "재난관리, 재난 거버넌스, 재난 시티즌십."『경제와 사회』(비판사회학회, 2014.12.)

이재은. "국가재난법제의 정비와 실효성 확보 방안."『한국위기관리논집』, 제10권, 제12호(2014.12.)

이창주. "미국에서의 국가안전보장 관련정보 공개제한에 관한 연구."『한국외국어대학교 박사학위 논문』(2013.2.)

대법원 2015.11.12.선고 2015도6809 전원합의체 판결.

헌재 1992.2.25. 자89헌가104 결정.

"경주 최강지진에 재난대처 총체적 무능 드러낸 국가의 위기관리."『뉴스1』, 2016. 9.13.

"경주 지진이 발생하는 동안 안전은 어디에도 없었다."『시사저널』, 2016. 9.17.

"지진 긴급재난문자 늦은 안전처, 최근 3년간 폭염경보 문자도 '늑장'."『경향신

문』, 2016, 9.27.

“안전처 또 ‘늑장 재난문자’…인명피해 집계도 혼선.”『매일경제신문』, 2016.10. 6.

Energy and the National Goals – A Crisis of Confidence, 15 July, 1979.

Robert Mandel. *The Changing Face of National Security: A Conceptual Analysis*. Westport, Connecticut: Greenwood Press, 1994.

The White House. *National Security Strategy of the United States*, 1988.1.

_____. *A National Security Strategy of Engagement and Enlargement*, 1995.2.
[http://www.au.af.mil/au/awc/awcgate/nss/nss-95.pdf]

_____. *The National Security Strategy of the United States of America*, 2002.9.

David A. Baldwin, “The concept of security.” *Review of International Studies,* 23/1(1997).

Harold Lasswell, “The Garrison State.” *American Journal of Sociology,* 46/4(1941).

로앤비, [http://www.lawnb.com/]

Abstract

The Perception of the new security on disaster management, and legal recognition

Chang Joo Lee (Sungkyunkwan University)

The definition of former national security has been limited to military sector dealing with external aggression. However, end of Cold War has lead its ideological notion to extend from military conflict to comprehensive security including fields in diplomacy, economy, environment and even coping with disaster management.

Combined with progression of information technology and development of transportation, recent 'Smart society' has pushed the boundaries between nations resulting in reestablishment of the term of the security.

'Disaster management' used to be regarded as mainly coping with natural disaster ruling out domestic affairs and public welfare. However, with the outbreak of man-made catastrophes, social disasters, hybrid and international disasters, its new trend has affected the recognition on its original term of national security containing terrorism and cyber security.

Korea has well adopted the advanced approach on broadened security by legalizing and institutionalizing supporting systems represented by establishment of 'The Ministry of Public Safety and Security'. However, it has recently faced wide criticism over coping with Gyeongju earthquake, typhoons and etc. The improvement of response systems with updated legislation is necessary to manage the new security disasters.

Key Words: national security, disaster, disaster management, man-made catastrophe, social disaster, hybrid disaster, international disaster, terrorism

투고일 : 2016.11.5. 심사일 : 2016.11.20. 게재확정일 : 2016.12.10.

V

온라인 뉴스 기반 국가안보 이슈 변화 분석

이영환 (건국대학교)
김찬우 (영남대학교)

Summary

이 연구에서는 개체명 인식 기법을 이용하여 신문 기사를 대상으로 주요 이해관계자 및 행위에 대하여 네트워크 분석을 수행하였고, 언론에서 나타난 주요 인물, 기관, 활동을 기반으로 국가안보라는 이슈의 변화를 분석하였다. 먼저 2013년~2016년 10월까지 국가안보가 포함된 신문 기사에서 개체를 추출한 후 기간별 개체의 차이를 살펴본 다음 개체별 네트워크 분석을 통해 개체의 구조와 내용을 분석하였다. 마지막으로 시계열 분석을 통해 시기별 개채 분포의 차이를 살펴보았다. 그 결과 국내 안보 이슈는 전통적인 군사안보에 초점이 맞춰 있고, 한미동맹의 강화를 통해 안보를 확보하려는 점이 확인되었다. 이를 통해 개체명 인식 기법 기반 네트워크 분석이 국가 안보 이슈 분석에 유용함을 확인할 수 있었다.

| 키워드 | 국가안보, 네트워크 분석, 개체명 인식, 텍스트 마이닝

1. 서론

소셜미디어 시대에 들어 다양한 스마트 기기를 통해 대중들이 의견을 표출하고 있다. 특히 소셜 네트워크 서비스(SNS)나 블로그, 댓글 등을 통해 실시간으로 생산된다. 이렇게 생산된 의견들을 수집할 수 있는 기술도 발전하고 있다. 또한 대용량 정보를 체계적으로 구조화하여 사용자에게 의미 있는 지식을 제공하는 방법론에 대한 연구도 활발하게 진행 중이다. 기본적인 방법으로는 텍스트 마이닝(Text Mining)으로 텍스트 중 단어의 빈도 분석을 통해 중요 키워드를 찾는 것이다. 텍스트에 담겨 있는 긍정, 부정, 중립 등 선호도 분석으로 의견을 확인하는 오피니언 마이닝(Opinion Mining)도 있다. 최근에는 개체명 인식을 통한 분석이 관심을 끌고 있다.

개체명 인식(Named Entity Recognition)은 텍스트에서 사용된 인명, 지명, 기관 등의 정보를 식별하여 분류하는 작업을 말한다. 개체명은 문서에서 중요한 핵심어로 자연어 처리(Natural Language Processing) 연구에서 다양하게 응용되고 있는데, 다양한 분야의 정보가 담겨 있는 문서 데이터에서 개체를 자동으로 추출하여 개체명을 인식하고, 그 중에서 핵심 개체를 도출하여 개체들 간의 연관관계 분석에 활용된다. 즉 개체 정보들 사이에서 새로운 지식을 자동으로 추론하는 과정을 통해 의미 있고 정확한 지식을 분석하여 제공할 수 있게 된다.

본 연구에서는 신문 기사를 대상으로 단어나 문장단위가 아닌 원문 텍스트에서 개체명 인식기를 활용하여 자동으로 추출된 개체를 기반으로 분석을 수행하였다. 주요 이슈를 다루는 신문 기사 텍스트에서 도출되는 개체의 성격과 그 개체의 시기별 분포 변화를 분석함으로써 이슈에 대한 관점이나 의견을 파악할 수 있기 때문이다. 신문 기사는 이슈에 대해 주요 이해관계자의 의견이 포함되어 있고, 포탈 사이트를 통해 분석 가능한 대량의 자료를 제공하기 때문에 연구 자료로 선택하였다.

이를 위해, 최근 국가안보 관련 기사를 대상으로 2013년 1월 1일부터 2016년 10

월 31일까지 46개월의 기사를 수집한 후, 전체 기사의 개체를 추출하기 위해 개체명 인식기를 사용하였다. 개체명 인식은 주로 인물, 지명 등이 추출되는데, 본 연구에서는 인물, 지명 외에 사건, 조직 등을 추가로 분석하고 그 개체들이 서로 어떻게 연결되었는지, 시간에 따라 어떻게 변화되었는지를 분석하였다.

이렇게 추출된 개체들을 세 단계로 분석하였다. 먼저, 국가안보관련 뉴스 기사에서 형성된 주제를 분석하기 위해 전체 데이터에서 인물, 지명, 사건, 조직으로 개체를 추출하여 그 특징을 분석하였다. 그리고 범주별로 도출된 개체명을 네트워크 분석 기법을 통해 분석하였다. 마지막으로 시기별로 구분하여 개체의 변화를 검토하였다. 이를 통해 개체명 인식을 통한 국가안보의 주요 이슈의 비중변화를 확인하였다.

따라서 본 연구는 46개월 간의 국가안보 관련 기사를 통해 나타난 국가안보 활동 중 주요 이해관계자(기관, 인물), 사건, 지역 등을 추출하고, 그들 간의 관계를 확인함으로써 활동의 변화를 분석한다. 즉 정부, 국가기관 등 기관과 국내외적으로 발생한 이슈나 사건 등이 분석대상이며, 이들 간의 관계 변화 양상을 확인하는 것이 분석 목적이다. 이를 통해 지속적인 관심을 받고 있는 영역과 관심이 줄어든 영역을 확인한 후 문제점을 분석하여 향후 국가안보 정책 수립에 필요한 요소가 무엇인지 제시하고자 한다.

2. 관련 연구

가. 국가안보

국가안보 개념의 형성은 근대 유럽 국가들의 탄생 이후 국가들 간의 전쟁 양상과 밀접한 관계가 있다.[1] 당시 국가의 가장 중요한 목표는 생존이고, 안보는 대내

1) 이수형・전재성, “국제안보 패러다임의 변화와 동북아 안보체제,”『국방연구』, 제48권, 제2호(2005), pp.71-100.

외적인 물리적 공격이나 공격의 위협으로부터 주권국가와 그 통치체제를 방어하는 것이다. 그리고 전통적으로는 국가를 기본 단위로 하여 국외적 위협(external threat), 주로 군사적 침략으로부터 국가 및 국민을 보호한다는 의미에서 안보라는 용어가 사용되었다.[2)]

오늘날 경제사회적 발전과 자유와 인권 등 보편적 가치에 기초한 정치체제가 확대되고, 기존 국가간 전통적인 위협뿐만 아니라 국제테러, 대량살상무기(WMD) 확산 등 새로운 안보문제들이 국가와 국민의 안전을 위협하고 있는 상황이다. 또한 빈곤, 환경오염, 질병의 확산 및 자원 확보를 위한 경쟁 등 다양한 요인에 의해서도 위협받을 수 있다는 인식이 되면서 기존 안보 개념이 변화되었다.[3)] 즉 경제, 에너지, 환경, 보건 등 비군사적 영역의 안보문제가 새롭게 부각됨에 따라 국제적인 공동대처와 아울러 국내적으로도 광범위한 영역에서 종합적인 대처가 요구되고 있다. 따라서 새로운 위협과 갈등요인을 극복하고 평화와 안정을 확보하기 위해서는 제반 분야에서의 안보역량 강화와 더불어 국제기구와 지역별 다자안보 대화를 통한 범세계적인 공동노력을 하고 있다.[4)]

따라서 서구 선진국들은 안보(security) 개념을 전통적 안보(conventional security)개념으로부터 포괄적 안보(comprehensive security) 개념으로 전환하였다. 과거 전쟁이나 무력 침공 등과 같은 전통적 안보 위기만을 국가 안전보장의 위협 요인으로 보았으나 국민, 영토, 주권, 핵심기반 등을 위협하고 마비시킬 수 있는 재난이나 질병, 전염병, 실업, 파산까지도 국가 안보를 위협하는 국가위기로 규정하고 그 관리체계를 구축하고 있다. 테러는 물론이고 각종 사회 위협요소, 국가사회의 안녕질서를 위협하는 요소들까지도 국가안보 위협 차원에서 다루고 있다.[5)]

---

2) 이재은, “포괄적 안보 개념하에서의 국가 위기관리 법제화의 의의와 내용 분석,”『한국위기관리논집』, 제2권, 제2호(2006), pp.19-35.
3) 윤이숙. “환경적 쟁점과 한국의 안보,”『국방연구』, 제52권, 제1호(2009), pp.75-96. 전웅, “21세기와 한국의 안보: 국제환경변화에 따른 한국의 안보 위협들,”『국방연구』, 제48권, 제2호(2005), pp.3-36.
4) 국가안전보장회의,『평화번영과 국가안보』, (서울: 국가안전보장회의 사무처, 2004).
5) 이재은, “국가안보 환경의 변화와 국가위기관리 - 포괄적 안보 개념 하에서의 국가위기 유형,”『한국위기관리논집』, 제9권, 제2호(2013), pp.177-198.

새로운 안보 위협 요소들을 파악하는데 도움을 주는 개념들을 살펴보면 다음과 같다.[6] 첫째, 포괄적 안보(comprehensive security)의 개념으로 군사뿐만 아니라 비군사 요소들까지를 포괄하여 설정되는 개념이다. 즉 정치, 경제, 사회, 문화, 환경, 자원, 기술과 대형재난 등 비군사 분야를 포함하는 포괄적인 개념으로 확대된 것이다.

둘째, 인간안보(human security)의 개념으로 안보의 주체와 위협받는 대상이 국가중심에서 개인과 인류 공동체 중심으로 확대된 것이다. 인간안보는 개인을 두려움(fear)과 결핍(wants)으로부터 해방시키는 것을 주요 목표로 하며, 안보의 주체, 실현가치, 위협근원, 안보수단의 측면에서 국가안보와는 구별되는 개념이다. 빈곤으로부터의 자유, 충분한 식량의 확보, 질병으로부터의 보호와 치료 보장, 환경오염과 자원고갈의 위협 대비, 고문, 전쟁, 내란, 범죄, 마약남용, 자살 등 신체적 안전의 보호, 공동체안보는 전통문화의 보존과 종족 유지, 정치안보는 시민권 확보와 정치적 탄압으로부터의 자유 등이 있다.

셋째, 협력안보(cooperative security) 또는 공동안보(common security) 개념이다. 이는 자국에 대한 군사적 또는 정치적 위협이 있는 경우는 긴밀한 관계에 있는 국가와 동맹을 체결하여 공동으로 대처한다는 집단방위(collective security)를 기반한다. 즉 적과 협력하여 원하지 않는 전쟁을 회피한다는 것으로 전쟁을 방지하기 위해서는 공격 무기나 군사 시스템을 배제하는 방식으로 진행된다.

넷째, 초국가적 위협(transnational threats) 개념은 주로 비국가 행위자(non-state actors)로 인해 발생하는 위협으로 국경을 초월(trans-boundary 또는 across border)한다. 예를 들어 재난, 질병, 난민, 환경오염 등의 경우 일국 차원에서 해결할 수 없는 문제이다. 따라서 글로벌 차원에서의 다자적인 공동접근을 통해 문제해결을 모색하게 된다.

이러한 포괄적 안보는 한국의 국가안보전략에서도 확인된다. 박근혜 정부는 2016년 안보 분야 국정기조로 '평화통일 기반 구축'으로 선정하고 '영토·주권 수

6) 김영호. "비전통적 안보위협과 군의 역할,"『평화연구』, 제17권, 제2호(2009), pp.157-187.

호와 국민안전 확보', '한반도 평화 장착과 통일시대 준비', '동북아 협력 증진과 세계 평화·발전에 기여'를 국가안보목표로 설정하였다.[7] 이에 따라 북한의 무력 도발, 잠재적 미래 위협, 초국가적 위협 등에 대하여 국민의 생명과 재산을 보호하고, 남북관계 정상화 및 적극적인 통일을 추진한다는 것이다. 이러한 배경에 따라 "통일 대박"이라는 메시지가 나타난 것이다.

다음으로 동북아 협력 및 세계 평화의 경우 주변국과의 평화, 안정을 추구하는 것이다. 특히 평화통일 기반 구축을 위해 북한 도발의 사전 억제 및 도발시 단호한 대응, 북한의 핵능력과 미사일 위협에 효과적 대응을 위한 한미 연합방위태세 강화 등이 주요 전략으로 설정하고 있다. 또한 테러, 사이버공격, 기후변화, 감염병, 대규모 재난 등 초국가적·비군사적 위협 및 미래 잠재적 위협에 대응하기 위해 주변국과 전략적 협력을 강화하는 등의 전략을 세우고 있다. 외교영역에서는 폭력적 극단주의, 난민, 기후변화, 사이버 안보 등과 같은 비전통적 안보 이슈가 세계적인 불안정 요인으로 지적하면서, 한반도의 경우 북한의 핵·미사일, 인권 문제 및 사이버 공격에 따른 대응에 초점을 맞추고 있다. 특히 인권 문제의 경우 유엔 북한인권사무소가 서울에 개소되면서 유엔을 중심으로 대북 외교를 진행하고 있다.[8] 즉 국내 안보영역에 대하여 재난, 질병, 테러 등 다자적인 영역의 경우 동북아 주변국과의 외교를 통해 평화를 추진하고 있으며, 대북 정책의 경우 핵, 미사일 실험 등으로 인하여 전통적인 안보 영역이 강화되고 있다.

나. 개체명 인식

개체명 인식(Named Entity)은 문서에서 개체명을 추출하고 범주를 결정하는 것을 말하여, 개체명의 범주는 인명, 지명, 조직명, 날짜, 시간, 화폐, 상품명 등을 포함된다.[9] 이러한 개체명 인식은 주로 정보 검색 및 추출, 문서 분류, 자동 정렬

7) 대한민국 국방부, 『2016 국방백서』(2016), pp. 32~33.
8) 외교부, 『2016 외교백서』(2016), pp.10~22.
9) 이경희·이주호·최명석·김길창, "한국어 문서에서 개체명 인식에 관한 연구," 『한국정보과학회 언어공학연구회 학술발표 논문집』(2000), pp.292-299.

등에서 이용된다. 따라서 해당 분야의 연구는 주로 컴퓨터 공학 분야에서 연구되고 있다.

최근 연구에서는 효율적인 개체명 인식을 위해 위키피디아와 프리베이스(Freebase)를 기반으로 학습하여 효율성을 높인 연구가 있다.[10] 즉 개체명 사전을 통해 키워드가 어느 범주에 들어가는지를 훈련하는 방법에서 새로운 언어나 개체명이 생길 경우 자동으로 범주를 나눌 수 있다는 것이다. 또한 자연어 기반의 인터페이스(Natural Language Interface)에서 발생하는 언어에 대해 개체명 인식을 효율적으로 추출하는 방식에 대한 연구가 있다.[11] 즉 SNS 상에 발생하는 텍스트에 대한 범주를 구성하기 위해서 실험한 연구이다. 또한 국립국어원 표준국어대사전과 세종 말뭉치에서 명사를 사용하여 사전을 구축하고 기계학습 기간의 개체명 인식 및 분류 실험한 연구도 있다.[12]

그러나 개체명 인식과 관련된 연구로 개체명 인식기를 활용한 연구는 거의 없는 상황이다. 즉 개체명 인식의 성능 개선을 위한 연구가 주로 이루어지고 있으며, 이를 활용한 연구는 아직 진행되지 않고 있다. 따라서 개체명 인식을 통해 뉴스 기사 분석에 적용하여 주요 의미를 파악하고 변화를 확인하는 것은 의미가 있을 것이다.

다. 네트워크 분석

최근 들어 사회과학 분야에서 네트워크 분석이 활발하게 이용되고 있다. 학술논문에 등록된 저자, 논문제목, 주요키워드 등의 텍스트를 대상으로 국가 간 학문분야 비교분석, 공저자 네트워크 분석, 공동연구 네트워크 분석 등이 사회연결망 분석 방법을 활용하여 연구가 되고 있다.[13]

---

10) 박영민・김예진・강상우・서정연, “개체명 인식 코퍼스 생성을 위한 지식베이스 활용 기법,” 『인지과학』, 제27권, 제1호(2016), pp.27-41.

11) 배경만・김성현・고영중・김종훈, “자연어 기반 인터페이스에서 개체명 패턴을 이용한 효과적인 개체명과 주제어 인식 방법,” 『한국정보기술학회논문지』, 제12권, 제1호(2014), pp.121-129.

12) 최윤수・차정원, “Word Embedding 자질을 이용한 한국어 개체명 인식 및 분류,” 『정보과학회논문지』, 제43권, 제6호(2016), pp.678-685.

특히 텍스트화된 자료를 네트워크 분석 방법을 활용하여 의미를 분석하는 의미연결망 분석도 활발하게 진행 중이다. 의미연결망 분석은 텍스트 내에 존재하는 단어들의 중요성과 연결성을 측정하는 것이다. 즉 텍스트 내에서 핵심적인 단어가 무엇이고, 그것들이 서로 어떻게 배열되고 연결되어 있으며, 텍스트에 포함된 각 주요단어가 네트워크 내에서 각 구성 노드(node)로서 어떤 역할을 수행하고 있는지에 대한 구조적 특성을 분석하는 것을 말한다. 네트워크는 구성하는 노드(node), 링크(link), 그리고 이들 간의 연결구조(structure) 등의 기본 요소를 가지고 있는데,[14] 네트워크 내의 노드는 각각 다른 위계적 역할을 가지며 이러한 위계적 역할의 차이는 네트워크 전체의 모습을 변화시킨다.[15] 즉, 단어가 전체 네트워크에서 어떠한 위치에 있는지, 연결된 단어는 무엇인지 등을 분석하여 그 의미를 파악할 수 있게 된다.

의미연결망 분석이 가지는 장점은 네 가지로 구분할 수 있다.[16] 첫째, 텍스트 데이터에서 구조화된 패턴 도출이 가능하다. 사용된 단어와 함께 사용된 단어들의 패턴을 확인함으로써 메시지 패턴을 확인할 수 있다는 것이다. 둘째, 텍스트에 포함된 단어들의 의미론적 연관구조 파악이 용이하다. 또한 단어들의 사용과 배열을 통해 단어들의 의미론적 연관구조를 파악하는 것으로 기존의 내용분석 방법보다 효과적이다. 셋째, 자료입력 실수와 노동력 투입시간을 줄일 수 있으며, 넷째, 메시지 내부에 잠재된 메시지 전달자의 의도를 계량화하고 도식화할 수 있다. 즉 분석에 프로그램을 활용하여 분석함으로써 대량의 텍스트를 짧은 시간에 분석할 수 있다는 것이다.

의미연결망 분석은 단어 간의 의미론적 연관에 주목하기 때문에 사용된 개별 단어보다는 특정 단어가 얼마나 반복적으로 사용되는지 공동출현 (co-occurrence)

13) 이수상, 『네트워크 분석 방법론(부산대학교 사회과학연구원 연구총서 2)』, (서울: 논형, 2013)

14) 장하용, "언론보도와 비평의 구조: 신문보도의 비평에 대한 네트워크 분석," 『한국언론정보학보』, 제 16호(2001), pp108-135.

15) Wasserman, S., & Faust, K. *Social Network Analysis: Methods and applications*, (Cambridge: Cambridge University Press, 1994)

16) 남인용・박한우, "대권 예비후보자 관련 신문기사의 네트워크 분석과 홍보전략," 『한국정당학회보』, 제6권, 1호(2007), pp.79-107.

하는 단어는 무엇이고 두 단어 사이의 연결은 어떻게 이루어지는가를 분석한다. 또한 단어의 관계성을 통해 의미화 패턴을 도출한다. 따라서 단어의 공동출현 관계는 메시지 안에서 특정한 의미를 만들게 된다.[17] 이러한 단어 간의 연결 관계를 토대로 신문기사의 의미를 파악하거나 발견된 의미를 통해 프레임을 도출하는데 유용한다.

따라서 관련 연구는 신문기사를 대상으로 연구가 이루어지고 있다. 예를 들어 인간배아 복제에 대한 연구결과를 다룬 신문기사를 대상으로 핵심 단어들간 연결망구조를 분석하여 시기별 언론 보도의 변화와 신문마다 상이한 프레임을 분석한 연구가 있다.[18] 또한 '빅데이터' 관련 신문 기사를 의미연결망 기법으로 분석하여 '빅데이터' 용어가 시기별로 변화되고 있는 점을 밝힌 연구가 있다.[19] 그 외 대통령선거에 출마한 예비후보자들의 이미지에 대해 언론이 어떻게 구조화하여 표현하고 있는지 분석한 연구,[20] 북한 관련 이슈에 대한 대통령 후보 합동 토론의 내용을 언어네트워크 기법을 이용해 분석한 연구,[21] 박근혜 정부의 '창조경제 개념'에 대한 언론의 보도내용에 담긴 의미가 무엇인지를 분석한 연구[22] 등이 있다.

사회적 이슈를 주제어로 선정해 네트워크 구조를 분석한 연구도 활발하게 이루어지고 있는데, '메르스'라는 주제어로 검색해 각 언론사의 보도경향과 주요단어들의 구조와 연결성을 조사한 연구,[23] 메르스 확산에 대한 정부의 위기 대응 메시지를 정부의 보도자료를 바탕으로 분석한 연구,[24] 한류에 대한 미국과 중국 언론

17) 박한우・Leydesdorff, "한국어의 내용분석을 위한 KrKwic 프로그램의 이해와 적용," 『Journal of the Korean data analysis society』, 제6권, 5호(2004), pp.1377-1388.
18) 김만재・전방욱, "언어네트워크 분석 기법을 활용한 인간배아복제 신문보도 분석," 『한국 생명윤리학회』, 제13권, 제2호(2012), pp.19-34.
19) 최윤정・권상희, " '빅데이터' 관련 신문기사의 의미연결망 분석," 『사이버커뮤니케이션학보』, 제31권, 제1호(2014), pp.241-284.
20) 남인용・박한우, 앞의 글.
21) 박성희, "제17대 대통령 후보 합동 토론 언어네트워크 분석: 북한 관련 이슈를 중심으로," 『한국언론정보학보』, 통권 45호(2009), pp.220-254.
22) 차민경・권상희, "언론의 '창조경제'에 대한 의제설정 의미연결망 분석," 『한국언론학보』, 제59권, 제2호(2015), pp88-120.
23) 권호천, "메르스 사태에 대한 신문보도의 의미연결망 분석," 『의료커뮤니케이션』, 제11권, 제1호(2016), pp.65-82.
24) 이미나・홍주현, "메르스 확산에 따른 정부의 위기 대응 메시지 언어 네트워크 분석," 『한국콘텐츠학회논문지』 제16권, 제5호(2016), pp124-136.

의 보도 프레임을 분석한 연구[25] 등의 다양한 주제로 연구들이 이루어져 왔다.

의미연결망 분석 방법론이 가진 장점을 바탕으로 다양한 분야에서 그 활용이 증가하고 있는 추세이지만 국가안보와 관련 보도기사의 분석에는 아직 그 적용이 이루어지지 않고 있다. 또한 개체명 인식을 활용한 연구는 거의 없는 상황이다. 따라서 본 연구에서는 빈도 기반 키워드 추출이나 연구자의 선택이 아닌 원문 텍스트에서 개체를 도출하는 개체명 인식 방법을 사용하여 네트워크 분석을 하고자 한다.

3. 연구 방법

가. 데이터 수집

언론은 주요한 사건이 발생했을 경우 관련 사실에 대한 보도가 집중적으로 이루어진다. 그러나 새로운 사건의 발생으로 인하여 기존의 사건에 대한 보도량은 줄어들게 된다. 따라서 상시적으로 국가안보와 관련된 이슈와 더불어 특정 시기에 집중적으로 논의되는 이슈를 수집하기 위하여 박근혜 정부 시기에 보도된 국가안보와 관련된 기사 전체를 분석의 대상으로 정했다. 자료의 수집을 위해 웹크롤링 기법을 사용하여, 2013년 1월 1일~2016년 10월 31일 동안 네이버 뉴스 섹션에 게재된 기사 중 국가안보가 등장하는 기사를 수집하였다.[26] 데이터 수집 결과 총 82,384건이 기사가 수집되었다. [표 1]은 기사 수집 결과를 연도별/월별로 구분하여 나타낸 것이다.

---

25) 최수진, “한류에 대한 미・중 언론보도 프레임 및 정서적 톤 분석,”『한국언론학보』, 제58권, 제2호(2014), pp.505-577.

26) 현재 네이버 뉴스섹션에서는 조선일보, 중앙일보, 동아일보, 한겨레, 경향신문 등 종합지 10종과 뉴스1, 뉴시스 연합뉴스, MBC뉴스, KBS뉴스, SNS 뉴스 등 통신사와 방송 14종, 경제지 7종, 인터넷 신문 5종, IT 4종, 스포츠/연애 48종, 매거진 16종, 지역신문 3종, 전문지 8종, 포토 5종, 정부브리핑, 성명자료실 등 기타 4종의 언론사에서 기사를 제공하고 있다.

[표 1] 국가안보 기사의 수집 결과

구분	2013년	2014년	2015년	2016년
1월	1,731	1,419	890	1,863
2월	**3,040**	1,927	1,190	**3,557**
3월	2,743	1,705	1,917	1,465
4월	1,865	2,114	941	910
5월	825	2,346	1,113	870
6월	2,007	2,025	906	1,355
7월	1,172	1,525	1,796	2,541
8월	1,134	1,943	**5,564**	2,259
9월	986	1,243	1,380	1,882
10월	1,276	**3,090**	1,875	1,809
11월	1,619	1,287	1,599	
12월	**3,098**	1,612	970	
합계	**21,496**	**22,236**	**20,141**	**18,511**

분석 대상인 국가안보 관련 기사 건수는 2015년 8월 5,564회로 가장 높았는데, 당시 남북 접촉 고위급 접촉하여 그 성과를 보고하는 보도가 높았기 때문이다. 다음으로 2016년 2월 3,557회, 2013년 12월 3,098회, 2013년 2월 3,040회 등의 순으로 나타났다. 또한 연도별로는 2014년도에 22,236회로 가장 많은 보고가 있었으며, 다음으로 21,496회의 기사가 있었다.

나. 데이터 전처리

수집된 신문 기사는 인터넷 사이트를 통해 수집된 웹 페이지 형식이기 때문에 언론사명, 연관된 기사 리스트, 신문사 저작권 문구 등의 불필요한 요소들이 있다.[27] 이러한 요소를 기사의 본문만 추출하는 작업을 진행하였다. 그러나 수집된

27) 예를 들어 웹페이지 기사 하단에 기사 본문과 연관된 기사나 [00신문의 이 시간 인기기사]와 같은 형식으로 신문사의 인기기사 등을 함께 나타나는 경우 제거하였다. 또한 '00신문은 한국온라인신문협회(www.kona.or.kr)의 디지털뉴스이용규칙에 따른 저작권을 행사합니다' 등의 신문사별 고정된 저작권 문구 등은 일괄 삭제하였다.

기사 중 사진 기사의 경우 제목만 존재하기 때문에 이미지만 존재하는 기사는 제외하였다. 또한 일반적인 텍스트 마이닝은 형태소 분석을 진행하는데, 본 연구에서는 원문을 대상으로 개체명을 추출하기 때문에 따로 형태소 분석을 통해 키워드를 추출하는 작업은 진행하지 않았다. 다만 분석 오류를 줄이기 위해 기사 본문에 사용된 특수문자('(', ')', '[', ']', '-', '▼', '】', '【', 'ⓒ' 등)은 일괄 제거하였다.

다음으로 개체명 추출 결과 동일한 의미의 단어가 줄임말의 경우 명칭을 통일하는 작업을 진행하였다. 예를 들어 기관 개체명 결과 '국가안보회의'나 '국가안보보장회의' 등은 동일한 표현으로 볼 수 있는데, 이와 같은 경우 '국가안전보장회의'와 같이 하나의 대표 형태로 통합하였다. 또한 인물 개체명 결과에서 나타나는 '박', '이' 등은 원문 기사에서는 '박 대통령', '이 대통령' 등에서 분석된 것으로 실제 '박근혜', '이명박' 등을 지칭하는 것이다. 따라서 단순 '박'을 '박근혜'로 변경하지 않고 '박 대통령'으로 표현된 원문에 한하여 '박근혜 대통령'으로 치환하는 과정을 거쳤다.

본 연구에서는 원문을 최대한 수정하지 않은 상태에서 개체를 추출하기 때문에 주로 명사 개념어를 통해 도출된다. 그러나 개체명 인식의 경우 동일한 단어가 장소나 기관으로 구분되어 나타날 수 있다. 예를 들어 "국방부는 그 사실을 부인했다"와 "박근혜 대통령이 국방부를 방문했다"라는 문장이 있을 경우 앞의 국방부는 기관을 뜻하지만, 뒷 문장에서 국방부는 장소를 뜻한다. 따라서 개체명 인식 결과에서 장소나 기관 등 구분된 개체 중 동일한 단어는 네트워크 분석에서는 한 개로 통합하였다.

다. 데이터 분석

본 연구에서는 국가안보 관련 기사에서 주제가 되는 키워드를 추출하기 위해 개체명 인식기를 사용하였다. 개체명 인식기는 텍스트 상에서 이미 등록된 인물, 지명, 사건 등을 추출하여 대량의 데이터에서 의미 있는 키워드를 추출하는 데 유용하여 정보 추출, 범주를 나누는데 사용되어 왔다. 본 연구에서는 창원대에서 개

발한 에스프레소 개체명 인식기(Espresso Named Entity Recognizer)를 사용하였다.[28] 사용한 개체명 인식기는 인물(Person), 이론(Field), 인공물(Artifacts works), 기관(Organization), 지역명칭(Location), 문화 용어(Civilization), 날짜(Data), 시간(Time), 숫자(Number), 사건(Event), 동물(Animal), 식물(Plant), 물질(Material), 용어(Term) 등으로 분류된다. 이 중 국가안보의 주요 행위자와 행위를 분석하기 위하여 인물, 기관, 지역명칭, 사건, 인공물을 선택하였다.

다음으로 각 개체가 문서 상에서의 관계를 보일 것으로 판단하고, 이러한 차이를 살펴보기 위해 동시 출현 네트워크를 구성해 분석하였다. 각 분류에서 상위 빈도 개체 50개 단어들 중 동일한 기사에 함께 출연한 동시 출현(co-occurrence) 빈도 행렬을 구성하였다. 특히 정제되지 않은 텍스트에서 동시 출현 빈도를 추출하기 위해 Python으로 코딩하여 계산하였다. 각 분류별 동시 출현 매트릭스는 NodeXL을 이용하여 시각화하였다.

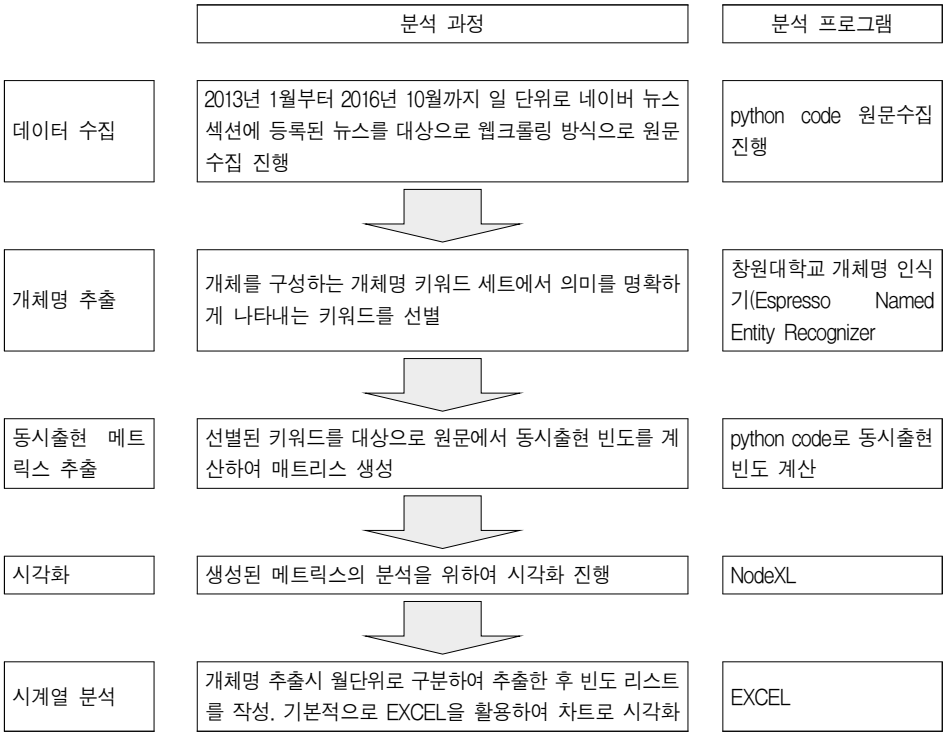
마지막으로 수집된 뉴스기사를 월 단위로 분리한 후 월별 개체명 빈도를 계산하여 개체의 분포가 시간의 흐름에 따라 어떻게 변화하는지 살펴보았다. 각 분류별 상위 50개 개체의 시기별 변화 양상을 파악하여 주요 이슈가 무엇인지 분석하였다.

즉 단계적으로 보면, 국가안보 관련 온라인 뉴스데이터를 수집한 후 기사 본문에서 주요한 의미를 가진 키워드를 추출한다. 추출된 키워드간의 맥락을 확인하기 위하여 매트릭스를 구성한 후 시각화하여 의미를 도출한다. 또한 단순 빈도나 전체 데이터에서의 맥락 외 월 단위로 주요 키워드의 변화를 살펴봄으로써 시간적 변화에 따른 양상들을 확인하여 이슈를 파악한다. 이러한 분석과정과 분석에 사용된 프로그램을 정리하면 다음과 같다.

---

28) 프로그램 사용은 ㈜ 더아이엠씨의 기술적인 지원을 받았음.

[표 2] 분석 과정 및 분석 프로그램



4. 분석 결과

가. 개체명 분석

2013년부터 2016년 10월까지 '국가안보'라는 주제어가 포함된 보도기사 내용에서 인물, 기관, 사건, 지역, 인공물의 범주로 상위 50위에 개체명별 주요 단어와 출현빈도의 추이를 정리해 비교한 내용은 [표 2]와 같다.

추출한 상위 출현빈도 주요단어를 간단히 비교하면 다음과 같다. 인물의 가장 상위 빈도수를 보인 단어는 '박근혜'로 35,433회의 출현빈도를 보였으며, 다음으로 '오바마(25,897회)', '김장수(8,628회)', '아베(7,518회)', '클린턴(5,875회)', '트럼프

(5,407회)', '김정은(5,396회)' 등과 같이 각 국가 수장들이 순차적으로 이어지고 있다. 특히 '오바마', '클린턴', '트럼트' 등 미국 대통령 및 당시 대통령 후보로 미국 정치 구도 변화에 대해 관심이 높은 것을 확인할 수 있다. 다음으로 '김관진(4,774회)', '장성택(4,558회)', '김기춘(3,692회)', '라이스(3,225회)', '김규현(3,062)' 등과 같이 국가안보의 주요 관료들이 다음으로 나타났다. 특히 '라이스'는 미 국가안보 보좌관 수잔 라이스(Susan Rice)로 한미 외교라인으로 인하여 언급이 높았다. 그 외 중국 주석 '시진핑(3,027회)', 러시아 대통령 '푸틴(2,636회)' 등 한반도 주변 국가 대표가 나타났으며, 국내 전임 대통령 '이명박(2,808회)', '노무현(2,674회)', '김대중(1,167회)'가 나타났으며, 국내 주요 정당의 정치인들이 나타났다. 특히 주목할 점은 가장 상위에 나타난 '박근혜', '오바마'의 언급 비율이 매우 높은 반면 3위 '아베'의 경우 1위와 약 4배 이상으로 차이가 난다는 점이다. 즉 한반도 국가 안보에 있어서 가장 중요한 행위자가 한미 관계라는 점을 확인 할 수 있다.

다음으로 기관의 빈도수를 살펴보면, '청와대'가 61,301회로 가장 높았으며, 다음으로 '국방부(16,253회)', '국가안보실(15,542회)', '국회(14,793회)', '백악관(12,297회)', 'NSC(10,989회)', '국가정보원(10,525회)' 등으로 국내 안보 기관과 미국 안보 관련 기관이 높게 나타났다. 특히 1위인 '청와대'가 2위 '국방부'에 비해 3.8배 높게 나타나 국가 안보와 관련하여 청와대가 주요 기관으로 나타났다. 그 다음으로 '통일부(10,518회)', 'IS(9,813회)', '민주당(9,531회)', '국가안전보장회의(8,027회)', '외교부(7,804회)', '유엔(6,478회)' 등의 순으로 나타났다. 특히 대북 이슈 관련 기관과 더불어 'IS'가 높게 나타나 국내 테러에 관심이 높아진 것을 확인할 수 있다. 그 외 국내 주요 행정부처가 다수 나타났다.

사건 관련 주요 단어 빈도수를 살펴보면, '지방선거'가 790건으로 가장 높게 나타났으며, 다음으로 '연평해전(673회)', '아시안게임(648회)', '군사훈련(486회)', '사드(THAAD: Terminal High Altitude Area Defense, 426회)', '잠수함발사탄도미사일(SLBM: Submarine-Launched Ballistic Missile, 341회)' 등의 순서로 나타났다. 즉 안보 관련 이슈가 2014년 6월 4일 지방선거에서 높게 나타났기 때문이며, '연평해전'의 경우 매년 추모식이 진행되고 있으며, 특히 연평해전 당시 전투 상황

이 영화로 나왔기 때문이다. 그 다음으로 '전당대회(319회)', '폐회식(289회)', '올림픽(287회)' 등이 나타났는데, 이는 리우 올림픽 당시 지카바이러스 우려로 인한 것으로 보인다.

[표 3] 개채별 주요 단어와 빈도수

순위	인물		기관		사건		지역		인공물	
	단어	빈도	단어	빈도	단어	빈도	단어	빈도	단어	빈도
1	박근혜	35,433	청와대	61,310	지방선거	790	북한	122,132	탄도미사일	745
2	오바마	25,897	국방부	16,253	연평해전	663	미국	82,465	통일대교	602
3	김장수	8,628	국가안보실	15,542	아시안게임	648	중국	47,939	여객기	563
4	아베	7,518	국회	14,793	군사훈련	486	서울	24,327	ICBM	359
5	클린턴	5,875	백악관	12,297	THAAD	426	남북	24,142	KAMD	303
6	트럼프	5,407	NSC	10,989	SLBM	341	일본	22,981	장거리미사일	297
7	김정은	5,396	국가정보원	10,525	전당대회	319	한국	21,722	항공기	294
8	김관진	4,774	통일부	10,518	폐회식	289	한반도	18,134	세종로	253
9	장성택	4,558	IS	9,813	올림픽	287	러시아	16,524	여객선	246
10	김기춘	3,692	민주당	9,531	대선	276	우크라이나	8,600	대량살상무기	244
11	라이스	3,225	국가안전보장회의	8,027	폐막식	273	시리아	7,377	화학무기	231
12	김규현	3,062	외교부	7,804	KADIZ	240	개성공단	7,063	쾌속정	206
13	시진핑	3,027	유엔	6,478	이산가족상봉	218	영국	6,084	북핵	205
14	남재준	2,936	새정치민주연합	6,180	기자간담회	214	판문점	5,917	무인항공기	199
15	이명박	2,808	새누리당	5,929	연합군사훈련	154	이란	5,282	백악관	179
16	노무현	2,674	공화당	5,254	공동기자회견	154	이라크	4,925	기관단총	168
17	푸틴	2,636	노동당	4,670	실무회담	144	프랑스	4,153	의원회관	167
18	윤병세	2,591	국무부	4,594	베트남전	137	동북아	3,798	SLBM	160
19	정홍원	2,313	안전보장이사회	4,338	공모전	135	독일	3,389	대통령궁	154
20	김무성	2,281	행정부	4,193	사격훈련	127	터키	3,161	국회의사당	148
21	리퍼트	2,173	인수위	3,933	세무조사	125	유럽	2,986	사격장	142
22	김정일	2,116	국방위원회	3,762	산업혁명	122	호주	2,880	경원선	134
23	류길재	2,043	NSA	3,119	MD	117	서해	2,857	경비정	134
24	안철수	1,974	FBI	3,089	국무회의	117	여의도	2,759	차기전투기	130
25	이병기	1,926	CIA	2,389	사망사건	115	베이징	2,650	자주포	121
26	헤이글	1,885	이슬람국가	2,075	재보선	109	남중국해	2,574	수류탄	106
27	안대희	1,849	북한군	1,811	이라크전	106	인도	2,462	크렘린궁	104
28	황교안	1,656	국무회의	1,806	DMZ	105	경기도	2,418	야스쿠니신사	103

29	유승민	1,556	국가안보국	1,795	한국전	100	연평도	2,285	정부서울청사	102
30	이정현	1,490	주한미군	1,669	사이버전쟁	97	이스라엘	2,154	목함지뢰	96
31	민경욱	1,408	미래창조과학부	1,512	행정고시	92	경북	1,965	광명성	96
32	김광진	1,392	유럽연합	1,509	월드컵	91	이집트	1,958	해안포	89
33	스노든	1,376	수석비서관회의	1,377	사법시험	90	쿠바	1,916	WMD	77
34	김병관	1,273	해양수산부	1,259	NLL	86	비무장지대	1,842	패트리엇	73
35	카터	1,194	정보위원회	1,219	열병식	78	중동	1,819	자동소총	66
36	김대중	1,167	최고위원회의	1,183	AIIB	76	필리핀	1,661	요격미사일	60
37	김일성	1,145	대통령비서실	1,178	시국미사	74	유럽연합	1,652	고등훈련기	55
38	원유철	1,144	한수원	1,100	국민투표	71	몰디브	1,622	항공모함	54
39	한기호	1,126	수니파	1,064	동계올림픽	68	태국	1,568	외교부청사	48
40	최경환	1,105	법무부	1,036	주민투표	68	홍콩	1,547	잠실실내체육관	48
41	부시	1,063	중앙정보국	1,017	항일전쟁	67	파리	1,477	현충사	47
42	허태열	1,041	기획재정부	971	백년전쟁	62	평양	1,416	경복궁	46
43	박정희	1,034	육사	967	베트남전쟁	58	파키스탄	1,296	정부세종청사	45
44	박흥렬	1,026	상임위원회	965	해킹방어대회	57	금강산	1,278	실내체육관	44
45	이석기	998	안전행정부	953	독수리연습	53	도쿄	1,223	워싱턴	44
46	이완구	985	워싱턴DC	900	국정감사	51	강원도	1,212	서울역	43
47	박지원	984	공산당	877	토론회	50	뉴욕	1,197	수소폭탄	42
48	김양건	979	사이버사령부	858	대남심리전	50	사우디	1,153	대륙간탄도미사일	38
49	김한길	955	합동참모본부	848	대피훈련	49	시드니	1,127	원자력발전소	37
50	정진석	951	방위사업청	826	취임식	49	말레이시아	1,097	전쟁기념관	37

지역 관련 주요 단어 빈도수를 살펴보면, '북한'이 122,132회로 가장 높았으며, 다음으로 '미국(82,465회)', '중국(47,939회)', '서울(24,327회)', '남북(24,142회)', '일본(22,981회)' 등으로 나타났다. 즉 국가안보와 관련해서 북한과의 관계가 가장 중요한 대상으로 보고 있으며, 다음으로 미국, 중국, 일본 등의 주변국과의 외교안보 관련된 이슈가 나타나고 있다. 그 외 '러시아(16,524회)', '우크라이나(16,524회)', '시리아(7,377회)', '개성공단(7,377회)', '영국(6,084회)' 등으로 나타났는데, 주로 우크라이나, 시리아 내전과 관련하여 러시아의 참전 등이 국제사회에서 중요한 이슈로 나타났기 때문에 이로 인한 국내안보에 미치는 영향, 향후 전망 등으로 해당 지역이 높게 나타났다.

마지막으로 인공물 관련 중 단어 빈도수를 보면, '탄도미사일'이 745회로 가장

높았으며, 다음으로 '통일대교(602회)', '여객기(563회)', '대륙간탄도미사일(ICBM: Intercontinental Ballistic Missile, 359회)', '한국형미사일방어체제(KAMD: Korea Air and Missile Defense, 303회)', '장거리미사일(297회)' 등 남북한 교류시 육로 공간인 '통일대교' 여객기 추락사고 등으로 인한 '여객기'를 제외하고 미사일 관련 키워드가 높게 나타나고 있다. 즉 북한이 지속적으로 탄도미사일 발사와 더불어 이에 대응한 방어체계에 대한 관심과 안보정책 수립에 따른 보도가 많아지면서 관련 단어가 높게 나타난 것이다. 그 외 '대량살상무기(244회)', '화학무기(231회)', '북핵(205회)', '무인항공기(199회)' 등 북한의 대량살상무기 확산에 따른 우려가 높아지면서 관련 키워드가 나타났다.

나. 네트워크 분석

주요 개체명 인식 분석에서 나타난 인물, 기관, 사건, 지역, 인공물의 범주로 상위 50위에 개체명별 주요 단어들이 전체 뉴스 기사에서 동시출현 빈도를 분석하여 네트워크로 시각화하면 아래의 <그림 1~5>과 같다.[29]

먼저 인물 상위 50개 키워드 간 네트워크(그림 1)를 보면, '김정은-장성택', '클린턴-트럼프'가 전체 인물네트워크에서 가장 높은 연결관계를 보였다. 즉 국내 언론에서 북한 내부 정권 변화 및 미 대선 결과에 따라 국내 안보 변화에 미치는 영향으로 커서 관심이 높다는 것을 확인된다. 박근혜 대통령과 높은 연결을 보인 인물을 보면, 남북한 대결구도에서 '김정은' 북한 노동당 위원장, 전임 대통령인 '이명박', 국가안보실장 '김관진', 미 대통령 '오바마' 순으로 나타났다. 반면 중국 '시진핑' 주석과 일본 '아베' 총리와 상대적으로 낮은 연결을 보이고 있다.

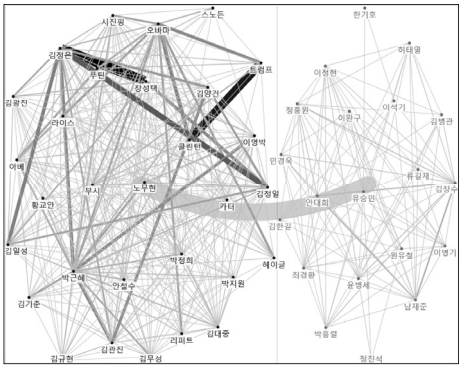
전체 네트워크를 클러스터링 한 결과 크게 두 개의 그룹으로 나눠지는데, 왼쪽 큰 그룹은 대북 안보와 관련된 인물들이 나타났고, 오른쪽 그룹은 주요 정당 인물들이 나타나고 있다. 국내 인물 그룹의 경우 '남재준' 국정원장과 김장수 전 국가

29) NodeXL 소프트웨어에는 다양한 클러스터 알고리즘이 있다. 그 중 대표적인 알고리즘인 Clauset- Newman-Moore 알고리즘을 사용하였다.

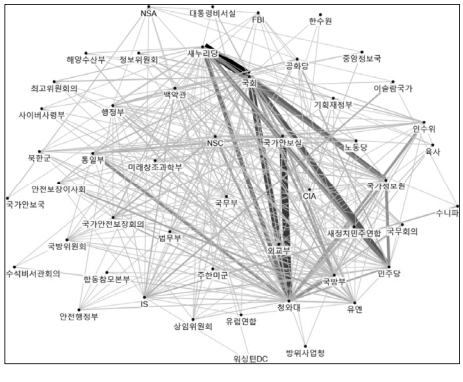
안보실장, ‘안대희’ 전 대법관이 상대적으로 높은 연결을 보이고 있는데, 이는 2014년 새 총리 후보에 ‘안대희’ 지명과 더불어 남재준 국정원장, 김장수 국가안보실장의 사표로 인한 것이다.[30]

다음으로 기관 상위 50개 키워드 간 네트워크[그림 2]를 보면, ‘새누리당-국회’, ‘청와대-국가안보실’, ‘청와대-국회’, ‘국가정보원-국회-청와대’ 등의 키워드가 강한 연결을 보였다. 즉 정부와 새누리당, 국가정보원에서 국가안보와 관련된 주요 메시지를 전달하는 것으로 나타났다. 다음으로 ‘청와대-통일부’ ‘청와대-인수위’ 등이 나타났으며, ‘민주당-국가정보원’도 나타났다. 즉 대북 이슈를 전담하는 통일부와 더불어 박근혜 대통령 인수위에서 ‘국가안보실’ 설치를 발표하면서 주요 기관으로 나타난 것이다.[31] 그 외 국내 주요 부처는 네트워크 외부에 나타나면서 상호 연결되는 정도가 낮게 나타났다.

[그림 1] 인물 네트워크



[그림 2] 기관 네트워크

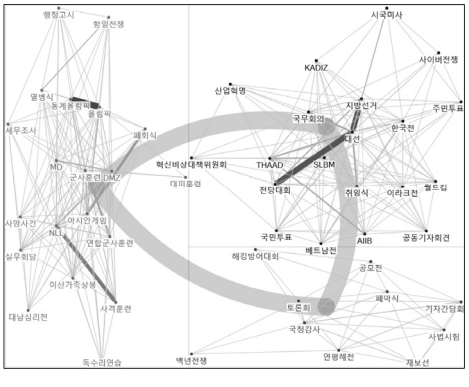


사건 네트워크[그림 3]를 보면, ‘지방선거-대선-전당대회’, ‘올림픽-동계올림픽’, ‘NLL-사격훈련’ 등의 사건 키워드가 높은 연결을 보였다. 즉 선거 시기 국가안보에 대한 언급이 높고, 리우올림픽이나 평창동계올림픽 등 국제 행사에서 안보의

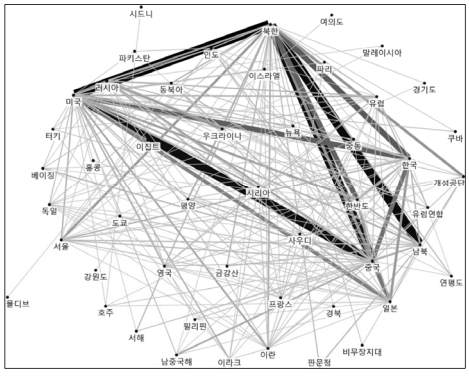
30) http://www.hani.co.kr/arti/politics/politics_general/638466.html(검색일: 2016년 11월 25일)
31) http://news.joins.com/article/10518067(검색일: 2016년 11월 25일)

중요성을 강조한 것이다. 그 외 서해 북방한계선(NLL)에서의 남북한 간의 대규모 사격훈련으로 인하여 높게 연결되어 나타났다. 전체 네트워크에서 그룹은 크게 3개로 구분되었는데, 왼쪽 그룹은 남북한 군사훈련 관련 사건 그룹이 나타났으며, 오른쪽 상단에는 국내 정치 갈등이 나타났으며, 오른쪽 하단에는 토론회, 공모전 등 시민 대상 안보 행사들이 나타났다. 특히 국내 정치 관련 이슈에서는 사드(THAAD)와 잠수함발사탄도미사일(SLBM), 아시아인프라투자은행(AIIB: Asian Infrastructure Investment Bank) 가입 등이 주요 이슈로 나타났는데, 사드(THAAD)와 잠수함발사탄도미사일(SLBM)은 북한의 탄도미사일과 관련된 이슈이지만 아시아인프라투자은행(AIIB)의 경우 중국 주도의 아시아 경제 협력의 영역으로 포괄적 안보의 경제 영역에 포함된다. 특히 'AIIB'와 'THAAD'가 강하게 연결되어 나타나 중국과의 경제협력과 더불어 미국과의 미사일방어 협력이 갈등되는 상황을 보여주고 있다.

[그림 3] 사건 네트워크



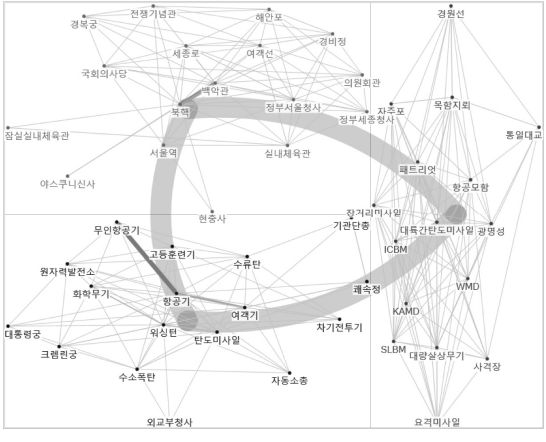
[그림 4] 지역 네트워크



다음으로 지역 네트워크(그림 4)를 보면, '미국-중국-북한'의 네트워크가 가장 강하게 나타났으며, 다음으로 '한국-미국-북한-일본'의 네트워크가 나타났다. 즉 국내 국가안보 이슈가 미국, 중국, 북한 3개국의 이슈를 중심으로 움직이고 있다. 그 외 '유럽연합', '유럽'의 국가들과는 상대적으로 약한 연결을 보이고 있다. 특히

남북한 간의 주요 공간인 '개성공단'이나 '비무장지대' 등은 네트워크에서 외부에 나타나며 낮은 연결을 보였다. 즉 국가안보는 북한을 둘러싼 미국, 중국, 일본 등의 국가가 주요 행위자로 지속적으로 나타나고 있으며 특히 북핵 실험이나 탄도미사일로 인하여 긴장감이 높아졌기 때문에 주변국이 높게 나타난 것이다.

[그림 5] 인공물 네트워크



마지막으로 인간이 만든 인공물에 대한 네트워크[그림 5]를 보면, '북핵-백악관', '항공기-무인항공기-여객기' 가 높은 연결을 보였다. 북한의 핵실험에 관련하여 미국의 반응에 대한 보도가 높은 것으로 나타났으며, 과학기술의 발전으로 무인항공기(드론)의 전장에서 활용이나 여객기와의 충돌위험 등이 보도되면서 무인항공기의 위험에 대해 언급되고 있다.

인공물 전체네트워크를 그룹으로 나눠본 결과 크게 3개의 그룹으로 나눠졌는데, 왼쪽 상단에는 북핵 관련하여 이슈가 나타났으며, 대북 제제 및 압박을 위한 한미 회동 등의 장소 및 북핵 관련 반대 시위[32]로 인하여 관련 장소가 함께 나타나고 있다. 왼쪽 하단에는 무인항공기를 활용한 공격에 대한 이슈가 나타나고 있

32) http://www.chogabje.com/board/view.asp?C_IDX=67722&C_CC=AZ(검색일: 2016년 3월 25일)

다. 오른쪽 그룹의 경우 북한 미사일 관련된 키워드가 다양하게 나타나는데, ‘광명성’, ‘목함지뢰’, ‘자주포’ 등 현재 북한에서 개발 혹은 사용된 무기에 대하여 나타나고 있으며, ‘패트리엇’, ‘요격미사일’ 등 북한 미사일 대응 전략에 대한 키워드로 함께 나타나고 있다. 즉 북한 미사일 공격에 대응하기 위해 군사안보에 대한 내용이 나타나고 있는 것이다. 따라서 인공물의 경우 대부분 대북 안보와 관련된 무기나 정책이 주를 이루고 있으며, 인간안보, 환경안보, 사이버 안보 등의 포괄적 안보 분야에 대한 부분은 낮은 것으로 나타났다.

다. 시계열 분석

언론은 주요 이슈가 발생할 경우 관련 이슈에 대해 수많은 언론사에서 보도를 하게 된다. 따라서 특정 기간에 빈도가 높아지게 된다. 이러한 문제의식을 바탕으로 앞서 상위 50개의 개체명의 시간의 흐름에 따른 개체 분포의 변화 추이를 비교하였다. 다만 50개 키워드의 월별 빈도를 차트로 나타낼 경우 가독성이 떨어지기 때문에 상위 20개의 키워드에 대하여 분석하였다.

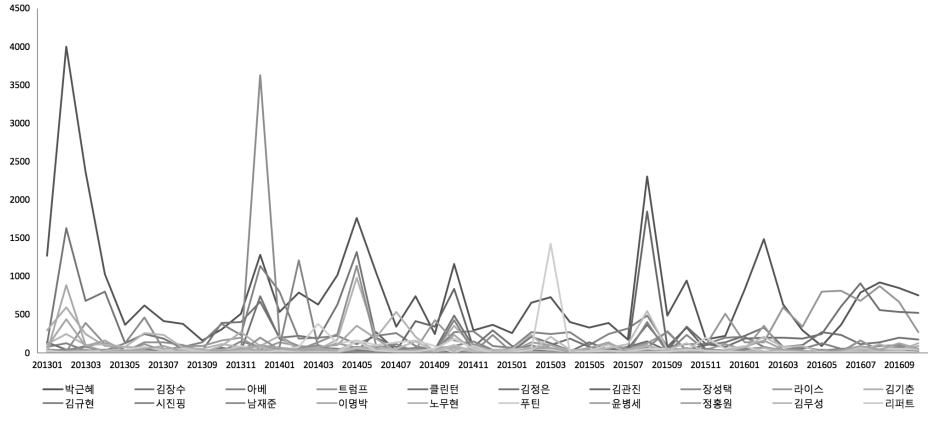
[그림 6]은 인물 개체명의 시기별 분포를 나타낸 것이다. 2013년 2월에 박근혜 당선인의 인수위에서 ‘국가안보실 신설’ 및 국가안보 정책에 대해 발표함에 따라 추세선이 최고점을 위치하였다. 다음으로 2015년 8월에는 ‘남북고위급 정상회담’을 통해 남북한 충돌 위기를 해소한 보도가 나오면서 높은 빈도를 보였다. 2014년 5월에는 세월호 참사로 인한 재난 위기관리에 대한 우려 및 북한의 서해 NLL 인근 해상사격훈련으로 인하여 안보에 대한 관심이 높아지면서 다시 상승하였다. 그 외 2016년 2월에는 박근혜 정부의 개성공단 폐쇄 및 국가안보를 초점에 둔 대통령 연설로 인하여 상승하였다. 특히 박근혜 대통령이 국회연설을 통해 “북한의 다양한 테러에 철저히 대비해야”한다는 발언과 더불어 북한의 4차 핵실험과 장거리 미사일 발사 및 사이버 테러 등의 대비를 강조한 것이 언론에 다수 노출되었기 때문이다.

관련하여 2013년 12월의 경우 ‘장성택’이 높게 증가한 것은 장성택 처형이 공식

확인되면서 대북 상황에 관심이 높아진 것이다. 관련하여 '김정은'과 '아베'가 함께 증가하였는데, 한국 외 일본에서도 북한 움직임을 주시했기 때문이다. 2015년 3월에 '리퍼트'가 크게 증가한 것은 당시 리퍼트 미 대사의 피습사건으로 인하여 한미동맹에 대한 우려 보도가 높게 나타나면서 증가한 것이다. 그 외 2016년 5월부터 미 대선 후보인 '트럼프'에 대한 관심이 증가하면서 미 대선 결과가 한반도 안보에 미치는 영향에 대한 논의가 나타나면서 빈도가 증가하였으나 미 언론에서 클린턴의 승리 예측으로 인하여 '트럼프'에 대한 빈도는 감소하는 추세를 보였다.

즉 상위 인물은 북한 인물 외 미국 주요 인물의 행보에 대하여 언론이 관심이 높게 나타났다. 미 대사 피습사건의 경우 사건 경위와 더불어 여러 정치적 요인에 대한 해석까지 보도하면서 국내 정치 세력에 대한 논란으로 확대되는 등 안보영역에 미국이 차지하는 부분이 매우 큰 것을 확인할 수 있다.

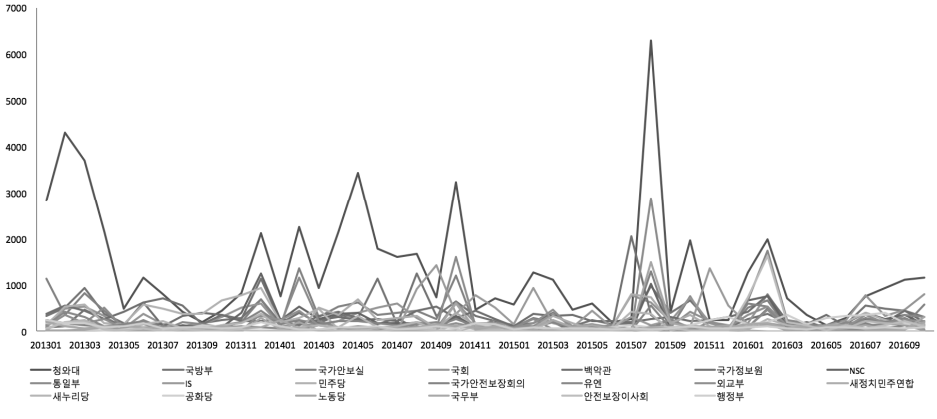
[그림 6] 인물 개체명 월별 빈도 변화(상위 20개)



[그림 7]은 기관 개체명의 시기별 분포를 나타낸 것으로 최고점은 2015년 8월에 '청와대'이다. 이때 남북협상 고위급 협상 결과에 따라 가장 높게 나타났는데, 이 기간에 '통일부', 'NSC', '노동당', '새정치연합' 등 정부 부처와 정당 등에서도 남북한 군사 위기를 해소한 것에 대하여 긍정적인 평가로 인해 상승하였다. 다음으로

2013년 2월에 청와대의 국가안보실 및 국가안보 정책 발표로 인해 기관으로 높게 나타났다. 이어 3월에는 관련 기관인 국가안보실, 국방부 등이 함께 소폭 상승하였다. 2014년 5월의 경우 국가정보원장과 국가안보실장 인선으로 인한 진통으로 관련 기관이 증가하였고, 2014년 10월의 경우 국정감사 기간으로 대북전단 살포, 세월호 사태 등의 이슈로 인해 국가안보 영역에 대한 질의응답으로 '청와대'와 더불어 '통일부', '국가안보실'의 빈도가 높아졌다. 2016년 2월의 경우 북한 4차 핵실험 이후 대북 제재안 논의로 인하여 '청와대', '안전보장이사회', '외교부' 등 외교 담당 기관이 함께 증가하였다. 즉 기관의 증가는 북한 관련 이슈로 대북제재나 북한 핵실험에 따른 대응으로 인하여 시기별 변화가 나타난 것임을 알 수 있다. 즉 북한의 3차 핵실험 시기인 2013년 2월 12일, 4차 핵실험인 2016년 1월 6일, 5차 핵실험인 2016년 9월 9일 등 각 기간별로 청와대의 빈도가 높게 나타나고 있어 해당 기간 동안 북한의 핵실험에 대한 정부의 비판으로 빈도가 증가한 것이다.

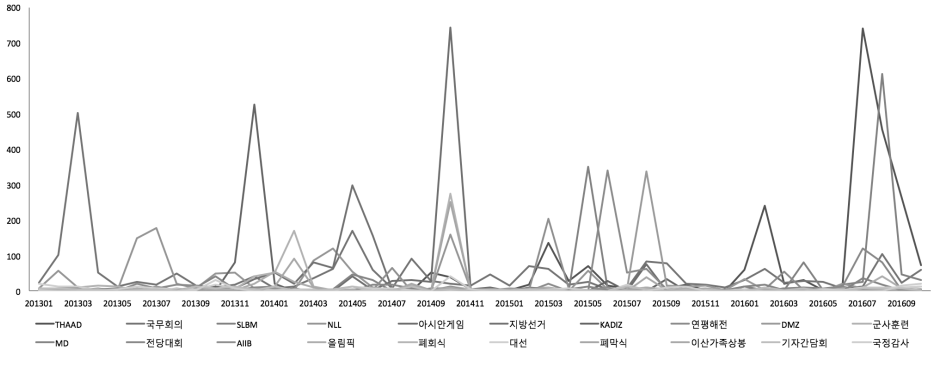
[그림 7] 기관 개체명 월별 변화 빈도(상위 20개)



사건 개체명의 시기별 분포는 아래 [그림 8]과 같다. 특히 2016년 7월은 'THAAD'가, 8월은 'SLBM'으로 인해 빈도수가 높게 나타났다. THAAD의 경우 성주 배치로 인해 사드배치 반대 집회와 지지 집회 등 갈등이 발생하면서 논란이

진행 중이다. SLBM의 경우에는 북한의 SLBM 발사로 인해 국내외의 대북 제재 관련 이슈가 높게 나타나면서 빈도가 높게 나타났다. SLBM 문제는 2015년 5월에도 다른 사건에 비해 높게 나타났음에도 불구하고 실제 지속적인 논의는 되지 않았다. 그 외 2014년 10월 '아시아게임'이 높게 나타났는데, 당시 폐막식에 북한 대표단과 면담을 하면서 높게 나타났다. 2015년 8월의 경우 'DMZ'가 높아진 것은 목함지뢰 도발이나 포격 등의 한반도 긴장으로 인해 비무장지대에 대한 관심이 높아지면서 관련 키워드가 높게 나타난 것이다. 즉 주요 사건을 보면 북한의 무력시위 및 도발로 인한 군사안보 영역이 높게 나타났고 대북 제재를 위한 안보정책이 강화되는 추세를 보였다.

[그림 8] 사건 개체 월별 빈도 변화(상위 20개)

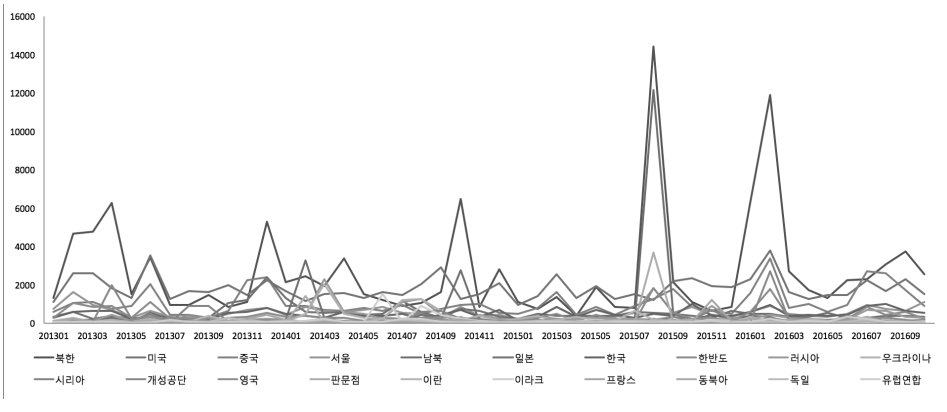


[그림 9]는 지역 개체명의 시기별 분포를 나타낸 것이다. 지역에 있어 추세선이 최고점을 보인 것은 2015년 8월 '북한'이고, 다음으로 2016년 2월에 역시 '북한'이 높게 나타났다. 2015년 8월의 경우 남북고위급 회담으로 북한 측 반응에 관심이 높아 지역 빈도가 높게 나타났으며, 따라서 '남북' 역시 함께 증가한 것을 볼 수 있다. 반면 2016년 2월의 경우 '북한'에 대한 대북제재로 인하여 '중국', '미국' 등 관련 국가와 더불어 '개성공단'이 높게 나타났다. 이는 정부의 제재 일환으로 개성공단 중단으로 인한 것이며, 관련하여 국내에서 찬반의 논쟁으로 인하여 높게 나

타난 것이다.

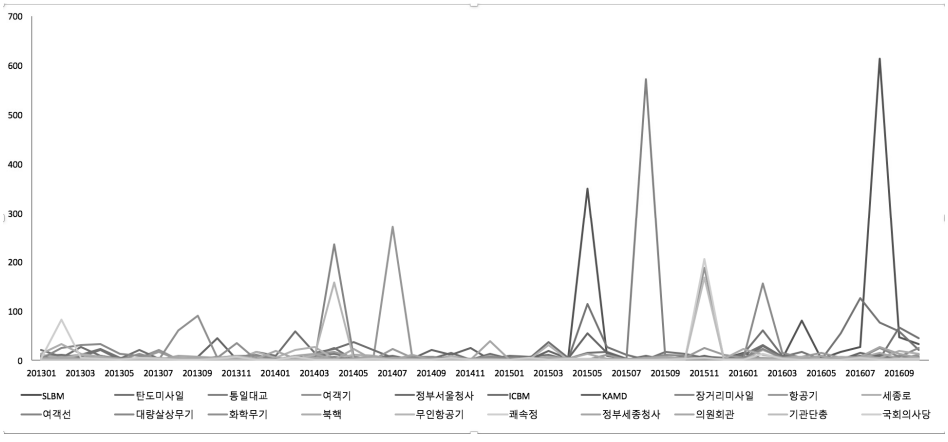
또한 시기별 변화에서 ‘북한’의 빈도 변화와 더불어 한반도 주변국인 ‘일본’, ‘중국’, ‘미국’ 등의 지역이 함께 변화하고 있어 북한의 활동에 주변국이 민감하게 반응하고 있음을 확인할 수 있다.

[그림 9] 지역 개체명 월별 빈도 변화(상위 20개)



[그림 10]은 인공물의 시기별 변화이다. 가장 높은 빈도를 보인 기간은 2016년 8월로 북한의 SLBM 발사 실험으로 인한 국내외 반응이 높았기 때문이며, 이는 2015년 5월 역시 같은 이유로 그 달에 높은 빈도를 보였다. 그 외 2015년 8월에는 남북 정상회담을 위해 육로 이동로인 파주 ‘통일대교’가 높았다. 그러나 2015년 11월에 다시 ‘쾌속정’, ‘기관단총’ 등 남북간 무력시위로 인하여 긴장이 높아지게 되어 해당 키워드가 높게 나타났다. 즉 인공물의 변화에서는 주로 군사안보의 긴장감을 높이는 무기에 대한 빈도 변화가 많았으며, 특히 미사일 관련 이슈가 최근 들어 더욱 높아지는 양상을 보였다.

[그림 10] 인공물 개체명 월별 빈도 변화(상위 20개)



5. 결론

본 연구는 국가안보에 대해 개체명 인식 방법을 활용하여 인물, 사건, 지역, 지역, 인공물 등을 추출하고 개체들의 어떻게 구성되어 있고, 이슈의 변화가 어떻게 되었는지 분석하였다. 이를 위해 2013년부터 2016년 10월까지 국가안보 관련 온라인 뉴스를 수집하고 개체를 추출한 후 여기에 포함된 개체의 공동출현빈도를 기준으로 매트릭스 데이터를 생성하였다. 이렇게 생성된 매트릭스 데이터를 네트워크 분석 프로그램을 이용해 시각화하고 각 단어들이 어떤 연관성을 가지고 있으며 그것이 의미하는 바가 무엇인지 도출하였다. 그리고 상위 개체에 대하여 시계열로 살펴보았다.

연구결과, 한국의 국가안보와 관련하여 한미일 동맹구조가 지속적으로 강조되고 있었으며, 대북 제재 정책이 주요 정책임을 확인할 수 있었다. 또한 국가안보의 다양한 영역 변화 중에서 여전히 전통적인 군사 안보 영역에 초점이 맞춰진 것을 확인할 수 있었다.

먼저 각 개체별 주요 단어 빈도를 보면, 인물의 경우 대통령을 중심으로 미 대

통령 및 후보에 대한 언급이 높아 미국 정치구도에 높은 관심을 확인할 수 있었다. 반면 대북 정책과 관련해서는 김정은 국방위원장 외 김정일, 김일성 등 현재 북한 대표 인물보다는 이전 인물에 대해 언급이 높아 북한 내부의 권력 구조에 대한 정보가 부족한 것으로 보인다.

다음으로 기관의 경우에는 청와대를 중심으로 국방부와 박근혜 정부에 신설된 '국가안보실'이 중요한 컨트롤 타워로 나타나고 있다. 사건이 경우 지방선거나 대선 등 국내 선거에서 안보이슈가 여전히 주요한 이슈인 것을 확인되었다. 그 외 사드(THAAD)나 잠수함발사탄도미사일(SLBM) 등 미사일 관련 전략이 주요한 이슈였다. 지역은 북한이 가장 높았으며, 다음으로 미국과 중국, 일본 등의 순으로 나타나 기존 북한 관련 이해관계자가 여전히 주요한 행위자로 나타났다. 반면 유럽 지역의 국가는 상대적으로 낮았다. 마지막으로 인공물은 탄도미사일이나 장거리미사인, 북핵 등 북한의 미사일 실험 등 무기 관련 키워드가 높게 나타났다. 즉 개체의 빈도 분석 결과 북한의 미사일 실험에 따른 주변국의 군사안보 대응이 주요한 이슈로 확인되었다.

개체명 빈도에서 상위 50개를 주요단어로 선정하고 해당 단어가 전체 국가안보 기사에서 어떤 구조적 특성과 의미를 가지고 있는지 알아보기 위해 의미연결망 분석을 실시하였다. 단어들의 연결을 확인하기 위하여 네트워크를 시각화해 분석하였다.

인물 네트워크의 경우 한반도 주변국인 중국 주석과 일본 총리는 빈도에서는 높게 나타났으나 박근혜 대통령의 연결은 낮게 나타났다. 반면 오바마 대통령과의 연결은 강하게 나타나고 있어, 국가안보에 있어 한미동맹에 초점이 맞춰진 것이 확인되었다. 그 외 정부의 안보 핵심 인사와 정당 주요 인물과는 그룹이 분리되는 양상을 보여, 정부와 정당 간의 유기적인 결합이 다소 낮은 것을 확인 할 수 있었다.

사건 네트워크의 경우 국내 선거에서의 '북풍'와 북한의 무력시위 두 개의 큰 이슈를 확인 할 수 있었다. 실제 북한의 무력시위를 국내 정치에 활용하는 사례는 지속적으로 일어났으나, 최근 들어 북한의 계속되는 핵실험이나 미사일 발사 실

험 등은 안보위기를 가져와 선거 국면에서도 안보가 더욱 더 강조 된 것이라 할 수 있다. 특히 중요한 점은 중국 주도의 AIIB와 THAAD의 강한 연결은 한반도 사드배치에 대해 중국이 민감하게 받아들인다는 점을 보여준다. 그러나 앞서 인물에서는 주로 박근혜 대통령과 오바마 대통령과의 강한 연결에 비해 시진핑 주석과는 약한 연결을 보고 있었어, 한국정부가 미국과의 동맹만 강조되고 중국과의 관계는 낮게 나타나고 있어 중국과의 관계 개선이 필요한 것으로 나타났다. 그 외 인공물의 네트워크의 경우 주로 북한의 미사일이나 무기 등이 네트워크에서 주요한 단어로 나타났다.

이러한 의미연결망의 내용과 유사하게 시계열 분석에서도 북한의 무력시위에 대한 주변국의 제재 조치 및 논의가 패턴으로 나타나고 있다. 기관 시계열 결과에 보듯 박근혜 정부 초기에 신설된 국가안보실이 사건 시계열에서 북한 핵실험이나 미사일 발사 실험의 변화 추이와 유사하게 나타나면서 국가안보의 컨트롤 타워로 역할을 하고 있으며, 특히 최근 SLBM의 실험에 대해 더욱 대북 제재를 위한 활동을 강화하고 있는 추세이다. 그 외 인공물에서는 미사일 위협 이외 목함지뢰나 서해안 NLL에서의 기관단총 시위 등 기존 무력을 사용한 시위가 나타나는 양상을 보여 전통적인 군사안보 영역에 대한 위협이 지속적으로 일어나고 있음을 확인할 수 있었다.

그러나 주의해서 볼 점은 아시아게임 시기의 남북한 고위급 회담이나 2015년 목함지뢰 사건 이후 위기 상황에서의 대화를 통한 위기를 해소하는 등에 대하여 높은 빈도를 보이는 것은 남북한 간의 대화 채널의 중요성을 보여주는 것이라 할 수 있다. 따라서 군사안보 측면에서 대북제재와 더불어 지속적인 대화 채널을 통한 갈등 해소가 필요하다. 또한 현재 안보의 축이 미국 중심으로 나타나고 있는 것은 미국 안보 정책 변화에 민감하게 변화할 수밖에 없어 지속적인 남북한 갈등 해소를 위한 정책 운영에 어려움을 가져올 수 있다. 따라서 한반도 주변국인 일본, 중국 등과의 다각화된 방향을 모색하여 남북한 간의 갈등상황에서 주변국의 협력을 이끌어 낼 수 있는 관계를 구축할 필요가 있다. 그 외 기관과의 연결에서 한국기관과 거의 나타나고 있지 않은 유럽연합 등과도 안보 정책 교류를 통해 한반도

의 평화를 구축을 위한 협력자로 둘 필요가 있다.

본 연구는 국가안보 분야에서 뉴스 데이터의 텍스트 데이터를 네트워크 분석을 통해 이슈를 도출한 것에 의미를 둔다. 또한 개체명 인식이라는 새로운 방법을 적용한 것 역시 의미가 있을 것이다. 그럼에도 불구하고, 본 연구는 몇 가지 제한점을 가지고 있다. 먼저 분석 대상의 한정적인 선택으로 다양한 관점이 제한된다는 점이다. 따라서 기간을 확대하여 시기별로 구분해서 분석이 필요할 것으로 판단된다. 다음으로 연구자의 주관성 개입의 문제이다. 주요 단어를 선택하는 단계에서 연구자의 주관성이 일부분 적용될 수 있다. 따라서 이러한 오류를 방지할 수 있는 노력이 필요하다. 마지막으로 개체명 인식기의 정확성 문제이다. 즉 신조어나 사전에 등재되지 않은 단어의 경우 분류의 한계가 있다. 이는 지속적인 개발을 통해 오류를 줄여나가는 작업이 필요할 것이다.

참고문헌

국가안전보장회의. 『평화번영과 국가안보』. 서울: 국가안전보장회의 사무처, 2004.

권호천. “메르스 사태에 대한 신문보도의 의미연결망 분석.” 『의료커뮤니케이션』, 제11권, 제1호(2016), pp.65-82.

김만재・전방욱. “언어네트워크 분석 기법을 활용한 인간배아복제 신문보도 분석.” 『한국 생명윤리학회』, 제13권, 제2호(2012), pp.19-34.

김영호. “비전통적 안보위협과 군의 역할.” 『평화연구』, 제17권, 제2호(2009), pp.157-187.

남인용・박한우. “대권 예비후보자 관련 신문기사의 네트워크 분석과 홍보전략.” 『한국정당학회보』, 제6권, 1호(2007), pp.79-107.

대한민국 국방부. 『2016 국방백서』. 서울: 국방부, 2016.

박성희. “제17대 대통령 후보 합동 토론 언어네트워크 분석: 북한 관련 이슈를 중심으로.” 『한국언론정보학보』, 통권 45호(2009), pp.220-254.

박영민・김예진・강상우・서정연. “개체명 인식 코퍼스 생성을 위한 지식베이스 활용 기법.” 『인지과학』, 제27권, 제1호(2016), pp.27-41.

박한우・Leydesdorff. “한국어의 내용분석을 위한 KrKwic 프로그램의 이해와 적용.” 『Journal of the Korean data analysis society』, 제6권, 5호(2004), pp.1377-1388.

배경만・김성현・고영중・김종훈. “자연어 기반 인터페이스에서 개체명 패턴을 이용한 효과적인 개체명과 주제어 인식 방법,” 『한국정보기술학회논문지』, 제12권, 제1호(2014), pp.121-129.

윤이숙. “환경적 쟁점과 한국의 안보,” 『국방연구』, 제52권 제1호(2009), pp.75-96. 전 웅, “21세기와 한국의 안보: 국제환경변화에 따른 한국의 안보 위협들.” 『국방연구』, 제48권, 제2호(2005), pp.3-36.

이경희・이주호・최명석・김길창. “한국어 문서에서 개체명 인식에 관한 연구.” 『한국정보과학회 언어공학연구회 학술발표 논문집』(2000), pp.292-299.

이미나・홍주현. “메르스 확산에 따른 정부의 위기 대응 메시지 언어 네트워크 분석.” 『한국콘텐츠학회논문지』 제16권 제5호(2016), pp124-136.

이수상. 『네트워크 분석 방법론(부산대학교 사회과학연구원 연구총서 2)』. 서울: 논형, 2013.

이수형・전재성. “국제안보 패러다임의 변화와 동북아 안보체제.” 『국방연구』, 제48권 제2호(2005), pp.71-100.

이재은. “포괄적 안보 개념하에서의 국가 위기관리 법제화의 의의와 내용 분석.” 『한국위기관리논집』, 제2권 제2호(2006), pp.19-35.

_____. “국가안보 환경의 변화와 국가위기관리 - 포괄적 안보 개념 하에서의 국가위기 유형.” 『한국위기관리논집』, 제9권 제2호(2013), pp.177-198.

외교부. 『2016 외교백서』, 서울: 외교부, 2016.

장하용. “언론보도와 비평의 구조: 신문보도의 비평에 대한 네트워크 분석.” 『한국언론정보학보』, 제16호(2001), pp108-135.

차민경・권상희. “언론의 ‘창조경제’에 대한 의제설정 의미연결망 분석.” 『한국언론학보』, 제59권, 제2호(2015), pp88-120.

최수진. “한류에 대한 미・중 언론보도 프레임 및 정서적 톤 분석.” 『한국언론학보』, 제58권 제2호(2014), pp.505-577.

최윤수・차정원. “Word Embedding 자질을 이용한 한국어 개체명 인식 및 분류.” 『정보과학회논문지』, 제43권, 제6호(2016), pp678-685.

최윤정・권상희. “ ‘빅데이터’ 관련 신문기사의 의미연결망 분석.” 『사이버커뮤니케이션학보』, 제31권, 제1호(2014), pp.241-284.

Wasserman, S., & Faust, K. *Social Network Analysis: Methods and applications*, Cambridge: Cambridge University Press, 1994.

http://www.hani.co.kr/arti/politics/politics_general/638466.html(검색일: 2016. 11. 25)

http://news.joins.com/article/10518067(검색일: 2016. 11. 25)
http://www.chogabje.com/board/view.asp?C_IDX=67722&C_CC=AZ(검색일: 2016. 3. 25)
https://ko.wikipedia.org/wiki/%EB%B9%85_%EB%8D%B0%EC%9D%B4%ED%84%B0 (검색일: 2016. 11. 24)

Abstract

Analysis of national security issues change based on online news

YoungWhan Lee (Konkuk University)

Chanwoo Kim (Yeungnam University)

In this study, we extracted key stakeholders and behaviors using the object recognition technique for newspaper articles on national security and conducted network analysis. First, we extracted named entity from newspaper articles containing national security from 2013 to October 2016, and then examined the difference in named entity by period. We analyzed the structure and contents of major issues through network analysis by named entity. Finally, we examined the difference in the distribution of named entity over time by time series analysis. As a result, domestic security issues are focused on traditional military security, and it has been confirmed that the Korea and US alliance is to be strengthened to secure security. Through this, it was confirmed that network analysis based on named entity recognition technique is useful for national security issue analysis.

Key Words: National Security, Network Analysis, Named Entity Recognition, Text Mining

투고일 : 2016.11.5. 심사일 : 2016.11.20. 게재확정일 : 2016.12.10.

VI

글로벌 기후변화 대응을 위한 차세대 지구관측위성 탑재체 획득 방안

은종원 (남서울대학교)

Summary

우주 산업은 21세기 가장 경쟁력 있는 산업으로 부각되는 미래의 핵심 산업이다. 하지만 우주 산업은 인프라 구축에 초기 투자비용이 막대하여 단기에 투자비용을 회수하기 어려워 민간 기업이 단독으로 우주 사업을 수행하는 것은 한계가 있다. 위성핵심기술은 동보성, 광역성, 고 정밀성, 항 재난성 등을 고려하여 다양한 정보를 제공할 수 있는 방향으로 개발되고 있다. 또한 우주기술은 정보통신, 측위, 영상 등의 기술과 융합되어 진화되고 있다. 우주기술 기반 지구관측 정보서비스는 우주개발 분야와 연계되는 특성이 있어 세계 주요국은 우주개발프로그램을 통해 차세대 지구관측 위성기술을 확보하고 있다. 이러한 위성기술 동향 및 변화에 따라 우리정부는 차세대 지구관측위성의 국내 자립개발에 대한 필요성을 인정하고 제반 세부추진계획 등의 기반사항을 마련하고 있다. 본 논문은 차세대 지구관측위성 탑재체가 국내 자립기술로 개발되어 글로벌 기후 변화에 대한 정확한 정보를 제공하여 국민의 행복 지수, 복지 및 안전 등에 크게 기여할 수 있는 차세대 지구관측위성 탑재체 획득 방안을 제시하는데 있다.

| **키워드** | 차세대 지구관측위성 탑재체, 미래 핵심기술, 국내 자립기술, 글로벌 기후변화

1. 서론

자연재해는 인간에 대한 재해 가운데 자연의 예상치 못한 변동이 원인이 되어 인간에게 피해가 발생하는 재해로 천재라는 의미를 가진다. 천재는 태풍, 가뭄, 홍수, 지진, 쓰나미, 화산폭발, 황사, 산불, 한파 등 대부분 기상재해로부터 나온다. 2011년 7월 말 서울 지역의 100년 만의 집중호우는 서초구 우면산 산사태로 16명이 숨지는 참사를 불러오기도 했다. 뿐만 아니라, 얼마 전에는 동남아 이상고온으로 인한 태국의 대홍수는 국토의 3분의 1을 물바다로 만들었고, 전 세계 40%의 하드디스크드라이브 [HDD; Hard Disc Drive]를 생산하는 HDD 업체의 생산 공장을 파괴했다. 자연재해로부터 인명 및 경제·사회적 피해를 최소화하기 위해 미국, 유럽, 러시아 그리고 중국은 저궤도 지구관측위성에 적외선 및 마이크로파 대역 탑재체 센서를 탑재, 기상재해 인자를 관측하여 날씨예보에 필수적인 수치예보 모델의 주요입력 자료를 제공하고 있다.

국외 저궤도 지구관측위성 개발 현황을 살펴보면, 미국은 NOAA-19 위성에 적외선 영상기(AVHRR-3; Advanced Very High Resolution Radiometer)와 적외선 탐측기(HIR-3; High Resolution Infrared Radiation Sounder), 수동형 마이크로파 탐측기(AMSU-A1/A2/B; Advanced Microwave Sounding Unit)를, 유럽은 METOP-A 위성에 수동형 마이크로파 탐측기(MHS; Microwave Humidity Sounder)와 적외선 탐측기(IASI; Infrared Atmospheric Sounding Interferometer)를, 러시아는 METEOR-3M 위성에 적외선 영상기(Klimaat; environment monitoring instrument)와 수동형 마이크로파 영상기/탐측기(MTVZA; Meteorological Instrument)를 탑재하여 기상관측을 수행하고 있다. 마지막으로 중국은 FY-3B위성에는 수동형 마이크로파 영상기(MWRI; Microwave Radiation Imager)와 적외선 탐측기(IRAS; Infrared Atmospheric Sounder), 그리고 수동형 마이크로파 탐측기(MWHS; Microwave Humidity Sounder)를 탑재하여 운용하고 있다.

우주 선진국들이 적외선 및 마이크로파 대역 탑재체를 운용하는 저의는 가시광

선 대역을 이용하는 광학 센서는 야간이나 구름 등이 끼어 있을 때 목표지역 촬영이 어렵지만 적외선 및 마이크로파 대역 탑재체 센서는 야간이나 악천후에도 관측이 가능하기 때문이다. 또한, 마이크로파 대역 탑재체 원천 기술은 진일보된 군사첩보위성 개발에 활용이 가능하다.

그러나 우리나라는 저궤도 지구관측위성의 탑재체로 사용 가능한 적외선 영상기 및 탑측기, 마이크로파 영상기 및 탑측기 등의 국내 기술은 국외 기술에 비하여 그 수준이 미약하다. 지난 2009년 8월과 2009년 6월 2차례에 걸쳐 나로호에 의해 발사되었던 과학기술 2호 위성의 탑재체인 마이크로파 영상기는 Ka 대역의 두 개 채널 (23.8, 37 GHz)과 수십에서 수백 Km의 해상도의 성능을 가지고 있다. 이러한 마이크로파 영상기 기술은 수 Km의 해상도와 다양한 채널을 가지는 국외 탑재체 기술과는 많은 차이가 있다. 따라서 다양한 사용자 요구사항이 반영된 고해상도 저궤도 지구관측위성의 탑재체가 안정적으로 운용될 수 있도록 초기에는 외국과 협력개발을 통해 관련 기술을 습득한 후 국내에서 자립개발이 이루어 질 수 있도록 탑재체 국산화 개발 로드맵을 수립하는 것은 매우 중요하다.

저궤도 지구관측위성은 정지궤도 보다 낮은 고도에서 다양한 센서를 활용 할 수 있으며 전 지구를 관측 할 수 있는 장점이 있다. 이러한 저궤도 지구관측위성은 기상예보의 중요 입력 및 참고자료를 제공하고 수증기, 해빙, 토양수분, 해수면 온도, 대기온도, 수문순환 등 다양한 인자의 기후적 변동과 이들과 연관된 기후변화의 이해에 결정적인 자료를 제공 할 수 있어 그 활용성이 증대되고 있다.

국민의 삶에 지대한 영향을 미치는 집중호우, 홍수, 가뭄 등 자연재해 예방 및 기후변화 분야의 역량을 강화하기 위해서는 정지궤도위성 이외에 지구관측위성인 다목적 위성 또는 차세대 소형위성 등 다양한 저궤도 지구관측 위성 탑재체를 우리나라 자력의 힘으로 독자 개발하여 이용할 필요가 있다. 자연재해는 인간의 생활과 생명을 위협하는 현상으로써 전 세계적으로는 연평균 약 15만 명 이상 자연재해로 생명을 잃고 있다. 이러한 자연재해에는 태풍, 집중호우로 인한 홍수 및 범람, 폭설, 폭염, 한파, 가뭄, 산불, 지진 및 산사태 등을 열거 할 수 있다. 특히, 중규모 위험기상 등으로 인한 집중호우는 지난 35년간 그 빈도가 2배 상승한 것으

로 나타나고 있다. 이러한 이상 현상은 지구온난화 등의 영향과 관계가 있는 것으로 이해되고 있다. 우리나라에 영향을 미치는 태풍은 연 평균 27개 정도가 발생하며 이중 3-4개가 직접적인 영향을 끼치고 있다. 이러한 기후변화에 따라 증가되고 있는 자연재해는 인명 및 경제·사회적으로 막대한 피해를 주고 있어 재해감시, 재난 대비를 위해 보다 더 정확한 감시가 필요한 실정이다.

자연재해인자의 관측은 저궤도 지구관측위성을 이용하여 효율적으로 관측될 수 있다. 기상관측 선진국에서는 많은 수의 저궤도위성 지구관측시스템을 운용하고 지속적인 운용계획을 수립하고 있다. 특히 기상관측에서 저궤도 위성의 활용은 낮은 고도에서 운용되는 특성으로 인해 가시광선, 적외선 및 마이크로파 영역에서 폭넓게 관측할 수 있다는 큰 장점을 가지고 있다. 특히 우주선진국에서는 많은 수의 위성 마이크로파 기상관측시스템을 이용하여 적극적으로 재해인자를 감시하고 수치모델의 필수 입력 자료를 생산·제공하고 있다.

우리나라는 2005년 우주개발진흥법의 제정과 국가우주개발중장기기본계획의 수정 등 제도적인 보완 노력을 하고 있다. 하지만 우리나라가 세계 11대 경제 대국으로 성장할 동안 위성을 독자 개발하여 국내 수요를 충족하고 수출할 정도의 능력을 가진 대표기업이 없는 실정이다. 특히 우리나라 우주개발 임무를 효율적으로 추진하고 국제 경쟁력을 강화하기 위한 우주산업 활성화 방안이 요구된다.

기후 변화에 따른 자연재해는 매년 인명 및 경제·사회적으로 막대한 피해를 주고 있어 재해감시(화산, 지진, 위험기상, 황사, 우주기상)를 위해 보다 더 정확한 감시가 요구되므로 차세대 지구관측위성 탑재체 획득 방안 연구는 매우 중요하고 연구할 가치가 있다. 더욱이 우리나라의 경우는 글로벌 기후 환경 변화에 대응 가능한 저궤도 지구관측위성을 보유하지 않고 있어 국가적 재난감시를 위한 중요 자료 획득은 외국 저궤도 지구관측위성에 전적으로 의존하고 있는 실정이므로 우리나라 지구관측관련 위성정보 관리 고도화를 위하여 차세대 지구관측위성 탑재체 개발은 반드시 필요하다.

따라서 본 논문의 주요 목적은 차세대 지구관측위성 탑재체가 국내에서 개발되어 정확한 자연재해 관련 정보를 제공하여 국민의 행복 지수 및 복지, 안전 향

상에 크게 기여될 수 있는 차세대 지구관측위성 탑재체 획득 방안을 제시하는데 있다.

2. 국내·외 우주 정책 동향

가. 국외 우주정책 동향

1980년대 냉전 종식이후 세계 각국의 우주기술 추진방향이 군수 분야에서 상업 분야로 전환되고 있다. 특히 90년대 이후는 정보화 시대의 핵심 산업으로 소형의 저궤도 위성을 이용한 이동통신 및 원격탐사 분야를 중심으로 미국 주도하에 급신장하고 있다. 미국 및 러시아 등 우주개발 선진국과 일본, 중국, 프랑스, 영국, 독일, 인도 등 우주기술 선진국들은 대부분 위성독자개발기술을 보유하고 있다. 최근의 위성기술개발 현황은 국제적 기술교류를 통한 저궤도 소형위성의 공동개발 및 활용에 치중하고 있는 추세이다.

최근 아시아권에서도 우주기술 분야가 선진국 전유물이 될 수 없다는 인식으로 중국, 태국, 파키스탄 등이 중심이 되어 아시아 우주기구설립이 본격 논의되는 등 아시아권 수요는 아시아권에서 공급하자는 기술 블록화 현상이 대두되고 있다. 또한 미국이 우주개발의 방향을 우주탐사로 변경하면서 전 세계의 주요 우주개발 국가들은 분주하게 우주탐사 참여의 기회를 찾기 시작했다. 국제우주정거장(International Space Station : ISS) 사업을 통해 우주분야 국제협력과 글로벌 리더십을 실현하고자 했던 미국의 의지는 우주왕복선 콜롬비아호의 참사로 실현가능성이 희박해 졌다. 그 후 미국은 이를 만회하고자 2004년 1월 '신 우주탐사 비전'을 발표하면서 우주개발 정책을 우주탐사로 선회하기에 이르렀고, 최근의 몇몇 사례는 미국 우주탐사의 국제협력을 통한 우주분야 글로벌 리더십의 강화에 대한 의지가 조금씩 실현되어가고 있음을 증명하고 있다.

최근 친디아(Chindia)로 불리며 첨단기술을 바탕으로 한 신흥 경제대국으로 부

상하고 있는 중국과 인도는 미국과의 우주탐사 분야 협력에 대한 의지를 표명한 바 있다. 인도는 달 탐사 무인우주선 '찬드라얀(Chandrayaan) 1호'의 제작을 위해 미국 항공우주국(NASA)과 협력하기로 2006년 5월 중순 합의하였으며, 중국도 2007년 4월 예정되어 있는 달 탐사위성의 발사를 미국과의 협력 하에 진행하는 것을 검토 중에 있다. 이와 같은 우주개발의 패러다임 변동과 함께 우주산업의 구조적인 변화도 나타나고 있다. 1990년대에서 2000년대를 지나오면서 나타났던 항공 산업계의 인수와 합병을 통한 거대기업화 현상과 비슷하게 우주분야도 유럽을 중심으로 하여 주요 산업체간의 인수와 합병이 활발하게 진행되고 있다. 미국의 우주개발 예산이 민수 및 군수분야를 통틀어 총 345억 달러로 전 세계 우주개발 예산의 75%를 차지하고 있으며, 프랑스와 일본이 20억 달러 정도의 예산을 지출하고 있다.

(1) 미국

미국은 우주의 산업화를 위한 지원정책으로 다음과 같은 정책을 실시하기로 했다. 먼저 우주산업능력을 유지 지원한다. 실증실험 과정까지의 비용위험을 부담하고, 국방성에 의한 군사위성 및 발사 로켓의 통합 발주와 함께 연구개발 자금을 지원한다. 그리고 우주산업확대를 실시한다. 또한 부가가치세를 면제하고 로켓 발사장(군사시설) 및 대형시험설비 등 인프라를 지원한다. 마지막으로 리모트 센싱 데이터의 민간구입 촉진을 도모한다.

(2) 유럽

유럽우주기구(ESA; European Space Agency)에서는 우주산업정책으로 회원국가의 기술 및 자금 기여도에 따른 보상을 보장해 줄 것을 약속하고 있다. 이는 경쟁력 향상과 비용 효율성이 고려된 연구개발 및 산업 활동을 추구하기 위한 것이다. 또한 우주의 산업화를 위한 지원정책의 화두로 '유럽의 자율성'을 내세우며, 2003년 유럽 우주백서를 통해 대미 의존 경감측면에서의 전략 산업으로 육성하겠

다는 의지를 표명했다. 주요 내용은 다음과 같다. 첫째, ESA 내 회원 국가의 기부를 통한 회원국 산업 활동을 지원한다. 둘째, 갈릴레오 프로젝트 추진을 통한 산업화를 촉진한다. 셋째, 러시아 기업과의 협력에 의한 저가 발사체 사업 개시, 유럽 각국과 러시아간 상호면세 협정을 체결한다. 넷째, 로켓발사장 등 인프라 정비를 통한 시설을 확보한다.

(3) 일본

2005년 3월 일본의 경제 산업성은 우주 산업의 진흥을 위해 2020년까지의 우주 기술 전략맵을 작성하였다. 우주 산업화를 위한 정부의 환경정비 움직임도 있다. 먼저 국제표준규격의 제정을 촉진한다. 또한 공동이용 시설을 정비하고, 군용 기술을 민간으로 이전한다. 그리고 법적기반 정비와 함께 해외사업을 지원한다. 민간 우주사업자의 지원을 위해서는 다음과 같은 정책이 제안된다. 먼저 세제지원, 저리융자, 무역금융 및 무역보험에 의한 지원, 정부수뇌에 의한 해외로의 매입지원(외교활동), 법적 환경정비 등이다. 로켓사업 지원에 있어서는 발사서비스의 부가가치세 면세, 인공위성 및 부품에 대한 부가가치세 면세, 발사장 정비를 통한 발사시기 제약완화, 로켓 수송을 위한 공항정비, 정부위성 발사의 보장 등이다. 또한 인공위성사업 지원에 있어서는 공통위성버스의 제작, 민생부품의 활용, 위성 CALS[1] 구축, 연구개발 종료 위성의 매각 등이 있다. 경제 산업면에서는 산업경쟁력 강화전략에 있어서 우주산업은 첨단기술과 고도한 소재부품이 사용되는 시스템으로서, 앞으로 유망분야로 간주되고 있다. 또한 안전보장에 필요한 산업이며, 방위기반의 유지와 강화를 위해 중요한 의미를 가진다.

---

1) CALS의 약어는 그 적용의 범위 및 개념의 확대에 따라 다음과 같은 변천이 있다.
- Computer Aided Logistic Support (1985년, 군수지원 전산화: 컴퓨터에 의한 병참지원)
- Computer-aided Acquisition and Logistic Support (1988년)
(무기체계획득 및 군수지원 전산화: 컴퓨터에 의한 조달 및 병참지원)
- Continuous Acquisition and Life cycle Support (1993년)
(통합물류 생산, 조달, 운영지원 자동화: 지속적인 조달과 제품의 라이프사이클 지원)
- Commerce At Light Speed (광속상거래, 1994년)

(4) 브라질

브라질은 1951년 설립된 국가연구위원회(the National Research council: CNR, 그 후 과학기술개발 국가위원회로 명칭 변경함)를 통해 전 분야의 산업화를 지원하게 된다. 1964년 국립경제발전은행(the National Bank for Economic Development, 그 후 경제 및 사회발전으로 확대)을 설립하고 과학기술개발기금(the Fund for Technical and Scientific Development: FUNTEC)을 만들어 기술개발연구를 지원하고 있다.

(5) 이스라엘

이스라엘은 미국 등 기존의 항공우주 선진국과 경쟁분야를 회피하고, 틈새시장이나 또는 큰 업체나 국가들이 시도하기 어려운 분야에 대한 집중 투자를 하고 있다. 자국 내 시장의 협소성을 극복하기 위하여 제품 개발 전 해외 시장에 대한 충분한 판매 가능성을 분석하고 70~80%의 해외 판매가 불가능하면 개발을 시도하지 않는다. 업체의 기술경쟁력 강화를 위하여 국내 개발의 경우 최대한 25%이내에서 개발비 지원, 더 이상의 지원은 업체 경쟁력 저하의 원인을 제공한다는 판단 아래 해외 국가 및 업체와의 협력으로 개발비용을 보충하고 있다.

나. 안보에 우주이용 동향

미국은 1958년에 세계 최초로 군용 통신위성을 발사하여 군 통신망을 구축하였고, 2009년에는 러시아 위성이 미국 위성에 충돌하여 우주감시 기능을 강화하고 있다. 2010년의 국가우주전략에 적극적으로 자국과 동맹국 우주시스템을 보호하기 위해 방호나 억지에 실패한 경우 파괴한다고 기술하고 있다. 특히 안보를 위해 사용되는 위성별 목적을 살펴보면, 지상영상을 수집하는 지구관측위성은 지상을 촬영하고, 전파수집위성은 지상의 전파신호를 수집하고, 정찰위성은 미사일 발사를 탐지하고, 통신위성은 각 부대 간의 통신에 사용하고, 우주상황인식시스템은

우주공간에 떠도는 우주파편과 타국의 위성 움직임을 모니터링하고 있다.

일본의 경우도 위성을 이용한 해양상황파악(MDA; Martime Domain Awareness), 우주상황파악(SSA; Space Situational Awareness), 탄도미사일 공격에 대응에 많은 노력을 하고 있다. 이상과 같이 우주는 지상의 지표와 전파를 감시하고 통신을 중계하는 지상 안보 감시기지제공 역할을 하면서 또한 그 자체인 우주 공간이 점차 안보 공간화하고 있어 안보에서 중요한 관심의 대상이 되고 있다.

다. 국내 우주정책 동향

우리나라의 우주개발은 비교적 짧은 역사임에도 불구하고, 점진적인 발전을 거듭해 오고 있다. 여기에는 정부의 명확한 목표설정과 강력한 추진 정책의 힘이 크다고 할 수 있다. 즉, 미래부(구 과학기술부)에서는 2015년까지의 우리나라의 우주개발 방향을 정립한 국가우주개발 중장기계획을 1996년에 수립하였으며, 1998년과 2000년 말 그동안의 변화와 새로운 수요를 반영하여 일부 내용을 수정 보완한 바 있다. 그리고 2005년 5월 17일에 '국가 우주개발 중장기 기본계획'의 제3차 수정이 국가과학기술위원회에서 결의되었고, 이번 수정을 통하여 2005년을 우주개발 원년으로 하여 향후 장기적으로 수행될 국가 우주개발에 대한 방향과 유연성 있는 목표 및 계획을 제시하였다.

우주개발 중장기기본계획 상의 우주개발 장기목표는 핵심 우주기술 개발로 독자적 우주개발능력을 확보하여 우주산업 세계시장 진출을 통한 세계 10위권 진입, 우주공간의 영역 확보 및 우주활용으로 국민 삶의 질 향상, 성공적 우주개발을 통한 국민의 자긍심 고취 등이 그 내용이다. 위성체 개발 부문에서는 1992년부터 2020년까지 총 19기(개발 중 6기 포함)의 인공위성 개발 (운용종료 7기, 운용 중 4기)을 통하여 저궤도 실용위성 및 정지궤도 위성의 국내 독자개발 능력 구축, 위성자료 수신처리 및 위성영상 활용 능력 확보, 다목적실용위성을 활용하여 세계 위성영상 시장 진출 등을 꾀하고 있다.

최근 들어서는 우주응용 기술의 개발을 위해 많은 노력을 기울이고 있다. 지구관측 인공위성을 이용한 원격탐사기술 개발, 우주정거장 사업 참여를 통한 우주공간에서의 과학실험 공간 확보, 우주항법시스템 사업, 우주인 배출 사업 등 우리나라의 우주분야도 실생활에서의 이용분야에 중점을 두고 발전해 나가고 있다. 이러한 미래 한국의 우주기술 선진화를 이끌어 가기 위해서는 정부의 확고한 우주개발 정책과 국민적인 동의, 우수한 개발인력과 예산이 그 뒷받침이라 할 수 있다. 이를 시기별로 살펴보면, 2008년까지 소형위성 자력발사능력을 확보하고 2010년까지 국내 기술에 의한 저궤도 실용위성을 독자 개발하여 세계우주산업 시장에 진출하기 위한 기반기술을 마련하였다. 이와 더불어, 저궤도 인공위성을 발사할 우주센터 건설을 2008년에 완수하였다. 이를 분야별로 세부 육성계획을 살펴보면 다음과 같다.

첫째, 인공위성 분야에서는 2015년까지 위성의 독자설계 능력을 축적하고 지구 및 환경관측 등 공공수요를 충족시키기 위하여 8기의 저궤도용 다목적 실용위성을 개발할 예정이다. 이를 위해 1999년 다목적실용위성 1호기에 이어, 2006년에는 국내 주도 설계기술로 개발한 다목적실용위성 아리랑 2호를 발사했다. 2010년에는 우리나라 최초 정지궤도 공공위성인 천리안1호가 성공적으로 발사되어 기상 및 해양 서비스를 제공하고 있다. 또한 2012년 5월 18일에는 아리랑 3호를 2013년 8월 22일에는 기상여건에 관계없이 고해상도의 정밀관측이 가능한 SAR (Synthetic Aperture Radar; 합성개구레이더)가 탑재된 아리랑 5호를 각각 성공적으로 발사하였다. 2015년 3월26일에는 아리랑 3A호를 발사하였다. 우리나라가 독자적으로 개발을 추진하고 있는 천리안 2호 위성인 정지궤도 복합위성(GEO_KOMPSAT 2A, 2B)이 현재 개발되고 있어 2018년 및 2019년 상반기에 각각 발사하게 되면 우리국민에게 삶의 질 향상에 기여하게 될 고도화 기상정보 및 환경 해양 정보 서비스를 제공하게 될 것이다. 통신방송위성분야에 있어서도 그동안 직구매방식에서 국내생산을 점차 확대될 것으로 기대된다.

둘째, 발사체 분야에서는 2008년까지 저궤도에 진입 가능한 소형 위성용 발사체를 개발하여 세계 10대 발사체 기술보유 국가로 진입할 예정이었으나 나로호

발사가 실패를 거듭하였으나 2013년 1월 30일 나로위성을 탑재한 나로호가 발사에 성공하여 우리나라는 아시아 지역에서 일본, 중국, 인도에 이어 4번째 위성 발사기술 보유국가로 진입하였다. 아울러, 세계에서 열한번째로 스페이스 클럽에 입성하게 되었다.

한국항공우주연구원은 나로호를 통해 축적한 기술과 경험을 바탕으로 지난 2010년부터 독자적인 우주발사체(KSLV-Ⅱ)를 개발 중에 있다. 한국형발사체는 1.5톤급 실용위성을 지구저궤도(600~800km) 에 투입할 수 있는 300톤급(75톤급 엔진 4기 묶음) 3단형 발사체다. 한국형발사체는 시스템 설계부터 제작, 시험, 조립, 발사운영까지 모두 독자 기술로 수행되고 있다. 한국형발사체는 투입된 기술, 소재, 인력을 모두 합쳐 90%이상 국산화를 목적으로 개발되고 있으며, 2020년에 예정된 발사에 성공하면 우리나라도 우주기술 개발 자립국으로 도약하게 된다.

3. 지구관측위성 탑재체 국내·외 개발 현황 분석

가. 저궤도 지구관측위성 탑재체 국외 개발 현황

지구관측 위성을 이용하는 분야는 주로 영상과 기상학에 집중되어 있다. 영상은 Google Earth와 Microsoft Live Local 등을 통하여 인터넷에서 많이 활용되고 있으며, 기상학은 일기예보 능력을 향상시키는 수치기상예측(NWP: Numerical Weather Prediction) 모델을 얻기 위하여 기상위성 자료를 일일 단위로 이용하고 있다. 기상학은 지구관측위성 데이터를 이용하는 분야 중에서 가장 정립이 잘 된 분야의 하나로, 위성으로부터 얻은 정보로 전 세계적 기상 서비스 제공하고 있다. 기상 전용 위성이 수십 년 동안 운영되어 오면서 지구의 많은 부분을 지속적으로 관측하고 있다. 향후 15년 동안 계획된 위성의 약 1/3인 80개 위성이 기상학을 주 목적으로 하고 있으며, 나머지 위성은 다양한 범위의 연구용, 상업용으로 사용될 것이다.

지구 환경 문제의 중요성, 그리고 위성 지구관측의 독특한 역할을 감안할 때, 많은 위성이 기후 또는 환경 연구와 같은 다양한 측면을 파악하는 용도로 사용될 것이다. 나머지는 지속 가능한 개발 전략에 필요한 정보 제공을 포함하여, 산업, 경제, 자연 자원의 전략적 계획과 관리에서 의사 결정을 보조하기 위해 활용될 것이다. 또한, 대지, 바다, 대기 조성에 관련된 정보를 제공하는 새로운 위성들이 최근에 발사되었거나 가까운 장래에 발사될 것이다. 위성에서 사용하는 측정 주파수가 증가하고, 위성 기술과 센서 기술이 향상되고, 지구관측 데이터의 접속과 분석이 보다 용이해짐에 따라 위성 데이터에 대한 수요 증가와 여러 분야에서 가까운 미래에 사용될 것으로 예상되는 새로운 서비스 구현에 기여할 것이다. 지구관측위성위원회(CEOS: Committee on Earth Observation Satellites)는 2027년까지 지구관측(EO: Earth Observation) 미션을 가진 약 260개 위성을 운용하거나 발사를 계획 중에 있다. 이 위성들에는 총 400개의 관측 장비가 탑재될 예정이다. CEOS에서는 위성에 탑재된 장비를 다음 표 1과 같이 분류하고 있다.

[표 1] CEOS에서 위성에 탑재체

위성탑재체	
Atmospheric Chemistry Instruments	대기화학 관측 장비
Atmospheric Temperature and Humidity Sounders	대기온도 및 습도 측정 장비
Cloud Profile and Rain Radars	구름 종류 및 강우 레이더
Earth Radiation Budget Radiometers	지구 복사량 측정 라디오미터
High Resolution Optical Imagers	고분해능 광학영상
Hyperspectral Imagers	초분광 영상
Imaging Multi-Spectral Radiometers (Passive MW)	다중 분광 영상 라디오미터 수동 마이크로웨이브
Imaging MW Radars	마이크로웨이브 영상 레이더
Lidars	라이다
Lightning Instruments	번개 관측 장비
Multiple Direction/Polarization Instruments	다중경로/ 편광 장치
Radar Altimeters	레이더 고도계
Scatterometer	산란계
SAR(Synthetic Aperture Radar,	합성개구레이더

자료 : 저궤도 기상위성 개발을 위한 기획연구, 2012, 국가위성센터

미래의 위성과 관측 장비에 대한 계획은 전적으로 새로운 형태의 측정 기술을 필요로 한다. 초분광(hyper-spectral) 센서, 구름 레이더(cloud radars), 라이더(lidars), 편광(polarimetric) 센서 등은 새로운 측정 기술을 이용한 장비이다. 이런 장비들은 대기온도, 수증기, 토양 수분, 해양 염분과 같은 주요한 파라미터에 대한 새로운 통찰력을 제공할 것이다. 해양 지오이드(geoid)를 보다 정확히 결정하려는 목적의 새로운 중력장 측정 위성도 계획되고 있다. 장기간의 데이터베이스를 얻기 위하여 기존의 주요한 측정을 지속적으로 할 수 있도록 하는 노력도 이루어지고 있다. 또한, 미래 계획의 우선권은 재해를 관리하고 주요 지구 시스템 프로세스(Earth System processes)를 연구하는 것에 있을 것이다. 주요한 지구 시스템 프로세스로는 물 순환(water cycle), 탄소 순환(carbon cycle), 빙권(cryosphere), 전 세계 기후 변화에서 구름과 에어로솔의 역할, 해수면(sea level) 상승 등이 있다. 수동형 마이크로파 탑재체 및 SAR 탑재체 개발현황 다음과 같다.

(1) 수동형 마이크로파 탑재체 개발현황

ATMS(Advanced Technology Microwave Sounder, 고도화 마이프로웨이브 탐측기)는 NGES에 의하여 개발되어졌고 목적은 AMSU-A1/A2와 AMSU-B/MHS의 3개의 탑재체를 계승하여 수동형 마이크로파 관측 능력을 조합하는 것이다. 또한 발전된 마이크로파 수신기 기술을 사용하여 전력 소모와 중량이 감소되었다. ATMS는 수동형 전 전력 방식 마이크로파 탐측기이며 열적외 탐측기와 관측 데이터를 조합하며 매일 지구 대기 온도 및 습도와 기압 프로파일을 제공한다. ATMS는 현재 운용중인 극궤도 환경 위성(POES) 위성들의 탑재체를 대체하기 위하여 만들어졌으며, 모놀리식 집적 회로(MMIC[2])를 사용하여 POES와 Aqua의 수동형 마이크로파 탐측기에 비하여 중량과 크기가 1/3 이다.

ATMS는 크로스트랙 스캔 방식을 사용하며 스캔 폭은 2300km이고 한 개의 풋

2) MMIC, Monolithic Microwave Integrated Circuit, 갈륨비소(GaAs) 등의 고속・고전도율의 반도체 기판 위에 마이크로파 주파수대(300 MHz~300 GHz)에서 작동하는 회로 소자의 접속 부분을 형성한 집적 회로

프린트(Foot Print)의 크기는 약 1.5km이다. 고유 관측 해상도는 1.5km 보다 좋으나 지상국 처리에서 SNR(Signal Noise Ratio; 신호대비 잡음)을 증가시키기 위하여 공간 평균화 계산을 수행한다. 그러므로 ATMS 데이터의 공간 해상도는 1.5km이다. ATMS는 3개의 안테나 빔폭을 갖는다. 온도 탐측 채널들은 2.2도이고 습도 채널들은 1.1도이다. 채널 1과 2는 5.2도의 빔폭이다.

각 스캔 주기 동안 주 반사기에 의한 온 보드 교정소스 관측을 사용한다. ATMS의 교정은 흑체와 심 우주관측에 의한 2 point 교정 서브시스템이다. 심 우주관측은 매 스캔 주기 마다 관측한다. 교정을 수행한 후 ATMS 데이터는 요구되는 마이크로파 탐측 측정의 높은 정확도를 만족한다. TMS의 데이터는 MIL(military)-STD(Standard)-1553B 버스 인터페이스를 사용하여 위성본체에 전송된다. ATMS는 약 85kg의 중량을 갖고 궤도 평균 전력 110W를 소모한다. ATMS의 전송속도(Data rate)은 20kbit/s(평균)과 최대 28kbit/s 이다.

(2) SAR 탑재체 개발현황

우선 2009년 ESA에 의해 개발된 SMOS (Soil Moisture and Ocean Salinity) 위성이 지구저궤도(LEO, Low Earth Orbit)로 발사되었고, 합성개구라디오미터(MIRAS, Microwave Imaging Radiometer using Aperture Synthesis)를 이용하여 토양수분 및 해양 염도를 측정한다. 또한 2012년 5월, 일본우주항공연구개발기구(JAXA, Japan Aerospace Exploration Agency)에서 개발된 AMSR-2 탑재체가 GCOM-W(Global Change Observation Mission - Water) 위성에 탑재되어 발사되었다. 2012년 7월부터 시작하여 현재까지 토양수분을 비롯하여 지구의 물 순환과 관련된 대기의 강수량, 해수면 온도 등을 포함한 8가지 물리 변수에 대한 관측 결과를 제공하고 있다. 다음으로 2013년 발사된 일본 JAXA의 지표면관측위성 ALOS-2(Advanced Land Observing Satellite-2)는 L-밴드 레이더를 사용하여 마이크로파를 방출하고 정보를 획득하기 위해 지상에서 반사되는 빔을 수신하는 위성으로 임무 목적으로는 고해상도 전천후 토양과 해수면 특성을 관측하는 것이

다. 추가적으로, 토지 모니터링(생물권, 빙권, 지구표면), 재해 모니터링의 빠른 관측 및 자원 탐사를 목적으로 한다. ALOS-2의 임무 센서로는 L-밴드 SAR 레이더인 PALSAR-2(Phased Array type L-band Synthetic Aperture Radar)가 탑재되어 있다. L-밴드 SAR 레이더는 위상배열레이더로 다수의 편광 기능을 가지고 있다.

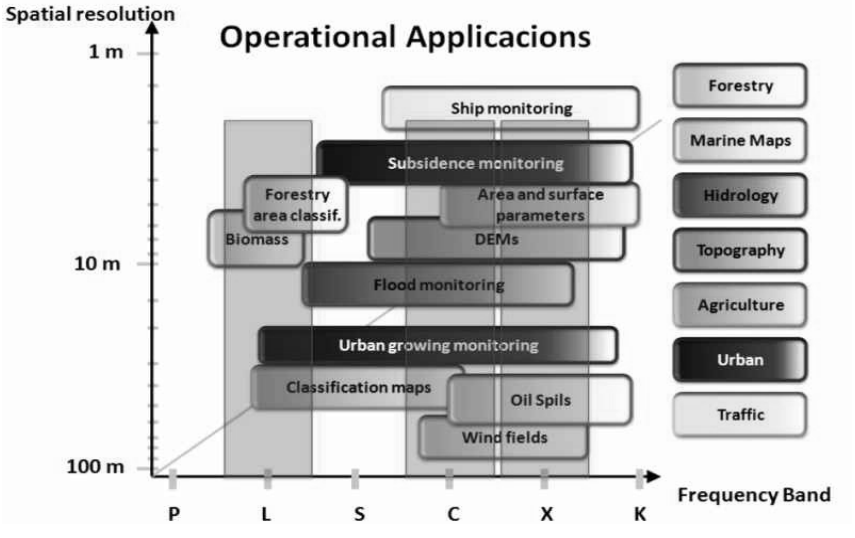
영국에서 2013년에 발사된 SSTL(사)의 NovaSAR-S는 지구관측에 혁신적인 개념을 제공한 위성으로, 상용 기성품의 조합을 이용하여 SSTL(Surrey Satellite Technology LTD.)의 저가, 소형위성 임무를 시험하는 소형 SAR 임무 위성이다. 이는 홍수 모니터링, 농업 작물평가, 온대와 열대 우림지역 모니터링, 토지 이용 매핑, 재해관리 및 해양프로그램(선박탐지, 기름 유출 모니터링, 해상 안전, 국방 응용프로그램의 보안 등)에 적용하는 것을 운용 임무로 한다. SSTL은 다수의 응용 프로그램에 대한 최종 솔루션을 위하여 Airbus Defence & Space에서 SAR 전문가들과 협력 개발 중에 있다.

러시아와 남아프리카공화국이 2014년에 발사한 '지구관측위성 Kondor-E'는 S-대역 SAR를 탑재한 지구관측위성 및 스파이 정찰위성이다. 이 위성의 평균고도는 500km (450~900km)이며, 궤도의 경사각은 약 98도이다. 장착된 SAR 영상의 해상도는 1~3m급이며, 관측 범위는 약 1,200km 정도, 레이더 안테나의 직경은 약 6m이다. 레이더 주파수는 9.6cm(3.13 GHz)인 S-대역이며 수명은 최저 3년에서 최대 10년이다.

미 항공우주국 (NASA: National Astronautics and Space Administration)과 인도 우주연구기구(ISRO; Indian Space Research Organization)는 전천후 영상레이더(SAR)를 활용하여 매 12일마다 지구표면을 지도화(Mapping)할 수 있는 지구궤도 과학 및 응용 임무에 대한 연구를 수행 중에 있다. 커버리지, 샘플링과 정확도 요구조건 등에 대한 요구를 충족시키기 위하여 시스템은 요구되는 완전 편광을 이용하여 미세 해상도에서 240km 대역폭을 달성하도록 설계되어있다. SAR는 전자광학카메라와는 달리, 비, 구름, 연기, 안개 등 기상조건이나 주야간, 역광 등 일조량에 관계없이 광범위한 지역의 영상획득이 가능한 특징이 있어, SEASAT에서 그 유용성이 확인된 후, SAR를 적용한 다양한 위성이 개발 및 활

용되고 있다. SAR 영상은 토양수분량, 강호수 면적, 습지대분류, 수계패턴, 홍수 감시 등 수자원 관리 외에도 선박감시, 기름 유출, 산림감시, 홍수관리, 토지이용 관리, 농업, 재난 감시 등 다양한 분야에서 활용되며, 주파수에 따른 영상 이용 분야와 요구 해상도는 앞의 그림 1과 같다.

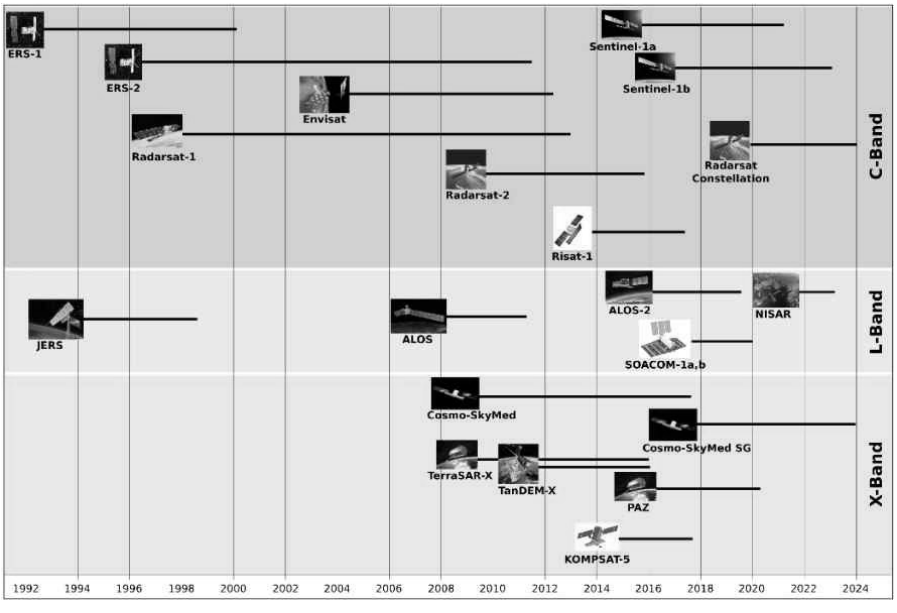
[그림 1] 영상레이더 활용분야와 해상도 및 주파수 관계



출처 : 한국항공우주연구원, 2016

한편, 위성 영상레이더의 경우, 위성에 탑재할 수 있는 레이더의 기기 무게 및 부피가 제한되고 우주공간과 지상 간 전자파의 감쇄특성이 다르기 때문이 L(약 1.2 GHz), C(약 5.3 GHz), X(약 9.6 GHz) 밴드 위주로 개발되어 활용되고 있으며, 특히 C밴드 영상레이더 신호는 식물에 대한 투과력은 L 밴드보다 떨어지나, 우리나라처럼 초목의 잎이 크지 않은 경우에, 토양수분관측 및 홍수 감시 등의 분야에서 활용될 수 있다. 다음 [그림 2] SAR를 탑재한 위성들의 로드맵이다.

[그림 2] 중요 위성영상레이더 로드맵



출처 : 한국항공우주연구원, 2016

상기의 센서별 동향과 함께, 특정 기관인 일본의 우주개발기관인 JAXA는 미래의 지구관측 임무에 사용을 목표로 관측센서 설계기술을 축적하고 10~20년 후를 내다보고 필요한 요소 차원의 기술연구, 센서시스템 연구를 하고 있고, 이들 센서 시스템을 이용한 임무를 국내외와 협력을 하고 있다. 이를 위해 JAXA는 센서연구 그룹을 운영하고 있다. 센서연구그룹은 관측위성의 눈인 각종 센서를 개발하여 새로운 영역을 개척하고, 이를 재난 등의 사회 안전에 활용할 목표로 관측센서를 총체적으로 검토하여 용도별로 개발을 장기적으로 추진하고 있다. 이 역량이 일본의 관측위성 역량으로 연계되어 기술력을 세계적으로 인정받고 있다.

나. 국내 저궤도 지구관측위성 개발 추진 전략 분석

(1) 개발 추진전략

다음 표 2에는 국내 저궤도 지구관측위성 개발에 관한 SWOT(Strength, Weakness, Opportunities, Threat) 분석에 따른 대응 전략이 기술되어 있다.

[표 2] SWOT 분석

Strength Weakness Opportunity Threat		강점(S)	약점(W)
		• 저궤도 위성시스템 개발 Infra 환경 구축 • 저궤도 위성 시스템 R&D • 인력 확보 • 정부의 적극적인 위성시스템 R&D 활성화 정책 및 지원 • 저궤도 지구 관측 위성 Model (CAS 500) 위성본체 확보	• 저궤도 지구관측위성 탑재체원천기반기술 취약 • 저궤도 지구관측위성 탑재체 산업화/상용화 기반 미비 • 저궤도 지구관측위성 운용 / 활용 국제협력 결여 • 저궤도 지구관측위성 탑재체 부품 제작업체 부족
기회 (O)	• 국가 위성시스템 기술개발투자 확대 • 거대 전 지구적 위성시스템시장 규모 • 저궤도 지구관측위성 탑재체기술 및 활용 틈새시장 개척가능 • 지구관측위성 데이터 활용에 따른 가뭄 및 홍수 대비 국가 정책수립 및 수행에 기여	S-O전략	W-O전략
		• 저궤도 지구관측위성 본체 국내 자체 개발 추진 • 저궤도 지구관측위성 국내외 마케팅을 통한 위성산업 활성 화 • 우리나라 수자원관리 및 국민의 삶의 질 고도화	• 저궤도 지구관측위성 탑재체 소요부품 국산화 • 저궤도 지구관측위성 탑재체 원체기반기술 확보 • 저궤도 지구관측위성 운용 및 활용 글로벌화 추진
위협 (T)	• 미국, 유럽, 일본 등 우주선진국들의 저궤도 지구관측위성 탑재체 기술 고도화 • 저궤도 지구관측위성 탑재체 기술 분야 경쟁 심화 • 저궤도 지구관측위성 탑재체기술 판매 및 기술이전 제한 • 우주선진국의 저궤도 지구관측위성 데이터 판매 회사 등장 • 국내 저궤도 관측위성 데이터 활용기반기술 위축	S-T전	W-T전략
		• 저궤도 지구관측위성 탑재체 국산화 기술 확보를 위한 지구관축위성 탑재체 연구소 설비 • 저궤도 지구관측위성 탑재체 국외업체와 공동개발 추진 • 저궤도 지구관측위성 탑재체및 활용 기술 획득을 위한 전문 인력 양성	• 국내 저궤도 관측위성 • 데이터 활용기반기술 개발 추진 • 위성선진국들과 국제협력을 통한 저궤도 지구관측위성 • 탑재체 및 활용기술 확보 • 저궤도 지구관측위성 탑재체 산업화/상용화 국가 정책수립

(2) 국내 고주파수 대역 탑재체 개발 역량 분석

(가) 위성탑재체 국내 기술수준(TRL: Technology Rediness Level, 기술성숙도)

국내 최초의 인공위성인 우리별 1호 (1992년) 및 2호 (1993년) 개발 성공으로 우리나라는 인공위성 개발 국가로 진입하였다. 다목적 실용위성 1호, 2호, 3호 개발 성공으로 실용급 위성 능력은 확보되었다. 다목적 실용위성 1호는 미국 TRW로부터 기술전수를 받아 제작되었다. 다목적 실용위성 2호는 다국적 기업인 EADS ASTRIUM (본체)과 이스라엘 ELOP (광학 탑재체)의 기술자문을 받아 제작되었다. 하지만 다목적 실용위성 3호의 본체와 탑재체는 대부분 우리기술로 독자 개발되었다. 정지궤도 복합위성인 천리안 1호 위성의 본체 및 통신 탑재체 역시 상당부분 국산화되었다. 이렇듯 우리나라는 지속적인 위성 프로그램 진행을

[표 3] X 대역 통신탑재체 분야 기술수준

분야	세부분야	기술적 난이도	국내기술 수준(TRL*)	개발가능성
통신 탑재체 체계종합	시스템 엔지니어링	10	6	보안체계, 신뢰도측면에서 부족 기술은 해외기술협력으로 보완하여 국산화 추진
PA (Product Assurance)	PA	8	8	자체기술로 국산화 추진
중계기	중계기시스템	10	6	설계측면에서 부족한 기술은 해외기술협력으로 보완하여 국산화 추진
	능동부품	9	7	국산화 추진, 일부 부품 도입 (고출력 증폭기 등)
	디지털 채널라이저	10	6	현재 우주인증 모델개발 중,
	수동부품	9	7	자체기술로 국산화 가능, 일부 부품 도입 (스위치 등)
안테나	안테나 시스템	9	7	설계측면에서 부족한 기술은 해외기술협력으로 보완 국산화 추진
	반사판	9	7	자체기술로 국산화 가능
	수동 급전부	9	7	자체기술로 국산화 가능
	성능/ 환경분석	8	9	자체기술로 국산화 가능

출처 : 차기군 위성체계 사업 분석을 위한 타당성 연구, 2012.4, (주)KT)

통하여 상당부분 기술 자립화를 이룬 것으로 평가되고 있다. 다음 표 3은 우리나라 통신위성 탑재체 분야의 기술성숙도 (Technology Readiness Level: TRL)를 정리한 것이다.

(나) 위성 탑재체 및 부품 국산화 현황 분석

천리안 1호 위성 통신탑재체 순수 국산기술 개발을 위해 중계기와 안테나의 부품, 시스템설계는 한국전자통신연구원(ETRI) 주관, 제작은 국내업체 중심 수행, 시험은 ETRI와 국내업체가 공동으로 수행하였으며, 통신탑재체 개발항목은 총 21종으로 국산화항목은 17종, 해외구매항목은 4종이다. 천리안 1호 위성개발 중 이루어진 국산화 부품 항목은 부가가치가 큰 중계기와 안테나 핵심부품인 RF 능동 및 수동부품, 위성안테나 급전부품과 반사판 등이 포함되었으며, 이들은 국내 기술진에 의해 설계 제작된 후에 성능 및 우주환경시험 등을 통해 검증이 완료되었다. 천리안 1호 위성의 국산화 통신탑재체는 다음 그림 3과 같다.

[그림 3] 천리안 1호 위성 통신탑재체 조립 형상 및 안테나 전개 형상

출처 : 한국전자통신연구원, 2012

국내 위성용 SAR 탑재체는 다목적실용위성5호에 X 밴드 SAR를 이탈리아 TAS(구, Alenia)에서 턴키방식으로 구매하여 장착한 수준이며 아직 개발된 것을

없다. X-밴드 이외의 SAR 탑재체에 대해서는, 국내의 기술개발 경험이 아주 미약하다. 한국항공우주연구원에서는 2018년 말에 EQM 제작을 목표로 X 밴드 외에도 C/Ku 밴드를 갖는 다채널 영상레이더의 핵심기술을 개발하고 있는 중이다. 다음 표 4는 SAR 탑재체 주요요소 기술 수준을 나타낸다.

[표 4] SAR 탑재체 주요 요소기술 수준

분 류		주요 부분품	요소기술개발 현황	기술 성숙도
안테나	전개장치	pyro 타입 전개장치	다목적위성 3호 태양전지판 전개장치	5
	방사장치	영상레이더 안테나	국내 개발사례 없음	3
송신단	발생기	파형발생기 (대역폭 300 MHz급 이상)	다목적 6호 개발모델 (대역폭 150MHz) 선행개발 항공용 레이더 개발모델 (대역폭 300MHz)	3
	증폭기	고출력증폭기	상용 통신용 TWTA 개발 경험	4
수신단	수신기	RF/IF수신기	통신용 RF 수신기 개발경험 (AP 항공우주, 세트렉아이, 쌀리드)	3

자료 : 한국항공우주연구원 추정치, 2016.10

우리나라는 미국, 유럽, 러시아, 일본, 중국, 캐나다, 인도에 이어 세계 8위의 우주 경쟁력을 갖는 나라로 Futron's 2009 Space Competitiveness Index에서 분석되었고, 프랑스, 영국, 독일, 이탈리아 4개국을 개별국가로 간주한 경우 우리나라는 세계 11위권으로 분석되고 있다. 그러나 사업진행 위주의 연구개발과 선진국의 기술 보호 정책에 따라 핵심기술에 대한 자립도는 높지 않은 것으로 평가되고 있다. [표 4]에서 제시된 것처럼 SAR 탑재체의 경우 관련 기술성숙도가 낮은 것으로 평가되어 미확보 기술에 대한 자립화 전략 및 기술 개발이 필요하다.

4. 차세대 지구관측위성 탑재체 개발 방안

가. 탑재체 시스템 개발 방안

차세대 저궤도 지구관측위성 탑재체 개발 방안에 관한 기술자립 가능성 및 평가는 다음 표 5에 제시되어 있다

[표 5] 탑재체 개발 방법 별 기술자립 가능성 및 평가

서브시스템	안테나	수신기	스캔구동	전기장치	조립/시험	지상검보정	시스템
해외구매개발	○	○	○	○	○	○	○
해외기술협력	○	○	○	○	○	△	△
해외공동개발	○	◇	○	◇	○	◇	◇
국내주도개발	◇	◇	○	◇	◇	◇	◇
국내독자개발	◇	◇	◇	◇	◇	◇	◇

주 : ○:해외 개발, △:협력개발, ◇:국내 개발

차세대 저궤도 지구관측위성 탑재체 개발 방안은 다음과 같이 분류된다. 해외구매 개발은 해외에서 기존 위성용 라디오미터 시스템 개발 경험이 있는 회사에서 기 개발된 하드웨어에 인터페이스 등 일부 규격변경만 요청하는 구매 개발하는 것이다. 해외 기술 협력 개발은 기존 위성용 라디오미터 시스템 개발 경험이 있는 해외 기관의 책임 하에 기술 협력형태로 개발. 그러나 기술 습득을 위해 시스템 설계, 지상 검보정 등은 국내 연구진이 직접 참여하여 개발을 수행하는 방법이다. 해외 공동 개발은 국외 위성용 라디오미터 시스템 개발 경험이 있는 해외기관과 공동 개발 형태로 진행. 국내 연구진이 시스템 설계부터 최종 검증까지 참여하고, 수신기 전기장치나 데이터 인터페이스 및 통신 모듈 등 개발이 가능 부분을 발굴하여 진행하는 방법이다.

국내 주도 개발은 일부 국내 제작이 어려운 안테나 시스템 및 스캔 구동 시스템은 국외에서 조달하고 반사기 및 수신기서브시스템 및 전기 서브시스템 등 국내 강점이 있는 부분은 개발하여 조달. 최종 시스템 조립, 정렬 및 측정 시험은 국내

에서 수행하는 방법이다. 국내 독자 개발은 위성용 마이크로파 라디오미터의 시스템 설계부터 최종 검보정까지의 전체 개발과정을 국내 기술로 독자 개발. 즉, 대부분의 주요 부분품도 국내 기술로 개발하여 조달하는 방법이다.

위의 [표 5]는 탑재체에 대한 포괄적 측면에서의 기술확보 방안이다. 이는 아직 우리가 위성의 눈인 센서를 포함한 탑재체 개발역량이 거의 전무한 상황에서 전문가들의 일반적 견해를 정리한 것이다. 우주개발중장기계획에서 제시하고 있는 향후 위성 수가 적지 않기 때문에 이들 위성에 탑재할 탑재체를 외국에 의존하는 현행 방식은 개선이 필요하다. 지금부터라도 향후 10년 정도 이후에 발사될 위성을 대상으로 하는 구체적인 센서와 탑재체 개발이 이루어져야 한다. 특히 국가 안보적 측면에서 보면, 센서 기술의 취약성으로 타국의 위성역량을 우리가 파악하기는 쉽지 않다. 센서 기술의 취약은 타국에 비해 우리가 손에 쥘 정보 역량이 뒤떨어지는 것이어서 위성기술이 아무리 발전하더라도 센서기술 확보 없이는 정보 역량 향상을 기대하기 어렵다. 따라서 지구관측위성을 포함한 안보 측면에서 중요한 센서에 대한 기술 확보계획이 수립되고 전문조직에서 장기적으로 이를 축적해 나아갈 필요가 있다.

나. 탑재체 서브시스템 개발 방안

(1) 안테나 서브시스템

안테나 서브시스템 개발 관련 기본개념은 다음과 같다. 지구로부터 복사되는 에너지를 수신하기 위하여 반사기를 통하여 피드 혼으로 에너지를 전달하는 옵셋 파라볼릭 구조 형태이며, 안테나 빔 효율은 90~95% 이상 필요하다. 그리고 다중 피드 혼 클러스터로 설계하고 피드 혼에는 도파관을 사용하여 이중 편파 수신 및 수동 소자를 구성한다. 이때 주요핵심기술 개발 방안은 다음과 같이 접근한다. CFRP(Carbon Fiber Reinforced Plastics) 구조와 알루미늄 증착 기술을 사용한 경량 반사기 설계와 안테나 효율을 만족하기 위한 단일 또는 이중 개구 반사기를 고려하여 설계하는 방법과 다중 피드 혼 클러스터로 설계하는 방법이 있다. 위성

부분품 설계안은 다음 [표 6]과 같다.

[표 6] 위성 안테나 부분품 설계 방안

구분	설계 내용
반사기	• CFRP 허니콤 구조와 알루미늄 증착, 95% 이상의 안테나 효율을 갖는 피드 혼과 반사기 구조
피드 혼	• 주파수에 따른 피드 혼 클러스터 구성 및 경량 구조, 하향 조사 및 멀티 피드 혼을 고려 설계
도파관 수동소자	• 주파수에 따른 수동 소자, 경량 구조 및 네트워크 설계
교정 타겟	• 심 우주 반사기는 안테나 효율을 고려하고 흑체 타겟은 1에 가까운 높은 흡수율을 고려한 설계

(2) 수신기 서브시스템

수신기 서브시스템의 기본개념은 다음과 같다. 저잡음을 갖는 수신기 설계가 필요하고 수신기 타입은 직접 검출 방식과 수퍼헤테로다인 방식으로 나뉘며 저잡음 증폭기의 사용 여부를 고려하여 설계한다. 수신기 서브시스템의 주요 핵심 기술은 저잡음 수신과 경량화를 위한 MMIC를 사용한 RF(Radio Frequency; 무선주파수) 블록기술이 필요하나 100GHz이상의 주파수는 MMIC 기술을 사용하기에는 제한이 있다. 수신기 서브시스템의 부분품 설계안은 다음 [표 7]과 같다.

[표 7] 수신기 서브시스템 부분품 설계 방안

구분	설계 내용
6~30GHz	직접검출 방식
50~60GHz	직접 검출 방식 및 디지털 스펙트로메터
89~95GHz	직접검출 방식
183GHz	수퍼헤테로다인 방식+저잡음 증폭기

(3) 전기회로 서브시스템

전기회로 서브시스템의 기본 개념은 다음과 같다. 수신기 서브시스템의 AD(Analog to Digital) 변환기 이후의 모든 전기적 신호처리, 데이터 포맷 및 저

장, 메카니즘 제어와 탑재체의 전력조절공급 기능을 제공하며, 전력 공급 장치, 탑재체 일반제어, 데이터 핸들링 장치, 하니스와 소프트웨어로 구성된다. 전기회로 서브시스템의 주요 핵심 기술은 탑재체 중량과 소비전력을 감소시키기 위하여 FPGA(Field programmable Gate Array)를 사용하고 수신기 서브시스템 채널들의 다중화를 위한 데이터 버스 시스템과 회전부의 간편성을 위한 우주용 슬립링 기술을 적용하여 확보한다. 전기회로 서브시스템의 부분체 및 구성품 설계안은 다음 표 8과 같다.

[표 8] 전기회로 서브시스템의 부분체 및 구성품 설계 방안

구분	설계 내용
다중화 장치	1553B나 CAN 버스 설계
회전부 전력 및 데이터 전송 장치	슬립링 사용 설계
DC(Direct Current)-DC 변환기	전력 조절 설계
데이터 처리장치	CPU(Central Processing Unit) 및 TM(Telemetry)/ TC(Telecommand)와 탑재 소프트웨어로 구성
신호 처리장치	데이터 처리 및 포매팅
모터조절 및 위치 검침 장치	모터 제어용 명령 및 모터 위치 검침 설계로 모터 검침은 리졸버를 사용.

다. 국내 기술 자립화 방안

지구관측위성용 수동형 마이크로파 및 SAR 탑재체는 아직 국내에서 우주급 개발 경험이 없다. 개별 특성상 만들 수는 있지만 정확도 및 성능 면에서 검증하고 확인할 수 있는 인프라가 구축되어 있지 않다. 그러므로 개발 경험이 있는 유수기업과 협력 개발을 통하여 기술 축적을 한 후에 개발하는 것이 타당할 것으로 사료된다. 지구관측위성용 수동형 마이크로파 및 SAR 탑재체 개발 모델은 다음과 같다.

실험 모델은 개별 구성품의 동작 및 알고리듬 개발을 위한 브레드보드 레벨 시험 개발용으로 사용한다. 수명 실험 모델은 스캔용 모터 시스템을 위해서는 동작 수명을 확인하기 위한 모델을 개발한다. 개발 모델(DM)은 상용 부품을 사용한 선행 개발 모델로 사용한다. 기능모델(EM)은 구조물을 포함하여 상용 부품을 사용

하여 데모를 할 수 있는 모델이다. 검증 모델(QM)은 군용 부품 이상을 사용한 검증을 위한 모델로 사용한다. 비행모델(FM)은 실제 비행에 사용되기 위한 모델이다.

5. 결론

범세계적으로 일어나는 중규모의 악 기상으로 인한 집중호우는 지난 35 년간 그 빈도가 2 배 상승한 것으로 나타나고 있다. 이러한 이상 기후 현상은 지구 온난화 등의 영향과 관계가 있는 것으로 이해되고 있다. 기후변화에 따라 증가되고 있는 자연재해는 인명 및 경제・사회적으로 막대한 피해를 주고 있다.

"기상+ST(Space Technology)+IT(Information Technology) 융합"의 결과물인 저궤도 지구관측위성 시스템은 저궤도 지구관측위성이 재해 관련인자 영상을 정확히 획득 할 수 있도록 고정밀 자세제어를 유지시켜 주는 위성체(Bus), 마이크로파 대역(3 MHz~300 GHz)에서 관측이 가능한 탑재체 센서, 지상에서 위성을 정교하게 제어하고 감시하는 위성관제시스템, 그리고 태풍, 산불, 화산폭발, 지진, 쓰나미 같은 재해 정보를 위성 및 지상무선망으로부터 수신・처리하여 재난 정보를 언제, 어디서나 정확하게 준 실시간으로 국민에게 전송하는 재해 재난 네트워크로 정의된다. 미국, 유럽, 러시아 그리고 중국은 저궤도 지국관측위성에 적외선, 마이크로파 대역 탑재체 센서 및 SAR를 탑재, 기상재해 인자를 관측하여 날씨예보에 필수적인 수치예보 모델의 주요입력 자료를 제공하고 있다.

국외 저궤도 지구관측위성 개발 현황을 살펴보면, 미국은 NOAA-19 위성에 적외선 영상기(AVHRR-3)와 적외선 탐측기(HIR-3), 수동형 마이크로파 탐측기(AMSU-A1/A2/B)를, 유럽은 METOP-A 위성에 수동형 마이크로파 탐측기(MHS)와 적외선 탐측기(IASI)를, 러시아는 METEOR-3M 위성에 적외선 영상기(Kllmaat)와 수동형 마이크로파 영상기/탐측기(MTVZA)를 탑재하여 기상관측을 수행하고 있다. 마지막으로 중국은 FY-3B위성에는 수동형 마이크로파 영상기(MWRI)와 적외선 탐측기(IRAS), 그리고 수동형 마이크로파 탐측기(MWHS)를

탑재하여 운용하고 있다.

이렇게 우주 선진국들이 마이크로파 대역 SAR 탑재체를 운용하는 저의는 가시광선 대역을 이용하는 광학 센서는 야간이나 구름 등이 끼어 있을 때 목표지역 촬영이 어렵지만 적외선 및 마이크로파 대역 탑재체 센서는 야간이나 악천후에도 관측이 가능하기 때문이다. 또한, 마이크로파 대역 탑재체 원천 기술은 진일보된 군사첩보위성 개발에 활용이 가능하다.

일본 정부는 일본을 먹여 살릴 '꿈의 10대 기술' 가운데 위성기술인 "위성(ETS-VIII, WINDS, Superbird-D)을 활용한 지진, 쓰나미 등의 자연재해 통합관측・감시시스템"을 선정하여 연구를 수행하고 있다.

우리나라 우주개발진흥세부실천계획(2010)에 의하면 기상 및 기후변화 감시위성이 "정지궤도" 복합위성에 국한되어 있어, 국민의 삶에 지대한 영향을 미치는 집중호우, 가뭄, 태풍, 황사, 산불 등 기상재해 예방 및 기후변화 분야의 역량을 강화하기 위하여 우리가 축적한 기상, ST, 그리고 IT의 융합을 통해 기상재해 및 재난에 대응하는 유용한 수단으로 활용할 수 있는 정책 대안이 필요하다.

정부는 범 부처가 합력하여 기상재해 및 재난으로부터 국민의 생명과 재산을 보호하기 위하여 정지궤도 위성뿐만 아니라 지구관측위성인 다목적위성 혹은 차세대 소형위성의 위성체(Bus) 모델을 이용하여 글로벌 기후변화에 대응할 수 있는 다양한 센서가 장착된 차세대 지구관측위성 탑재체 개발 체계 구축을 추진하여야 한다. 이를 위해서는 센서를 포함한 탑재체 기술 확보계획과 위성에 활용계획이 연동되도록 수립되고, 지구관측용 센서를 포함한 안보적 측면에서 중요한 센서의 설계기술, 요소기술을 축적하고 개발하는 전담조직을 만들거나 지정하여 장기적으로 운영할 필요가 있다. 센서기술은 4차 산업 혁명에서 핵심적 기술 가운데 하나로 센서기술 확보 없이는 새로운 산업 창출도 어렵다. 기후변화관측을 포함한 지상관측을 위한 각종 센서 개발이 우주공간활용, 안보적 활용, 새롭게 부상하고 있는 새로운 산업 활용과 불가분의 관계이기 때문에 센서개발과 센서활용을 연계하는 통합계획을 마련해 이를 실현할 필요가 있다.

참고문헌

은종원 외.『우리나라 위성통신 및 우주산업발전사』. 도서출판 영, 2011.

은종원・조황희.『ST-IT 컨버전스 위성통신융합기술』. 도서출판 영, 2014.

은종원.『우리나라 위성산업 경쟁력 제고 방안에 관한연구』. 통신위성우주산업연구회논문지, 8(1), 2013.

은종원 외.『국가환경위성센터 효율적 관리 방안』. 국립환경과학원, 2015.

Alasdair McLean. “PFI in the Sky, or Pie in the Sky? – Privatising Military Space.” *Space Policy*, vol. 15, no.4(November 1999).

David A. Newell, Gary Rait, Thach Ta, Barry Berdanier, David Draper, Michael Kubitschek. “GPM microwave imager design, predicted performance and status.” in Proc. *IGARSS* (2010), pp. 546~549.

D. B. Kunkee, G. A. Poe, D. J. Boucher, S. D. Swadley, Y. Hong, J. E. Wessel, and E. A. Uliana. “Design and evaluation of the first Special Sensor Microwave Imager/Sounder,” *IEEE Trans. Geosci. Remote Sens.*, vol. 46, no.4 (Apr. 2008), pp. 863–883.

P.W. Gaiser et al.. “The WindSat spaceborne polarimetric microwave radiometer: Sensor description and early orbit performance,” *IEEE Trans. Geosci. Remote Sensing*, vol. 42, no. 11 (Nov. 2004), pp. 2347–2361.

稻畑 廣行, 三菱電機宇宙事業の海外展開と國への期待について, *Space Japan, Review*, No. 74 (June/July 2011).

http://www.mod.go.jp/j/procurement/pfi/siryou/xband.pdf (검색일: 2012.11)

http://directreadout.noaa.gov/miami04/docs/weds/Pete_Wilczynski.pdf(검색일: 2012.12)

http://nmsc.kma.go.kr/jsp/homepage/contents/chollian/choll_info.jsp(검색일: 2016.10)

Abstract

A Feasible Acquisition Method of the Next Generation Earth Observation Satellite Payload Systems for Dealing with Global Climate Change.

Jong Won Eun (Namseoul University)

Space industry is a future core technology which is emerging as the most competitive industry in the 21st century. However, it is said that private enterprises may have some limitations to running the space business independently because the space industry requires not only to spend enormous amount of investments at the beginning stage of business but also have difficulties to get the correct amount of investments in a short period of time. These days, satellite core technologies are being developed as a way to provide various information by considering simultaneously sending, wide area covering, highly precide, and anti-disaster technologies. Also, space technologies are being convergently developed in the different technological fields such as information and communication, global positioning, and image. The Earth observational information service based on the space technologies has some characteristics to be connected with the fields of space development. Several advanced countries are achieving the next generation earth observation satellite technologies through their space development programs. Such a trend and change of satellite technologies, Korean government has realized the necessity for the domestic independent development of next generation of earth observation satellites, and are preparing the profound items such as detailed implementation plans. This paper is to provide a feasible acquisition method of the

next generation Earth observation satellite payload which should be developed in Korea in order to provide accurate information related to global climate change as well as to contribute to the enhancement of the Korean people's happiness index, welfare, and safety.

Key Words: Next Generation Earth Observation Satellite Payload, Future Core Technology, Domestic Independent Technology, Global Climate Change

투고일 : 2016.11.10. 심사일 : 2016.11.20. 게재확정일 : 2016.12.10.

필진 소개

(게재순)

곽덕환

현 한남대학교 교양대학 교수. 중국 푸단대에서 국제정치학 석, 박사학위를 받았으며, 주요 논문은 “중국의 대미 관계 변화 연구”, “중국의 대북한 외교 관계 변화 연구”, “중국의 대러시아 외교 관계 변화 연구” 등이 있음.

전완주

현 국가안보전략연구원 수석연구위원. KAIST에서 항공우주공학박사 학위를 받았으며, 주요 논문으로 “최근 일본의 우주개발 확대 동향과 특징고찰”, “최근 중국의 우주개발 강화 동향과 美·日의 대응동향 평가”, “중국의 범지구적 위성항법시스템 구축배경과 파급영향 고찰”, “최근 중국의 우주개발 확대 동향과 특징 고찰” 및 “美·日의 지역 위성항법시스템 공동개발 동향과 추진배경·의도 분석” 등 다수 있고, 주요 연구보고서로는 “동서독간 전략물자 수출통제 현황 및 시사점 연구” 등 다수 있음.

윤봉한

현 국가안보전략연구원 책임연구위원·동국대학교 국제정보대학원 겸임교수. 미국 펜실베니아 주립대학교(Pennsylvania State University)에서 석사, 고려대학교에서 박사학위를 받았음. 주요 논문으로 “소셜미디어를 이용한 외로운 늑대 테러리스트의 급진화에 관한 연구”(2015), “국내에서의 외로운 늑대 발생 가능성에 관한 연구”, “사이버공간에서의 외로운 늑대 테러리스트의 급진의식화 실태에 관한 연구” 등이 있음.

이창주

현 성균관대학교 초빙교수. 현 국가안보전략연구원 연구위원(비상근). 한국외국어대학교 법과대학 법학사, 성균관대학교 대학원 정치학 석사, 한국외국어대학교에서 법학 박사 학위를 받았음(행정법). 연구분야는 정보공개법, 정보보호 관련법, 위기관리 및 재난관리, 정책학 등. 주요 저서 및 논문은 “미국에서의 국가안전보장 관련 정보 공개 제한에 관한 연구”(2013) 등이 있음.

이영환

현 건국대학교 경영대학 기술경영학과 조교수, 공공데이터제공분쟁조정위원회 조정위원, 현 W3C 블록체인커뮤니티그룹 공동의장, 한국데이터사이언스학회 특임이사, 한국강소기업진흥학회 수석부회장, 한국금융ICT융합학회 부회장. 미국 일리노이대학 컴퓨터학과에서 인공지능학으로 박사학위를 받았음. 주요 저술서는 "웹 3.0세상을 바꾸고 있다" (단독저술, 2010), 주요 논문으로는 "Nation Image and its Dynamic Changes in Wikipedia" (공저, 2017), "국가이미지 분석을 위한 위키피디아 실시간 동적 온톨로지 구축 알고리즘 및 적용" (단독저술, 2016) 등이 있음.

김찬우

현 영남대학교 통일문제연구소 연구원, 오피니언라이브 빅데이터분석센터 책임연구원. 영남대학교 정치외교학과에서 박사학위를 받았으며 2014년 4월부터 2016년 5월까지 더아이엠씨 데이터사이언스연구소 책임연구원으로 재직하였음. 주요 저술로는 2013년 "산업표준 보유 및 표준화 활동 추이로 본 한국 산업표준 정책의 특징과 변화", 2016년 "빅데이터를 기반으로 한 MISP의 소비자 평가 및 니즈 분석(우수논문발표상 포스터부문)" 등이 있음.

은종원

현 남서울대학교 정보통신공학과 교수. 미국 유타주립대학교에서 전자물리학 박사학위를 받았음. 미항공우주국 NASA 선임연구원, 한국전자통신연구원(ETRI) 책임연구원, 한국과학재단우주전문위원, World DMB 부회장, 산업클러스터학회부회장, 통신위성우주산업연구회장 등 역임. 현재 ICT 프레스 클럽 전문위원으로 활동 중. 주요 저서 및 논문으로 『ST-IT 컨버전스 위성통신 융합기술』(공저 2014), 『위성 지상국 융합기술- 지구관측위성을 중심으로』(공저 2016), 『환경위성지상국 시스템 가용도 예측분석 연구』(공저 2016), "A Microstrip Dual-Band Bandpass Filter Using Feed Line with SIR"(공저 2017) 등 다수의 연구가 있음.

최근 발간자료 안내

2015

| 봄호 |

1. 한국 공공분쟁의 특징과 해결방안 : 정부 관료의 역할을 중심으로 최영진
2. 독일 '통일정책'의 한국적용의 의미와 방안
   : 프라이카우프, 잘츠기터, 연대세를 중심으로 김종수
3. 미중 양대강국체제의 부상과 한국의 중견국 외교 전략 차정미

| 여름호 |

1. 북한에서의 불평등 이양호
2. 세계 각국의 군사력 효율성 측정과 개선
   : DEA-Tier 분석을 통한 벤치마킹 정보의 도출 서호준
3. 21세기 전염병과 보건안보 : 국가안보의 시각을 중심으로 조성권
4. 국방부 군종교 제도의 효율적 운용방안: 군 민간성직자 활용을 중심으로 전요섭
5. 통일대비 북한이탈주민 창업 활성화를 위한 정책과제 조봉현
6. 나선지역에서 다국적 산업단지 개발의 가능성 분석 조유현

| 가을호 |

1. 북한의 사이버 공격 대응을 위한 효과적인 법정책 모색 오일석 · 이승열 · 김소정
2. 전쟁과 평화 : 미국전쟁 수행방식의 '반정치적'성향을 사례로 이현휘
3. 한미동맹의 재조정과 주한미군 평택 재배치에 대한 고찰 윤지원
4. 북 '약한 민족주의, 강한 실리주의' : 젊은 세대 낮은 통일의식의 원인과 시사점 심양섭 · 지창호
5. 계파정치 극복을 위한 네트워크 정당모델과 오픈 프라이머리 논의 채진원

| 겨울호 |

2016

| 여름호 |

『신안보연구』 원고모집

국가안보전략연구원은 학술지 『정책연구』를 2016년부터 『신안보연구』로 제호를 변경해서 연 2회(6·12월) 발간하고 있습니다. 『신안보연구』는 사이버·테러·보건안전·기후·환경·재난·위기관리, 난민문제 등 새로운 안보 이슈를 중심으로 한 논문을 수록합니다.

저희 연구원은 이 분야의 학술 및 연구활동에 종사하시는 분들의 논문기고를 환영합니다. 보내주시는 기고문은 소정의 심사를 거쳐 게재하고, 채택된 원고에 대하여는 소정의 원고료를 지급합니다. 저희 연구원은 시사 또는 학술적인 내용으로 독창적이고 정책대안이 담긴 논문을 선호합니다. 단, 다른 곳에 게재되지 않았거나 게재될 계획이 없는 논문이어야 합니다.

기고문은 200자 원고지 150매 내외를 기준으로 『신안보연구』 기 출간문을 참고하여 작성하시되 600자 내외의 서술식 국·영문 요약문도 작성해 주셔야 합니다. 기고문은 최종원고와 요약문을 기고자의 연락처와 함께 편집위원회 E-mail 주소(policy@inss.re.kr)로 보내주시기 바랍니다.

『신안보연구』 편집위원회

The Studies of New Security Challenges

Institute for
National Security Strategy

ISSN 2508-2728