# 세계 각국의 사이버 안보 전략과 우리의 정책 방향-미국을 중심으로[1)]

이 강 규*

ICT의 발전과 안보 개념의 확장으로 사이버 안보의 중요성이 대두되고 있다. 그러나 우리나라는 아직 통합적이고 체계화된 사이버 전략을 가지고 있지 못하다. 최근 미국을 비롯한 ICT 주요국들은 사이버 안보에 대한 자국의 전략을 내놓고 있는 바, 이에 대한 이해는 우리의 사이버 안보 전략의 정립에도 도움이 될 것으로 사료된다. 미국은 올해 두 가지 보고서를 통해 전통적인 안보에 관한 논의내용과 논리를 사이버 공간으로까지 확장하는 동시에, 미국의 이익이 반영된 사이버 공간의 국제규범 정립을 강조하였다. 영국, 일본, 독일, 호주 등도 자국의 이익에 기초하여 자국의 특성이 반영된 전 방위적이면서도 국제협력을 강조하는 정책을 제시하고 있다. 이에 따라 우리나라도 우리의 ICT 현실과 그에 따른 국가이익을 반영한 정부 차원의 포괄적이면서도 체계적인 사이버 안보전략 수립을 마련하여야 할 것이다.

## 목 차



* 한국국방연구원 안보전략연구센터 연구원, (02)961-1814, kangkyulee@kida.re.kr

1) 본 글의 내용은 연구자의 개인적인 견해이며, 소속 연구원의 공식적인 입장이 아님을 밝힙니다.

# Ⅰ. 서 론

ICT 기술의 발전과 급속한 확산으로 우리 생활에서 ICT가 차지하는 비중이 점점 증대되고 있다. 즉, ICT의 활용은 단순한 생활의 일부가 아니라 생활 전체에 투영되고 있으며, 이에 따라 사이버 공간(cyberspace)이라는 가상의 공간도 더욱 활성화되었다(Jordan, 1999, pp.1~7). 더불어, 사이버 공간과 현실 공간의 간극이 점점 엷어지면서 기존의 현실 공간에서 다루어졌던 많은 이슈들이 사이버 공간으로까지 확산되어 가고 있다.

안보 개념이 사이버 영역으로 확장된 사이버 안보도 이러한 맥락에서 파악할 수 있다. 안보의 개념 자체가 매우 복잡하고 어려운 개념이지만(Baldwin, 1997, pp.12~17), 국가 안보가 중시되던 냉전기 이후에는 인권, 환경, 에너지, 테러 등이 새로운 안보 영역으로 등장하였고(정상화, 2010, pp.10~16; 장의관, 2005, pp.26~41), ICT의 발전으로 안보의 영역이 사이버 공간으로까지 확장되었다. 사이버 안보는 개인, 기업, 국가, 국제기구 등이 행위주체가 될 뿐만 아니라 군사, 정치, 경제, 사회 등 전 분야를 포괄한다(서동주, 2008, p.11). 예컨대, 스턱스넷(Stuxnet) 웜 바이러스의 이란 핵 시설 공격, 우리나라의 2009년 분산 서비스거부(DDoS) 공격 및 최근의 2011년 농협 사이버 테러 사태 등과 같은 사이버 공격은 사이버 공간에만 한정되는 문제가 아닐뿐더러 피해의 정도도 생활의 불편을 넘어 실제적이고 직접적으로 영향을 미칠 정도로 점차 강해지고 있다.

그럼에도 불구하고 우리나라에는 아직까지 통합적이고 체계적인 국가 차원의 사이버 안보 전략이 부재한 실정이다. 국정원 주도의 국가 사이버 안전 전략회의를 통해 사이버 안보 마스터플랜이 마련될 예정이나, 이는 사이버 안보와 관련된 첫 번째 산물이라는 점에서 어느 정도까지 포괄적이면서도 동시에 구체적인 내용을 담을 수 있을지 의문스럽다. 한편, 우리나라에는 각국의 사이버 안보 대응에 관한 기초적인 내용의 소개도 미흡한 실정이다.[2)]

2) 대표적인 예로 해마다 출간되는 《국가정보보호백서》(방송통신위원회 외)와 한국인터넷진흥원의 《인

이에 따라 본고에서는 미국을 중심으로 주요국의 사이버 안보 전략을 통해서 사이버 안보 대응과 관련한 글로벌 동향을 파악하고, 이를 바탕으로 우리의 사이버 안보 전략에 대한 기본 방향을 제시하고자 한다.

# Ⅱ. 미국의 사이버 안보 전략

## 1. 오바마 행정부의 등장과 사이버 안보의 적극적 강조

사이버 안보에 대한 관심이 오바마 행정부의 등장으로 시작된 것은 아니다. 전임 부시 대통령 시절에도 'THE NATIONAL STRATEGY TO SECURE CYBERSPACE' (2003년 2월) 등 사이버 안보와 관련한 보고서를 발표하면서 선도적인 입장을 보였다.[3] 하지만 오바마 대통령 취임 이후에는 보다 적극적인 태도를 보여, 사이버 안보를 국가 안보의 중요한 일부분으로 간주하고 있으며 소극적인 방어에서 한 걸음 나아가 적극적인 대응으로 변화하는 모습을 보여주고 있다. 그 대표적인 예가 사이버 안보 관련 보좌관 직위를 신설한 것과 사이버 사령부의 창설이다.

오바마 대통령은 2009년 사이버 안보 관련 보좌관을 신설하여 초대 짜르(czar)로 부시 전 대통령 때 사이버 보좌관이었던 하워드 슈미트(Howard A. Schmidt)를 임명하였다. 더불어 4성 장군을 사령관으로 하는 사이버 사령부(U.S. Cyber Command, USCYBERCOM)를 2010년 5월에 신설하였다. 미 사이버 사령부는 전략 사령부(U.S. Strategic Command, USSTRATCOM)에 속하며, 육군 사이버 사령부(Army Cyber Command, ARCYBER), 제24 공군(24th USAF), 함대 사이버 사령부(Fleet Cyber Command, FLTCYBERCOM), 해병 사이버 사령부(Marine Forces Cyber Command:

---

터넷&시큐리티 이슈》에 주요국의 사례가 포함되어 있긴 하지만, 극히 적은 분량이 담겨있을 뿐이다. 따라서 본고에서는 사이버 안보에 가장 적극적인 미국을 비롯하여 가급적 다양한 국가들의 사이버 안보 전략을 소개하는 데 의의를 두고자 한다.

3) 동 보고서에서는 미국의 핵심 기초시설에 대한 사이버 공격의 예방, 사이버 공격에 대한 미국의 취약성 감소, 사이버 공격으로 인한 피해와 회복 기간의 최소화를 목표로 하고 있어, 다소 소극적이고 방어적인 전략을 취하고 있음을 알 수 있다.

MARFORCYBER)로 구성된다.[4)]

이외에도 미국은 정부 차원의 보고서를 통해 사이버 안보에 대한 접근 방법과 미국의 입장을 정립하는 데 노력하고 있다. 즉, 기존의 사이버 정책을 재고하고, 새로운 정책 마련을 위해 2009년에 '사이버 정책 검토 보고서'(Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure)를 내놓았으며, 이를 기반으로 올해 5월 16일에 '사이버 공간에 대한 국제 전략: 네트워크 세계에서의 번영, 안보 및 공개성'(International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World 이하 ISC) 보고서를 발표하였다. 또한 국방부 차원에서는 이례적으로 7월 14일에 '사이버 공간에서의 국방부 작전 전략'(Department of Defense Strategy for Operating in Cyberspace, 이하 SOC)을 공개하였다. 이하에서는 최근에 공개된 두 가지 보고서를 중심으로 미국의 사이버 안보 전략에 대해 살펴보도록 한다.

## 2. 미국의 사이버 안보 전략의 주요 내용[5)]

### (1) 사이버 공간에 대한 국제 전략 보고서(International Strategy For Cyberspace)

'사이버 공간에 대한 국제 전략 보고서'는 사이버 공간 정책 수립, 사이버 공간의 미래, 정책 우선 사항, 향후 방향의 4개 장으로 구성되어 있다.

먼저, 사이버 공간에 대한 전략적 접근방법에 대해서 미국은 네트워크 기술이 미국과 전 세계에 막대한 잠재력을 지니고 있다는 데에 국제 사이버 공간 정책의 기반을 두면서 성공적인 성취에 기초하고, 도전과제를 인식하며, 원칙에 따라 대응해야 한다고 밝히고 있다. 여기서의 원칙은 표현의 자유 등의 자유를 존중하고, 프라이버시를 보호하며 정보의 자유로운 이동을 보장하는 것을 말한다. 그리고 성공적인 성취는 디지털 네트워크를 통해 우리 사회와 경제가 큰 이득을 얻어왔다는 점을 중시한다는 것

4) www.stratcom.mil/factsheets/Cyber_Command, 접속일: 2011. 5. 10.

5) 본 절의 내용은 두 가지 보고서를 요약 및 정리한 것으로 이강규(2011), 미국 사이버 전략 보고서를 통해 본 우리의 사이버 안보 전략 수립 방향, 《주간국방논단》(未刊)의 내용을 보완한 것이다.

이다. 도전과제의 인식은 이러한 성취와 동시에, 미국의 국가 안보 및 경제 안보뿐 아니라 국제사회와 관련하여 기술적 문제, 지적재산권 도용 등의 새로운 도전을 가져다 줄 수 있다는 점을 말한다. 특히, 전통적인 방식의 갈등이 사이버 공간으로 확대되면서 국제평화와 안보를 위협하고 있다는 점을 지적하고 있다(ISC 2011, pp.4~5).

그리고 해당 보고서는 사이버 공간의 미래에 대한 제시에 대해서 "사이버 공간에 대한 접근과 이용에 경제적 또는 기술적 제약이 없어야 한다는 점을 강조하면서, 미국의 목표는 개방적이고(open), 상호운용이 가능하며(interoperable), 안전하고(secure), 신뢰할 만한(reliable) 정보와 통신 기초시설을 증진시키기 위해 국제적으로 노력하는 것"이라고 밝혔다(ISC 2011, p.8). 또한 이러한 정보와 통신 기초시설을 통해 국제무역 및 거래를 지원하고 국제안보를 강화하며 표현의 자유와 혁신을 고양할 수 있을 것으로 예상하고 있다. 한편, 이러한 목표를 달성하기 위해서 미국은 책임 있는 행동 규범(norms of responsible behavior)에 따라 국가들이 행동하도록 하고, 협력관계를 지속하며 사이버 공간에서의 법의 지배(rule of law)를 지원하는 환경을 구축하고 유지할 것이라고 밝히고 있다(ISC 2011, pp.8~9).

규범과 관련하여서는 전통적인 원칙과 신규 원칙을 설명하고 있다. 전통적인 원칙으로는 표현과 결사의 자유 등 근본적인 자유를 견지하고(upholding fundamental freedoms), 재산권을 존중하며(respect for property), 프라이버시를 중시하고(valuing privacy), 범죄에서 보호하며(protection from crime), 자위권(right of self-defense)을 행사할 수 있다고 언급한다. 특히, 사이버 공간에서 자위권 개념을 언급한 것이 특징적인데, 본 보고서에서는 "유엔 헌장에 부합하는 방식으로 국가는 사이버 공간에서의 특정 공격 행위(aggressive acts)에 대항하는 고유한 자위권을 보유한다."고 밝히고 있다(ISC 2011, p.10).

또한 보고서에서는 신규 규범과 관련하여 글로벌 상호운용성(global interoperability), 네트워크 안정성(network stability), 신뢰할 만한 접근성(reliable access), 다중 이익관계자의 관리(multi-stakeholder governance), 사이버 안보의 충분한 주의의무(cybersecurity due diligence)를 거론하고 있다. 이 중에서도 사이버 안보의 충분

한 주의 의무란 국가가 손상(damage)이나 오용(misuse)으로부터 정보 인프라를 보호하고, 국가 시스템의 안전을 확보하는 데 있어서 자신들의 책임을 인식하여 이에 따라 행동해야 한다는 것을 말한다(ISC 2011, p.10).

이에 따라 미국은 사이버 공간의 미래에 있어서 자신의 역할을 외교(diplomacy), 국방(defense) 및 개발(development)의 3D 영역에서 밝히고 있다. 외교에서는 협력관계(partnership)의 강화를 강조하고 있다. 외교적 목표를 "개방적이고, 상호운용이 가능하며, 안전하고, 신뢰할 만한 사이버 공간의 본래적인 가치를 인식하면서 국가들이 협력하고 책임 있는 이해상관자로서의 역할을 하는 국제 환경에 대한 컨센서스(consensus)를 구축하도록 유도하는 데 노력"하는 것이라고 밝혔다(ISC 2011, p.11). 이러한 목표 하에 같은 생각을 가진 국가들과 명확한 합의를 이끌어내는 것을 시작으로 사이버 규범 정립을 위해 양자적이나 다자적인 협력관계를 강화하고, 국제기구 및 다자적인 조직들과 협력하고 있다. 협력의 대상에는 민간 분야, 학계, 시민사회 등이 망라되어 있다. 특히, 네트워크 생태계의 안전 등에 있어서 민간 분야와의 협력을 중요하게 여기고 있다(ISC 2011, p.12).

국방 분야에 있어서는 우선 네트워크 및 시스템을 파괴하고자 하는 사람들에 대해 다른 나라들과 함께 대항하면서 책임 있는 행동을 고양하고, 필요성(necessary)과 비례성(appropriate)을 유지하면서 악의적인 행위자를 억지(dissuading)하고 억제(deterring)하며, 이들 국가의 핵심 자산에 대한 자위권을 보유하는 것을 목표로 삼는다고 밝히고 있다. 여기서 억지는 국내적으로 민간과 전체 정부 부분이 합심하여 정보 시스템과 네트워크 복구 능력 등을 확보하며, 국제적으로 기술 및 군사 분야의 협력을 발전시켜 네트워크에 대한 공격에 대응하는 것이다. 그리고 억제에 있어서는 국내적으로 국가 안보 및 경제 안보를 위협하는 범죄자와 비국가 행위자에 대해 모든 국가가 사법권을 행사하며, 국제적으로는 법 집행당국 간의 공조와 법제화 등을 협력하는 것을 의미한다. 또한 사이버 공간의 적대행위에 대응하기 위해 미국은 군사협력관계에 있는 국가들과 공조하고, 외교, 정보, 군사 및 경제 등 국제법적으로 허용되는 모든 수단을 동원할 권리를 지니고 있다고 하면서도 군대는 가장 마지막 수단이 될 것이라

고 말하고 있다(ISC 2011, p.12~14).

끝으로, 개발과 관련하여 기술 능력과 사이버 안보 능력의 구비 및 정책관계의 확립을 강조하고 있는데, 이의 기본적인 목표는 국가별 양자 및 다자기구를 통해 해외에서 사이버 네트워크를 강화하며 보다 긴밀한 협력관계를 구축할 수 있도록 노력하는 것이다. 또한 이러한 노력은 앞서 언급한 개방적이고, 상호운용적이며, 안전하고, 신뢰할 만한 네트워크에 대한 공감에 기초한 것이다(ISC 2011, pp.14~15).

한편, 사이버 공간의 미래를 위한 정책적 우선 사항은 다음과 같은 내용을 제시하고 있다. 앞서 미래의 사이버 공간을 위한 목표를 실현하기 위해 미국은 경제, 사법 등에서의 중점 사항을 제시하고 있다. 경제적으로는 국제표준(international standards), 혁신역량(innovative), 공개 시장(open market)을 증진하고, 네트워크 보호를 위해 보안 능력, 신뢰성 및 복원력(resiliency)을 확보하며, 법집행에 있어서 공조와 법치를 확대해야 한다고 밝히고 있다. 또한 효과적이고 포괄적인 구조를 통해 인터넷 관리를 증진하고, 근본적인 자유들과 프라이버시를 뒷받침하는 인터넷 자유를 구축해야 한다고 주장한다(ISC 2011, pp.17~24).

이 중에서 흥미로운 몇 가지만 살펴보면, 네트워크 보호에 있어서는 먼저 ASEAN, ARF, APEC, OECD, UN 등의 다자기구에서 사이버 안보를 다루기 위한 노력을 계속 촉진하고, 사이버 공간의 활동에 관한 지역 및 국제적인 합의를 위한 노력을 계속해 나가야 한다고 말하고 있다. 또한 미국 네트워크에 대한 침투와 네트워크 분열(network disrupting)을 감소시키고, 정보 기초설비의 사고관리(incident management), 복원력(resiliency) 및 복구력(recovery)을 확보해야 한다고 주장한다. 끝으로 업계와 협력하여 보안에 대한 첨단기술의 공급사슬(supply chain)을 향상시킬 것을 주문하고 있다. 이러한 공급에는 소프트웨어 및 하드웨어가 모두 포함된다(ISC 2011, pp.18~19).

인터넷 관리(Internet governance)에 있어서는 인터넷의 개방성과 혁신성을 가장 중요시해야 한다고 언급하고 있다. 특히, 일부 국가들이 자의적인 정당성을 기준으로 정보의 자유로운 이동과 정부에 반대되는 활동을 제한하는 것을 비판하고 있다. 한편, DNS를 비롯한 글로벌 네트워크의 보안성과 안정성을 확보해야 하며, 인터넷 관리에

있어서 복잡하게 얽혀 있는 이해관계자들에게 논의의 장을 제공하도록 노력해야 한다고도 밝히고 있다(ISC 2011, pp.21~22).

군사 분야와 관련해서는 21세기의 안보 도전을 준비하기 위해 첫째, 군사 분야에서 신뢰할 수 있고, 안전한 네트워크의 필요성이 증대되고 있다는 사실을 인식하고 받아들여야 한다는 것이다. 둘째로는 사이버 공간에서의 잠재적인 위협에 대응하기 위해 기존의 군사동맹을 활용하고 발전시켜야 한다고 주장하고 있다. 즉, 사이버 안보는 일국의 능력으로 대처할 수 없기 때문에 군사동맹과 협력을 강화하여 집단 억제 능력(collective deterrence capabilities)을 강화해야 한다는 것이다. 끝으로, 집단 안보를 강화하기 위해 동맹국 및 협력국과의 사이버 공간에서의 협력을 확대해야 한다고 보고 있다(ISC 2011, pp.20~21).

마지막으로 인터넷 자유에 있어서는 인터넷이 신뢰할 수 있고 안전한 표현과 결사의 자유를 위한 장(platform)이 되도록 시민사회의 행위자들을 지원하고, 시민사회 및 NGO의 인터넷 활동을 불법적인 디지털 침입(digital intrusion)에서 보호하기 위해 이들과 협력하여 안전장치를 마련해야 한다고 밝히고 있다. 또한 상업 데이터의 프라이버시 보호를 위해 국제공조를 증진하고, 자유로운 인터넷 접속을 위해 종단 간(end-to-end) 상호운용성을 확보해야 한다고 강조한다(ISC 2011, pp.23~24).

### (2) 사이버 공간에서의 국방부 작전 전략(Department of Defense Strategy for Operating in Cyberspace)

'사이버 공간에서의 국방부 작전 전략' 보고서는 2010년 '국가 안보 전략'(National Security Strategy)과 2010년 '4년 주기 국방검토 보고서'(Quadrennial Defense Review Report)의 사이버 안보 관련 내용에 기초하여 5가지 전략적 이니셔티브(Strategic Initiative)를 제시하고 있다. 하지만 기본적인 방향은 ISC의 영향을 보다 직접적으로 받았을 것으로 판단된다. 왜냐하면 양 보고서의 작성 시기가 유사하고, ISC가 공개된 후 SOC에 대한 내용이 언론을 통해 일부 공개되었기 때문이다.[6] 특히, '사이버 국방

6) "Cyber Combat: Act of War"(2011. 5. 31), THE WALL STREET JOURNAL. 한편, 보고서의

전략' 발표 시에 윌리엄 린(William Lynn) 미 국방부 차관이 언급한 '사이버 공격에 대한 군사적 대응'은 ISC에서 기술된 내용이라는 점에서 더욱 그러하다. 다만, 본고에서 살펴보는 보고서는 공개용으로 이보다 2배 정도 분량의 비공개용 보고서에는 구체적인 대응 전략과 함께 군사적 대응에 따른 논란이 보다 자세하게 논의되었을 것으로 추측된다. 이하에서는 SOC에서 제시된 전략적 이니셔티브를 중심으로 살펴보도록 한다.

〈표 1〉 전략적 이니셔티브의 주요 특징

| 구 분 | 주요 특징 |
|---|---|
| 전략적 이니셔티브 1 | 사이버 공간을 새로운 작전 영역(domain)으로 천명 |
| 전략적 이니셔티브 2 | 사이버 보안(cyber hygiene) 강조 |
| 전략적 이니셔티브 3 | 전(全) 정부 차원(whole-of-government)의 총력 대응 |
| 전략적 이니셔티브 4 | 동맹국, 협력국 및 민간 영역과의 협력 |
| 전략적 이니셔티브 5 | 우수 인력 확보와 지속적인 장비 업그레이드 |

자료: "Department of Defense Strategy for Operating in Cyberspace", 2011.

첫 번째 전략적 이니셔티브는 "사이버 공간을 국방부가 사이버 공간의 잠재력(potential)을 최대한 이용할 수 있도록 조직하고(organize), 훈련하고(train), 장비를 갖추도록 하는(equip) 작전 영역(operational domain)으로 간주한다."는 것이다(SOC 2011, p.5). 이를 위해 전략 사령부(USSSTRATCOM) 산하에 사이버 사령부(USCYBERCOM)를 만들고, 사이버 사령부의 사령관이 국가안보국(NSA) 국장을 겸임토록 하였다. 보고서에서는 사이버 사령부의 역할에 관해서는 훈련, 정보보호(information assurance), 상황인식(situational awareness), 네트워크 복원력과 네트워크 안보 확보 등을 통해 사이버 공간의 위험을 관리한다고 밝히고 있다. 또한 COP(Common Operating

공개가 특정 언론을 통해서만 이루어졌다는 점과 언론 공개 이후부터 실제 보고서 공개까지 일정 정도의 시차가 있었다는 점에서 각계의 반응에 따라 중요 내용에 대한 내부적인 토론과 수정이 이루어졌을 것으로 생각된다.

Picture)를 유지하고 집단적 자위를 구축하며, 협력관계를 형성하여 보존성(integrity)과 가용성(availability)을 확보하는 것도 사이버 사령부의 역할로 들고 있다. 끝으로는 전투 사령부·지원부서 등과 긴밀히 협력하여 적재적소에 혁신적 능력을 신속히 투입하여 통합 능력(integrated capabilities)을 개발하기 위해 노력해야 한다고 제시하고 있다(SOC 2011, pp.5~6).

두 번째 전략적 이니셔티브는 '국방부 네트워크 및 시스템을 보호하기 위해서 새로운 국방(defense) 작전 개념을 채용'하는 것이다(SOC 2011, p.6). 보다 구체적으로는 '사이버 보안(cyber hygiene)'을 강화하고, 내부 위협을 억지하고 완화하기 위해 인력의 통신, 책임, 내부 감시 및 정보관리 능력을 강화하는 것을 말한다. 또한 국방부 네트워크와 시스템에 대한 침입을 방지하기 위해 적극적인 사이버 방어 능력을 구비하여 새로운 방어 작전 개념을 개발하고 구조설계를 전산화(computing architecture)하는 것을 뜻한다(SOC 2011, p.6~7). 이러한 전략은 보안에 취약한 프로그램의 지속적인 업데이트와 보안 프로그램 등의 활용 등 개인들의 활동과 주의를 강조하고 있는 것으로 보인다. 다만, 새로운 작전 개념에 대해서는 구체적인 내용이 제시되지 않고 있다. 직원들의 보안 의식 제고에 목적을 두었다는 점에서 직원들이 사용하게 되는 새로운 형식의 보안 시스템일 수도 있고, 교육 방식일 수도 있을 것으로 예상된다.

세 번째 전략적 이니셔티브는 "미국의 기타 정부기관 및 기구 그리고 민간과 협력하여 전(全) 정부 차원(whole-of-government)의 사이버 안보 전략이 가능하도록 한다."는 것이다(SOC 2011, p.8). 이는 네트워크를 대상으로 하고 네트워크를 통해 확산되는 사이버 공격의 특성상 어느 한 부문을 통제한다고 해서 문제를 해결할 수 없다는 인식이 반영된 당연한 결과로 보인다.

네 번째 전략적 이니셔티브는 "미국의 동맹국 및 우방국들과의 관계를 공고하게 하여 집단적 사이버 안보를 강화한다."는 것이다(SOC 2011, p.9). 이는 세 번째 이니셔티브와 맥락을 같이한다. 일국 내에서의 협력도 중요하지만, 전 세계가 그물망처럼 얽혀 있는 정보화 시대에는 어느 일국의 능력만으로 사이버 공격을 방어하고, 주변국 또는 기타 국가로의 파급을 방지한다는 것이 쉽지 않기 때문이다. 이 부분에서는 ISC

의 내용을 언급하면서 집단적 자위권과 집단적 억지(collective deterrence)를 강조하고 있다. 특히, 사이버 공격의 경우 자료를 파악하기가 기술적으로 곤란한 경우가 많기 때문에 이러한 측면에서 타국과의 협조와 공동 훈련 등을 통한 대응 능력의 배양이 절실히 요구된다.

마지막 전략적 이니셔티브로는 "우수한 사이버 인력과 신속한 기술 혁신을 통해 국가의 능력(ingenuity)을 배가(leverage)한다."고 밝히고 있다(SOC 2011, p.10). 사이버 안보의 특성상 개인의 역량에 따라 공격 능력과 방어 능력이 좌우되는 경향이 크므로 우수한 인력의 양성과 확보가 매우 중요하다. 더불어, 국방부가 급속하게 발전하는 ICT 기술을 따라가기 위해서는 하드웨어적인 측면뿐 아니라, 소프트웨어적인 측면에서의 혁신과 업데이트도 소홀히 할 수 없다. 이와 관련하여 기술 진보의 신속한 반영, 일괄적이기보다는 테스트를 거친 점진적인 채택, 속도를 맞추기 위한 주문 요구 자제, 다양한 수준의 감독, 보안조치 개선 등을 IT 기술 획득에 있어서의 원칙으로 제시하고 있다(SOC 2011, pp.10~12).

## 3. 미 사이버 전략 보고서의 주요 함의

지금까지 살펴본 두 보고서가 가지는 의미를 생각해 보면 다음과 같다.

우선, 두 보고서 자체가 가지는 의미를 무시할 수 없다. ISC의 경우 사이버 공간에 대한 미국의 전반적인 시각과 입장을 체계적으로 정리한 보고서라는 점에서 의의가 있다. 사이버 공간에 대한 기술적 이용 등에 대한 내용보다는 안보, 정치, 경제적 측면 등 거시적인 방향을 전반적으로 다루고 있으며, 사이버에 관한 주무부서인 국토안보부를 비롯하여 국무부, 국방부, 재무부 등이 두루 참여했다는 점에 주목할 필요가 있다. 그리고 SOC의 경우에도 일국의 국방부 차원에서 사이버 안보에 관한 전략 보고서를 내놓았다는 점 자체가 의미를 지닌다.

양 보고서가 가지는 의미를 각각 살펴보면, 먼저 ISC의 경우 제목 자체가 많은 것을 내포하고 있다고 볼 수 있다. 미국은 '세계'(global)라는 표현 대신 '국제'(international)라는 표현을 쓰고 있다. 이는 세 가지 측면을 의도한 것으로 파악할 수 있다. 첫째,

오바마 행정부 이후 '다자'(multilateral)와 협력을 강조하는 정책 방향을 사이버 공간에 반영한 것으로, 본문에서도 언급했듯이 미국 단독이 아니라 동맹국(alliances) 및 협력국(partners)과의 협조를 통해 사이버 공간에서의 미국의 목표를 달성하겠다는 의도이다. 둘째, 첫 번째 의도와 맞물려 사이버 공간 자체가 초국가적(transnational)인 무형의 공간으로 어느 한 나라의 의도와 능력으로 관리할 수 있는 공간이 아니라는 사이버 공간의 특징을 미국도 인정하고 있다는 것을 알 수 있다. 셋째, 결국 사이버 공간에서도 기존의 현실적이고 물리적인 공간과 마찬가지로 국제적인 차원에서의 규범이 필요하다는 점을 강조하고, 미국이 이러한 규범 설정에서 이니셔티브를 가지려는 의도로 보인다. 이와 관련하여 기존의 현실적이고 물리적인 공간에 적용하던 국제 규범의 주요 내용을 사이버 공간으로까지 확장하여 그대로 적용하려는 것과 사이버 공간의 특수성을 고려한 새로운 규범을 정립하려는 의도를 보여주고 있다. 기존 규범의 확장과 새로운 규범의 창설 모두 각국과의 협력과 동의가 필요한 것으로, 향후 미국은 이 두 가지 측면에 주력할 것으로 사료된다.

또한 인터넷이 가지는 개방성과 표현의 자유 등을 강조했다는 점에 대해서도 주목해야 한다. 이것은 일견 인터넷이 지니는 본래의 특성일 수도 있으나, 다른 측면에서 보면 미국이 중시하는 민주적 가치의 표현이기 때문이다. 즉, 이는 사이버 공간이라는 영역을 공유하면서도 각기 다른 정치 체계 및 이념을 지니고 있는 국가들에 대한 일종의 외교적 압박 수단이 될 수 있는 것이다. 그리고 이를 통해 미국이 SNS로 촉발된 재스민 혁명을 어떻게 평가하고, 자국의 인터넷 검열을 강화하는 중국에 대해 어떤 태도를 견지할 것인지가 보다 명확해졌다고 볼 수 있다.

미국의 사이버 안보는 사이버 국방(cyber defense)의 차원으로 강화된 인상이다. 이 부분은 SOC와 관련하여 검토해야 할 필요가 있다. SOC를 통해 미국의 사이버 안보 전략에 대해 생각해 볼 수 있는 사항들은 크게 다음의 몇 가지로 집약될 수 있다. 첫째, 사이버 공간을 또 하나의 전장(domain)으로 공식 규정하였다는 점이다. 사이버 전쟁에 관한 논의는 새삼스러울 것은 없지만(Arquilla and Ronfeldt, 1993, pp.141~148), 금번에 미국이 이를 공식적으로 하나의 전장으로 규정했다는 점은 기존에 적용

되던 무력충돌법(Law of Armed Conflict) 등의 국제규칙을 사이버 공간에도 동일하게 적용하겠다는 의도로 파악할 수 있다. 이 중에서도 미국이 중점을 두고 있는 점은 사이버 공격에 대한 자위권 대응으로 보인다. 국방부 보고서에서는 이 부분을 비중 있게 다루어지 않았으나, ISC에서는 매우 조심스러우면서도 명시적으로 언급하고 있다. 즉, 유엔헌장을 거론하며 사이버 공격에 대해서도 현실세계에서와 같은 물리적인 군사적 대응을 할 수 있다는 가능성을 열어 둔 것이다. 더욱이, 국방부의 고위 인사들이 이 부분을 여러 차례 언급하고 있다는 사실에서 이번 보고서의 방점이 이 부분에 있음을 보여준다고 할 수 있다.

둘째, 공조와 협력을 강조하고 있다. 여기에는 정부 기관들 간의 협력, 민간과의 협력뿐 아니라 국제적 협력까지도 포함된다. 사이버와 안보가 결합된 사이버 안보는 사이버 자체의 확장과 안보 개념의 변화로 그 자체가 담당해야 하는 영역이 매우 넓다.[7] 더불어, 사이버 공간은 물리적 공간이 아니기 때문에 종래의 국경 개념이 무의미하고, 여러 국가를 경유하여 행해지는 경우도 빈번하다. 또한 전문적인 무기운용이나 전쟁교리 등이 필요한 분야가 아니라 기술적인 면이 강한 영역이기 때문에 군이나 정부기관의 인력보다 민간 자원이 우수한 경우가 많아, 이들의 활용이 절실하다는 것을 나타내고 있다.

셋째, 급속하게 발전하는 ICT 기술을 국방 분야에, 적시에, 적절하게 수용하는 노력을 소홀히 하지 말아야 한다는 점이다. 일반적인 무기는 개발에서 시험을 거쳐 실전에 배치되기까지 짧게는 수년에서 길게는 수십 년이 소요되는 데 비하여, 사이버 안보에 중요한 바이러스나 백신 기술은 하루가 다르게 실사용이 가능한 수준으로 개발되고 있다. 여기서 가장 문제되는 것은 역시 비용이다. 경제 문제가 큰 이슈인 미국의 현 상황에서 이 부분이 부각되지는 않았지만, 다른 최신 무기 및 장비 획득에 비해 사이버 안보와 관련된 비용은 비교적 저렴하다는 점에서 크게 문제될 것 같지는 않다.

7) ICT 분야의 가장 권위 있는 국제기구인 국제전기통신연합(ITU)의 사이버 안보에 대한 정의만 하더라도 정책, 도구, 대항조치, 지침, 위기관리, 관행 등이 모두 포함되어 너무 모호하고 포괄적이다 ("Definition of cybersecurity", www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx).

마지막으로 이러한 전략 보고서를 공개하는 것 자체가 미국이 사이버 안보에 대해 방어적 측면에서 만족하지 않고 적극적이고 공세적인 태도를 보일 것이라는 점을 시사한다. 오바마 미 대통령은 이미 핵무기나 미사일 사용의 경우와 마찬가지로 사이버 전쟁에 대한 가이드라인이 되는 행정 명령(executive order)에 서명하였고, 제임스 카트라이트 합참 부의장도 순전히 방어 위주인 사이버 전략에 변화가 필요하다고 역설한 점에서 이러한 짐작을 가능하게 한다.

# Ⅲ. 기타 주요국의 사이버 안보 전략[8)]

## 1. 보안과 안보를 동시에 강조하는 영국

영국은 국가안보 보고서라고 할 수 있는 'A Strong Britain in an Age of Uncertainty: The National Security Strategy'(2010)에서 사이버 공격을 테러공격에 이어 두 번째 우선순위에 두고 있을 만큼 사이버 안보에 대한 관심이 각별하다. 하지만 사이버 공격의 위험성에 대해 현재까지는 주로 지적재산권의 도용이나 정보 유출에 두고 있는 듯하다.

영국 사이버 안보의 본격적인 내용은 총리실에서 작성한 'Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space'(2009. 6)(이하 CSSUK)을 통해서 보다 구체적으로 알 수 있다. 영국의 사이버 안보는 상기 국가안보 전략에 따라 다음과 같은 원칙을 준수해야 한다. ① 인권, 법의 지배, 정당하고 신뢰할 수 있는 정부, 정의, 자유, 관용 및 기회라는 핵심 가치에 기초해야 한다. ② 냉정하게 위험, 목표 및 능력을 평가해야 한다. ③ 가능한 한 안보적 도전과제를 조기에 해결해야 한다. ④ 국제적으로는 다자적 접근을 취해야 한다. ⑤ 국내적으로는 협

8) 주요국은 ITU의 IDI, EIU의 Digital Economy Ranking, WEF의 NRI라는 3가지 지수의 2009 및 2010년 순위 중 상위 10위권 이내의 국가들을 그 대상으로 하였다. 각 지표의 2010년 순위는 이성휘(2010), pp.5~9.

력관계를 통해 접근해야 한다. ⑥ 정부 내에서는 보다 통합적인 접근방법을 개발해야 한다. ⑦ 강력하고 유연하면서도 균형 있는 능력을 보유해야 한다. ⑧ 안보를 강화하기 위해 계속해서 투자하고 학습하며 개선해야 한다(CSSUK 2009. p.10).

이러한 원칙에 기초하여 해당 보고서는 3가지 측면에서 사이버 공간에서 영국의 이익을 확보해야 한다고 주장하고 있다. 즉, ① 지식·능력 및 정책결정을 통해 ② 사이버 공간에서의 위험을 줄이고, ③ 기회를 활용하는 것이다. 보다 구체적으로 살펴보면, 위험 감소에 대해서는 적의 동기와 능력을 감퇴시켜 사이버 운용(cyber operations)의 위협을 줄이고, 사이버 운용에 있어서 영국 국가 이익의 취약성을 감소시키며, 영국 국가 이익에 대한 사이버 영향력을 줄인다는 것이다. 사이버 공간에서의 기회 활용에 대해서는 위협 행위자에 대한 첩보 및 정보를 수집하고, 영국의 정책에 대한 지지도를 향상시키며, 적을 방해하는 것이다. 끝으로 이를 위해서는 지식과 인식(awareness)을 개선하고, 원칙과 정책을 개발하며 관리(governance)와 정책결정을 발전시키고 기술적 능력과 인력 능력을 향상시켜야 한다는 것이 주요 내용이다(CSSUK 2009, p.16).

한편, 영국의 보고서는 다른 나라와 달리 사이버 위협의 행위자와 공격 유형을 간략하면서도 명확하게 밝히고 있다는 점이 흥미롭다. 즉, 국가뿐 아니라 범죄자 및 테러리스트가 사이버 위협의 행위자가 될 수 있다고 보고 있으며, 전자적 공격·공급사슬(supply chain)의 파괴·무선신호 조작 및 고출력 주파수를 통한 공격 등을 사이버 위협의 유형으로 제시하고 있다(CSSUK 2009, pp.13~14).

끝으로 보고서에서는 사이버 안보의 도전과제를 해결하기 위해 영국 정부가 전(全) 정부 차원의 프로그램을 창설하고, 협력자들과 긴밀히 협조하며, 사이버 안보국(OCS) 및 사이버 안보 운용센터(CSOC)를 설립할 것이라고 밝히고 있다(CSSUK 2009, p.21).

〈표 2〉 영국 정부의 사이버 안보 확보 노력

| | 조 치 | 내 용 |
|---|---|---|
| 1 | 전 정부 프로그램 (cross-government programme) 창설 | 영국의 전략적 사이버 안보 목표를 추진하기 위해 다음의 우선순위들을 다룰 수 있는 추가적인 재정 마련<br>- 안전하고 복원력을 갖춘 시스템<br>- 정책, 원칙, 법류 및 규제 이슈<br>- 인식 및 문화 변화<br>- 기술 및 교육<br>- 기술적 능력 및 R&D<br>- 활용(exploitation)<br>- 국제적 관여<br>- 관리(governance), 역할 및 책임 |
| 2 | 협력자들과의 긴밀한 공조 | 공공부문, 산업, 민간 자유 단체, 대중 및 국제적인 협력자들과 협력 |
| 3 | 사이버 안보국 (Office of Cyber Security, OCS) 설립 | 정부 차원의 전략적 지도력과 응집력 제공 |
| 4 | 사이버 안보 운용센터 (Cyber Security Operations Centre, CSOC) 설립 | - 사이버 공간의 건전성을 적극 모니터하고 사건 발생 시 대응을 조정<br>- 영국 네트워크 및 사용자들에 대한 공격을 보다 적절하게 파악<br>- 기업체와 대중들에게 위험에 관한 보다 유익한 정보와 권고를 제공 |

자료: "Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space", p.21, 2009. 6.

## 2. 정보 보안 중심의 일본

일본에서는 사이버 안보(cyebr security)보다는 '정보 안보'(information security)라는 표현을 더 많이 쓰고 있다. 일본의 방위백서의 안보환경 평가에서 사이버 전쟁과 사이버 안보를 다루고는 있으나(*Defense of Japan*(Annual White Paper), 2010, pp.15~16), 일본의 사이버 안보 전략에 대해서는 나와 있지 않다. 대신 2006년에 정보 보안과 관련한 'The First National Strategy on Information Security-Toward the realization of a trustworthy society'를 발표한 후 이 보고서를 평가하고 보다 장기적인

방향을 담은 'Secure Japan 2009'와 'The Second National Strategy on Information Security: Aiming for Strong 'Individual' and 'Society' in IT Age'를 발표하였다. 그리고 2010년에는 2009년 보고서의 연장선상에서 'Information Security Strategy for Protecting the Nation'(이하 ISSPN)을 발표하였다. 이들 보고서는 주로 내각관방 산하의 정보시큐리티정책회의(Information Security Policy Council)에서 주관한 것들이다.

2010년 보고서를 살펴보면, 먼저 2009년의 보고서의 내용을 계속 추진하면서도 발생 가능한 사이버 공격을 고려한 정책 강화와 대응 조직의 설립, 정보 안보환경의 변화에 적응하기 위한 정책 수립, 보다 적극적인 정보보호 조치 마련 등을 기본 정책 방향으로 제시하고 있다. 이러한 정책에 입각하여 ① IT 위험을 해소하여 국민 생활의 안전을 실현하고, ② 사회경제 활동의 토대로서 ICT 정책의 통합성 강화와 사이버 공간에서의 위기관리 전문성과 국가 안보를 강화하는 정책 시행, ③ 국가 안보, 위기관리 및 국민·사용자 보호의 측면을 포괄적으로 고려하는 3극(triadic) 정책 수립, ④ 경제성장 전략에 기여하는 정보 안보 수립, ⑤ 국제 협력 강화를 추진하겠다고 밝히고 있다(ISSPN 2010, pp.5~6).

보다 구체적인 조치들은 〈표 3〉에서와 같이 대규모 사이버 공격에 대한 대비와 정보 안보환경의 변화에 적합한 정보 안보 정책 강화로 대별되어 제시되어 있다.

〈표 3〉 일본 정보보호의 구체적 조치

| 분류 | 조치 | 내용 |
|---|---|---|
| 대규모 사이버 공격에 대한 대비 | (1) 대응 준비 조직 | - 대규모 사이버 공격에 대한 정부의 초기 대응 준비<br>- 공공부문과 민간부문의 협력<br>- 사이버 공격에 대한 보호 강화<br>- 사이버 범죄 단속<br>- 사이버 공격에 대한 국제협력 강화 |
| | (2) 일일 사이버 공격 정보 수집 및 공유 시스템 구축과 강화 | - 통신시스템 강화<br>- 각국과 정보공유 시스템 구축 및 강화 |

| 분류 | 조치 | 내용 |
|---|---|---|
| 정보 안보환경의 변화에 적합한 정보 안보정책 강화 | (1) 국민 생활을 보호하는 정보 안보 기초시설 | - 정부 기초시설 통합<br>- 핵심 기초시설 강화<br>- 기타 기초시설 강화<br>- 국가정보시큐리티센터(NISC)의 기능 향상 |
| | (2) 국민·사용자 보호 강화 | - 정보 안보 활동 추진<br>- '정보안보보안지원서비스(가칭)' 설립 제안<br>- 개인정보보호 증진<br>- 사이버 범죄 단속 강화 |
| | (3) 국제 협력 강화 | - 미국, ASEAN, EU 국가들과의 협력 강화<br>- APEC, ARF, ITU, Meridian, IWWN과 같은 국제 회의체를 통해 정보공유 시스템 구축<br>- 연락처로서의 NISC의 기능 향상 |
| | (4) 기술 전략 촉진 등 | - 정보 안보 R&D 전략적 촉진<br>- 정보 안보 인력 배양<br>- 정보 안보 관리 수립<br>- 정보 안보 관련 법률 시스템 조직 |
| | (5) 정보 안보 관련 법률 시스템 조직 | - 사이버 공간 안전 및 신뢰성 향상을 위한 조치 식별<br>- 각국과 정보 안보 법률 시스템 비교 |

자료: Information Security Policy Council(2010), "Information Security Strategy for Protecting the Nation", pp.8~19.

## 3. 국가 안보 차원에서 바라보는 호주

호주에서 사이버 안보와 직접적으로 관련된 기관에는 컴퓨터 긴급 대응팀인 CERT Australia(Australia's national computer emergency response team)와 사이버안보운용센터(Cyber Security Operations Centre, CSOC)가 있다. 이 밖에 법무부, 통신미디어국(ACMA), 안보정보국(ASIO) 등도 사이버 안보와 관련된 정부 조직이다.

호주의 사이버 안보 전략은 2009년 법무부 주관으로 선보인 'CYBER SECURITY STRATEGY'(이하 CSS)에 비교적 자세히 기술되어 있다. 동 보고서는 사이버 안보를 "전자적 또는 유사 수단에 의해 처리되고, 저장되며, 전파된 정보의 비밀성, 이용가능

성 및 완전성에 관련된 조치"(Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means)로 정의하고 있다(CSS 2009, p.5).

한편, 보고서에서는 목표와 전략적 우선 사항을 제시하고 있다. 주요 목표(aim)는 호주의 국가 안보를 뒷받침하고, 디지털 경제의 혜택을 극대화하는 안전하고(secure), 복원 가능하며(resilient), 신뢰받는(trusted) 전자적 운용 환경(electronic operating environment)의 유지(maintenance)이다(CSS 2009, p.5). 또한 '국가 전략 성명'(National Security Statement)의 내용에 어긋나지 않도록 사이버 정책도 국가 리더십(national leadership), 책임 공유(shared responsibilities), 협력 관계(partnerships), 국제적 차원의 적극적 관여(active international engagement), 위험관리(risk management), 호주 가치의 보호(protecting Australian values)라는 원칙들에 기초하고 있다(CSS 2009, p.8). 세부 목표는 다음과 같다. 첫째, 모든 호주 국민들이 사이버 위험을 인식하고, 자신들의 컴퓨터를 안전하게 보호하며, 온라인에서 자신들의 정체성·프라이버시·금융을 보호할 수 있는 조치를 취하도록 한다. 둘째, 호주의 사업체들은 운용의 완전성(integrity)과 고객들의 정체성 및 프라이버시를 보호할 수 있는 안전하고 복원 가능한 정보통신기술(ICT)을 운용하도록 한다. 셋째, 호주의 정보통신기술이 안전하고 복원 가능하다는 점을 호주 정부가 보증한다(CSS 2009, pp.10~14).

이러한 목표의 달성을 위해서 호주 정부는 7가지 전략적 우선 사항을 설정하고 있다. 7가지 전략적 우선 사항은 위협의 인식과 대응, 문화 변화, 관-산 협력, 정부 시스템, 국제적 관여, 법 집행, 지식·기술 및 혁신이다. 각각의 내용은 〈표 4〉와 같다.

〈표 4〉 호주 사이버 안보 전략의 전략적 우선 사항

| | 분 야 | 내 용 |
|---|---|---|
| 1 | 위협의 인식과 대응<br>(Threat Awareness and Response) | 정부의 핵심 시설 및 기타 국가 이익에 관련된 시스템을 중심으로 복잡한 사이버 위협에 대한 탐지, 분석, 완화 및 대응 향상 |

| | 분 야 | 내 용 |
|---|---|---|
| 2 | 문화 변화(Cultural Change) | 호주 국민들이 온라인상에서 스스로를 보호할 수 있도록 정보, 자신감 및 실질적인 도구를 통한 교육 및 권한 부여 |
| 3 | 관-산 협력(Business-Government Partnerships) | 기초시설, 네트워크, 제품 및 서비스의 안전과 복원력을 개선하기 위해 기업들과 협력 |
| 4 | 정부 시스템 (Government Systems) | 정부와 온라인으로 연결되는 시스템을 비롯하여 정부의 ICT 시스템 보호에 있어서 모범례(best practice) 모델화 |
| 5 | 국제적 관여 (International Engagement) | 호주의 국가 이익을 뒷받침하는 안전하고 복원력이 있으며 신뢰받는 글로벌 전자 운용환경 증진 |
| 6 | 법 집행 (Legal and Law Enforcement) | 사이버 범죄를 적발하여 기소할 수 있는 효과적인 법 체계 및 집행 능력 유지 |
| 7 | 지식, 기술 및 혁신 (Knowledge, Skills and Innovation) | 혁신적인 솔루션 개발을 위한 R&D를 통해 숙련된 사이버 안보 인력 증진 |

자료: Attorney General's Department(2009), "CYBER SECURITY STRATEGY", pp.10~14.

## 4. 무력을 배제하지 않는 독일

독일의 경우에는 다른 국가들과 비교해서 조금 늦은 올해에야 사이버 안보 전략을 내놓았다. 독일의 사이버 안보 전략의 가장 큰 특징은 다른 나라들과 달리 미국의 사이버 안보 전략과 유사하게 무력의 사용을 암시하고 있다는 점이다. 2011년 2월에 내무부가 발표한 'Cyber Security Strategy for Germany'(이하 CSSG)에서 사이버 안보는 민간을 중심으로 이루어져야 한다고 하면서도, 이러한 민간의 조치는 군대(Bundeswehr)의 조치에 의해 보완될 수 있다고 밝히고 있다. 더불어, 사이버 안보가 독일의 예방적(preventive) 안보 전략의 일부에 속한다고도 언급하고 있다(CSSG 2011, p.5). 문자 그대로만 보자면, 독일의 사이버 안보 전략은 미국의 사이버 안보 전략과 유사하면서도 논란의 여지가 더욱 많다고 할 수 있다. 예방적 차원에서의 조치가 만약 실제적인 무력 사용까지 포함하는 것이라면, 이는 현실 세계에서도 논란이 많은 예방적 자위권 문제로 귀결되기 때문이다.

또한 CSSG에서는 ICT의 특성을 감안하여 국제적인 공조도 강조하고 있다. 다만, 국제공조에서 국가 단위를 언급하기보다는 UN, EU, NATO, G8 등 다자기구와의 협

력을 강조하고 있다는 점이 다른 국가들과 차이를 보이고 있다.

한편, 독일은 10개의 전략 분야를 설정하고, 전략적 목표와 조치들을 보고서에 담고 있으며, 구체적인 내용은 〈표 5〉와 같다.

〈표 5〉 독일 사이버 안보의 전략적 목표와 조치

| | 분 야 | 내 용 |
|---|---|---|
| 1 | 핵심 정보 기초시설의 보호 | 민관 간의 정보공유에 기초한 협력 강화가 필요하고, 이를 위해 핵심 기초시설 보호(CIP) 이행계획의 연장이 중요 |
| 2 | 독일 IT 시스템의 안전 확보 | - 시민과 중소기업이 사용하는 IT 시스템의 안전을 위해 사회 단체와 정보 및 조언을 공유하고, 공급업체들이 보안을 위해 적절한 조치를 취하도록 함<br>- 중소기업을 지원하기 위해 경제기술부는 TF를 구성 |
| 3 | 행정 분야의 IT 안보 강화 | - 국가는 데이터 보안의 귀감이 되어야 하며, 전자 오디오 및 데이터 통신의 기초가 될 공통적이고 통일적이며 안전한 네트워크를 구축<br>- 이를 위해 중앙과 지방 간의 적절한 자원 배분이 필요 |
| 4 | 국가사이버대응센터(National Cyber Response Centre) | - IT 사고 발생 시 모든 국가 기구들 간의 협력을 최대화하고 보호 및 대응 조치를 조정하는 역할<br>- 이를 위해 IT 제품의 취약성, 공격의 유형, 침입자 정보에 관한 정보공유가 필요하며 개별 주체의 책임 의식이 중요<br>- 사이버 사고의 예방을 위해 국가사이버안보위원회에 정기적, 그리고 특정 사건 발생 시 권고문 제출 |
| 5 | 국가사이버안보위원회(National Cyber Security Council) | - 연방정부, 공공부문 및 민간부문의 협력을 위해 설립<br>- 총리실, 외무부, 내무부, 국방부, 경제기술부, 법무부, 재정부, 교육연구부, 각 주 대표들이 참석<br>- 산업계는 준회원으로 참석, 학계 대표는 필요한 경우 참석 |
| 6 | 사이버 공간에서의 효과적인 범죄 통제 | - 사이버 범죄, 간첩 활동, 파괴(sabotage)에 대한 사법당국의 능력 강화가 필요<br>- 글로벌 사이버 범죄 활동이 유럽의 '사이버 범죄 협약'(Cyber Crime Convention)에 기초하여 해결될 수 있도록 노력하며, UN 차원에서도 이러한 협약이 추가로 필요한지에 대해 검토할 필요가 있음 |

| | 분 야 | 내 용 |
|---|---|---|
| 7 | 유럽과 전 세계의 사이어 안보 확보를 위한 효과적으로 조율된 조치(action) | - EU 차원뿐 아니라 UN, OSCE, 유럽의회, OECD, G8 등과 협력<br>- NATO가 사이버 안보를 책임 분야로 고려해야 함 |
| 8 | 신뢰할 만한 정보기술의 사용 | - 사회경제적인 측면을 고려한 보호 계획의 개발이 필요<br>- 국제표준보다는 기술의 다양성을 존중 |
| 9 | 연방당국에서의 인력 개발 | - 당국 내에서 추가 인력의 필요성 검토<br>- 부처 간 협력 강화를 위한 인력 교환 |
| 10 | 사이버 공격에 대한 대응 도구 | - 정부 당국 간 협력을 통해 조정되고 포괄적인 대응 도구 마련<br>- 필요한 경우 연방 또는 주정부 차원의 권한 규정 신설 검토 |

자료: Federal Ministry of the Interior(2011), "Cyber Security Strategy for Germany", pp.6~12.

## 5. 주요국 사이버 안보 전략의 의미

이상에서 살펴본 4개국 외에도 여러 국가들이 자국의 사이버 안보 전략을 수립하거나, 수립하기 위해 노력하고 있다.[9] 사이버 안보에 대한 주의환기, 분야와 대상을 가

9) 캐나다는 'Canada's Cyber Security Strategy: For a Stronger and More Prospective Canada' (2010)를 통해 캐나다의 사이버 안보는 미래의 사이버 위협을 예방하고, 탐지하며, 해소하여 캐나다의 국익에 도움이 되도록 사이버 공간을 활용해야 한다고 밝혔다. 전략 방향에 있어서는 법의 지배(rule of law), 수용성(accountability) 및 프라이버시 등 캐나다의 가치를 반영하고, 사이버 위협에 대응하기 위한 부단한 개선 노력에 임하며, 전 정부 차원의 총력 대응을 취하고, 각 주 및 지방과의 협력관계를 강화하며, 동맹국들과의 긴밀한 협력 관계 구축을 위해 노력해야 한다고 강조했다.
중국의 경우 정부 차원의 공식적인 사이버 안보 전략은 보이지 않지만, 중국판 국방백서에서 중국 국방의 주요 목표와 임무 중에 사이버 공간에서의 국가 안보 이익을 수호해야 한다는 점을 명시하고 있고, 군의 정보화 능력을 강조하고 있다는 점과 최근에는 '왕뤄란쥔(網絡藍軍)'이라는 사이버 부대를 운용하고 있다는 사실을 공식적으로 인정했다는 점에서 사이버 안보에 대한 지대한 관심을 엿볼 수 있다.
인도는 통신정보부에서 'National Cyber Security Policy: For secure computing environment and adequate trust&confidence in electronic transactions'라는 제목으로 초안이 나온 상태다. 이 보고서는 '적절한 절차와 기술적 보안 조치를 통해 정보와 정보 시스템을 보호하는 활동'인 사이버 안보와 사이버 국방은 사이버 안보와 위협의 성질, 보호해야 할 자산 및 보호에 적용되는 메커니즘이 다른 사이버 국방을 구분하고 있는 점이 특징이다.
또한 네덜란드는 올해 2월 'The National Cyber Security Strategy(NCSS): Success through coo-

리지 않는 협력과 공조 강조, 사이버 안보를 위한 인력 양성과 국민의식 강화 등의 일반적인 전략 방향은 미국 및 기타 주요국에서 크게 다를 바 없이 나타난다. 이는 이들 국가들이 ICT 기술과 사이버 공간의 활용에 있어서 큰 차이가 없기 때문이라고 볼 수 있다.

다만, 각국의 안보 정책도 자신들의 상황에 따라 각기 다르듯이 사이버 안보 전략에 있어서도 크게 두드러지지는 않지만, 개별적인 차이점이 존재한다. 우선, 미국을 제외한 주요국들의 사이버 안보 전략이 미국과 가장 크게 다른 점은 미국이 자신의 전략을 글로벌 차원으로 확대하는 데 중점을 두고 글로벌 차원의 사이버 공간에 대한 규범이나 합의를 도출하기 위해 노력하는 모습을 보이는 반면에, 기타 주요국들은 국제적인 협력을 강조하면서도 협력의 수준이 미국이 생각하는 것보다는 낮다는 점이다. 즉, 미국이 동맹 수준의 협력을 요구하고 있다면, 이들 국가들은 공조 수준의 협력에 머무르는 듯한 모습을 나타내고 있다는 것이다. 덧붙여 미국만이 국방부 차원에서의 전략을 내놓고 있다는 점을 보더라도 그 차이를 알 수 있다.

또한 사이버 안보 전략에는 각국의 정치적 특색이 곳곳에 반영되어 있다. 예컨대, 지방정부와의 관계나 자국의 문화를 고려한 점을 들 수 있다. 이들 두 가지는 모든 나라에 해당될 수 있는 사항이지만, 사이버 안보 전략을 접근하는 데 있어서 각국의 시각차를 엿볼 수 있는 부분으로 여겨진다. 그리고 사이버 안보 전략을 수립하거나 공개하는 부처의 차이도 이에 대한 연장선으로 볼 수 있다. 백악관과 총리실 등 최고 통치기관에서 사이버 안보 전략을 발표한 국가도 있고, 내무부·법무부·정보통신부 등 개별 부처 차원에서 담당하는 국가도 있기 때문이다.

마지막으로 앞에서 소개한 각국의 사이버 전략의 기저에는 경제에 대한 위협을 방지해야 한다는 의식이 강하게 자리 잡고 있다고 볼 수 있다. 즉, 기존의 국가 안보의 주된 영역인 영토 보전이 사이버 공간에서는 무의미할 수 있기 때문에 보다 현시적인 경제 분야에 대한 우려가 많이 반영되어 있다고 할 수 있다. 이러한 사실은 오늘날

peration'을 발표했는데, 개개인에 대한 책임 강조를 넘어서 사이버 안보를 위한 규제로 자율규제(self-regulation)를 강조하고 있다는 점이 차별적이다.

금융 분야를 비롯한 경제 전반이 ICT에 크고 의존하고 있는 사실에서도 짐작할 수 있다.

## Ⅳ. 결론-우리의 사이버 안보 정책 방향

이상 각국의 사이버 안보 전략을 종합해보면, 다음과 같은 특징을 엿볼 수 있다. 먼저, 각국의 사이버 안보 전략은 사이버 공간의 특성상 공통점이 많으나, 개별 국가만의 성향 및 특징이 반영된 측면도 강하게 나타난다. 또한 ICT가 발달된 국가들은 대부분 사이버 안보에 관한 정부 차원의 전략이 마련되어 있으며, 전 정부 차원에서의 노력을 강조하고 있다. 다만, 주무부처는 각국의 상황에 따라 조금씩 다르다. 더불어, 사이버 공간의 특성을 감안하여 공공부문과 민간부분의 협력, 개인과 조직 차원의 노력, 동맹국 등 국제적 협력을 중요하게 다루고 있다. 그리고 사이버 인력 양성 및 교육 또한 많은 국가들이 강조하고 있는 부분이다. 끝으로, 사이버 공간의 특성상 기존의 전통적인 안보적 관점과 기술적 보안의 관점이 혼재되어 있다.

우리의 사이버 안보 정책도 이러한 점들을 고려하고 반영해야 할 것이다. 우선, 사이버 안보에 대한 전 사회적 차원에서의 인식 정립이 필요하고, 이를 기초로 사이버 안보를 관장할 주무기관을 명확히 설정해야 한다. 둘째, 사이버 안보 전략 수립 시 잘 갖춰진 ICT 기초시설, 사이버 공간의 활용도가 높은 현실, 사이버 전력을 강화하고 있는 북한과의 대치 상태 등 우리나라의 특수성을 적절히 반영해야 한다. 셋째, ICT의 특성상 기존 안보 차원의 동맹국과 경제 분야의 협력국 등 타국과의 공조 및 협력 강화에 진력을 다해야 한다. 마지막으로 미국과 독일 등 사이버 공간에 대한 기존의 군사력 활용 가능성을 언급한 국가들의 사례에 비추어 사이버 공격에 대한 사이버 공격 대응, 사이버 공격 징후 시 예방 차원의 선제적 대응, 사이버 공격에 대한 물리적 공격 등 다각도로 적절한 대응 매뉴얼을 검토할 필요가 있다.

## 참고자료

김도승 (2009), "사이버 위기 대응을 위한 법적 과제-미국의 사이버위기 대응체계 현황과 시사점을 중심으로", 《방송통신정책》, 제21권 17호 통권 470호, pp.21~57.

김주홍 (2001), "정보화시대에 대비한 한국의 안보정책 방향 연구", 《국제정치논총》, 제41집 1호, pp.69~92.

방송통신위원회·행정안전부·지식경제부 (2011), 『2011 국가정보보호백서』.

서동주 (2008), "한국정치학에서 '사이버 공간·안보' 연구 동향과 정책적 함의", 《국가전략》, 제14권 2호, pp.5~32.

이성휘 (2010), "G20 국가의 IT산업 경쟁력 비교", 《IT SPOT Issue》, SPOT 2010-S15.

장의관 (2005), "지식정보화 시대의 국가 안보정보 관리전략", 정보통신정책연구원.

American Forces Press Service (2011. 7. 14.), "Lynn: cyber Strategy's Thrust is Defensive". www.defense.gov/news/newsarticle/.aspx?id=64682. 접속일: 2011년 7월 25일.

Arquilla, John and Ronfeldt, David (1993), "Cyberwar is Coming!", *Comparative Strategy, Vol 12*, No.2, pp.141~165.

Australian Government (2009), "CYBER SECURITY STRATEGY". http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~AG+Cyber+Security+Strategy+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf. 접속일: 2011년 7월 15일.

Baldwin, A., David (1997), "The concept of security", *Review of International Studies, 23*, pp.5~26.

Bronk, Christopher (2011), "Blown to Bits: China's War in Cyberspace", August-September 2020, *STRATEGIC STUDIES QUARTERLY*, pp.1~20.

Department of Defense (2011), "Department of Defense Strategy for Operating in Cyberspace". http://www.defense.gov/news/d20110714cyber.pdf. 접속일: 2011년 7월 30일.

Department of Information Technology(India) (2011), "National Cyber Security Policy(Discussion draft)". http://www.mit.gov.in/sites/upload_files/dit/files/ncsp_060411.pdf. 접속일: 2011년 7월 20일.

DeWeese, Steve, Krekel, Bryan&Bakos, George (2009), "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation", McLean, VA: Northrop Grumman Corporation(Prepared for The US-China Economic and Security Review Commission). http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf. 접속일: 2011년 7월 20일.

Federal Ministry of the Interior (2011), "Cyber Security Strategy for Germany". http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Sicherheit/css_engl_download.pdf?__blob=publicationFile. 접속일: 2011년 8월 1일.

Geer, E., Daniel, Jr. (2010), "Cybersecurity and National Policy", *Harvard National Security Journal, Vol 1.*, pp.203~215.

Government of Canada (2010), "Canada's Cyber Security Strategy-FOR A STRONGER AND MORE PROSPEROUS CANADA". http://www.publicsafety.gc.ca/prg/ns/cbr/ccss-scc-eng.aspx. 접속일: 2011년 7월 25일.

Information Security Policy Council(Japan) (2010), "Information Security Strategy for Protecting the Nation". http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf. 접속일: 2011년

5월 10일.

Jordan, Tim (1999), "Cyberpower: The culture and politics of cyberspace and the Internet", New York: Routledge.

Kristin M. Lord and Travis Sharp(eds.) (2011), "America's Cyber Future: Security and Prosperity in the Information Age", Washington: Center for a New Americam Security(CNAS).
http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20I_0.pdf. 접속일: 2011년 7월 10일.

THE WALL STREET JOURNAL (2011. 5. 31), "Cyber Combat: Act of War".

Whitehouse (2011), "International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World".
http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. 접속일: 2011년 5월 25일.