issue BRIEF

북한의 사이버 공격과 위협에 대한 우리의 대응
– 2014년 11월 소니(Sony) 사건의 교훈 –

2015-05
APR. 6, 2015

아산정책연구원

신창훈 | 글로벌거버넌스센터장

1. 머리말

지난 3월 31일 정부는 북한의 사이버공격과 사이버전의 위협에 대응하기 위해 청와대 국가안보실에 사이버안보비서관을 신설하겠다고 발표했다. 또 오는 5월 경 '사이버 국가안보전략(National Cyber Security Strategy)'이 발표될 것이란 관측도 나오고 있다.

정부의 이러한 움직임은 우리가 잘 인식하지 못하는 북한의 사이버공격이나 사이버전 위협에 대비해 인적·전략적 측면을 갖춘 사이버 정책을 마련한다는 의미여서 환영할 만하다.

최근 미국은 북한의 소니픽쳐스엔터테인먼트사(이하 소니) 사이버 공격에 대응하는 조치를 발표했다. 이런 미국의 사례에 비추어 한국 사이버안보비서관의 바람직한 역할 설정과 효율적이고 지속 가능한 사이버안보정책과 전략 수립을 위해 아래 5가지 요소를 고려할 것이 요구된다.

첫째, 남북의 사이버 성숙도와 의존성의 차이로 발생하는 비대칭적 취약점을 보완하기 위해 사이버 방어력을 최대한 강화할 것.

둘째, 사이버 방어력 강화와 병행해 억지(deterrence)전략을 마련하고 사이버전과 관련한 명확한 교리(doctrine)와 태세(posture)를 확립해 공개할 것.

셋째, 사이버 국가안보 전략은 억지력 향상에 더해 복원력(resilience)을 강화하는 전략도 반드시 담을 것.

넷째, 새로 임명될 사이버안보비서관은 기술적 방어 능력 향상은 물론 사이버전략에 관한 명확한 입장과 비전도 제시할 것.

다섯째, 청와대 국가안보실은 사이버전과 관련, 비전통안보(non-traditional security)라는 전략적 담론 차원의 논의를 펴면서 대비책을 마련할 것.

2. 현실적 위협이 된 북한의 사이버공격·사이버전[1]

2013년 3월 20일 오후 2시경 KBS, MBC, YTN 등 주요 방송사는 물론 농협, 신한은행 등 금융기관의 대부분 컴퓨터가 일시에 작동을 멈췄다. 마스터부트레코드(MBR)[2]가 파괴돼 재부팅 되지 않고, 볼륨부트레코드(VBR)[3]도 파괴돼 복구가 불가능해지는 등 전산망이 대대적으로 마비가 되는 사태가 벌어졌다.

총 32,000여 대의 컴퓨터를 포함한 전산망이 파괴되는 등 이로 인한 피해액이 무려 8,600억 원 이상으로 추정되고 있다.[4] 4월 10일 정부는 "북한의 정찰총국 소행으로 추정한다"는 조사결과를 발표했다. 피해규모 뿐 아니라 속수무책으로 당한 현실을 반영하듯 '3.20 전산대란', '3.20 전산망 마비 사태' 혹은 '3.20 사이버테러' 같은 표현이 등장했다. 나아가 '다크서울 공격(DarkSeoul attack)'이라는 별칭까지 얻게 됐다. 언론은 사태 1주년과 2주년을 맞는 작년과 올해 3월 20일을 전후로 비중 있게 사태를 재조명했고 국책 연구소 등은 공개회의도 열었다.

그런데 이런 보도와 행사에는 정작 국민이 궁금하게 여기는 중요한 물음은 빠져 있었다. 바로 '2013년 3월 20일의 북한 공격에 정부는 어떤 대응 조치를 취했는가'라는 질문이다.

2013년 3월 20일부터 북한의 사이버공격은 단순한 가능성을 넘어 안보는 물론 우리의 사이버공간을 겨냥하는 구체적이고 현실적인 위협이 됐다. 이 공격은 북한 추종 세력의 자발적 행위가 아니라 북한의 사이버부대가 우리의 금융기관과 방송사를 공격한 사건이었다. 단순한 DDoS(분산형서비스거부)공격으로 해당 웹사이트의 작동을 일시적으로 중단시킨 것이 아니라 추정치가 8,600억 원 규모인 대형 피해를 발생시켰다는 점에서 파멸적이고 파괴적인 공격행위였다.

그런데도 북한에 어떠한 보복조치를 취했는지 정부는 전혀 공개하지 않고 있다. 보복조치를 했지만 밝히는 것이 적절치 못하다고 주장할 수도 있다. 우리의 방어력을 보강하는 등

내실을 다지는 게 더 중요하지 보복이 필요하지 않다고 할 수도 있다. 다 일리가 있지만 남북의 사이버전(cyber warfare)에 나타나는 비대칭성에 대한 이해를 바탕으로 한 대책과 전술 및 전략은 물론 억지력도 함께 고려하지 않은 이들의 견해가 설득력이 있을지는 의문이다.

3. 남북한 사이버 환경 및 사이버전 능력의 비대칭성

북한의 사이버공격·사이버전에 대한 지속 가능하면서도 효율적인 대응책은 남북의 사이버 환경과 사이버전 수행 능력에 대한 정확한 평가에서 출발해야 한다. 평가에 기초가 되는 자료와 지식은 상당히 많이 공개돼 있다. 정책 제언이라는 목적에 한정해 공개자료를 기초로 평가와 관련된 몇 가지 결론을 내리면 다음과 같다.

첫째, 한국의 사이버 환경은 민간(산업계)과 정부·공공 영역이 분리돼 있지만 북한은 그렇지 않다. 북한의 경우 사이버공간을 소유하고 운영하는 주체는 국가 즉 정부이기 때문에 모든 사이버 환경은 철저히 중앙집권화된 계획과 통제하에 놓여 있다.

이는 정책의 효율성에 큰 차이를 발생시킨다. 한국은 일관성 있는 사이버안보 정책의 수립을 위해 민간과 공공 영역이 협력해야 하므로 시간이 걸리고 비용이 들어간다. 이런 상황은 위기 때 신속한 대응을 하는 데 걸림돌이 될 수 있다. 그러나 북한은 어떤 위기에서도 신속히 대응할 수 있을 뿐 아니라 협력과 대화를 위한 비용도 들지 않는다. 이런 사이버 환경의 차이는 사이버공격·사이버전 수행의 비대칭성을 만드는 원인이 된다.

둘째, 사이버 환경의 차이는 비대칭적 취약성(asymmetric vulnerabilities)을 발생시켜 공격 유혹을 강하게 유발한다는 점에 주목해야 한다. 비대칭적 사이버 환경은 2014년 4월 호주전략정책연구원(Australian Strategic Policy Institute, ASPI)이 발표한 보고서[5]의 사이버 성숙도(cyber maturity)라는 지표에 잘 나타나 있다. 보고서는 사이버 성숙도라는 지표를 산출하기 위해 1) 거버넌스, 2) 군(military), 3) 디지털 경제 및 사업, 4) 사회적 참여를 수치화 해 평가하는 방식을 취했는데 이에 따른 남북의 사이버 성숙도 지표는 〈표 1〉과 같다.[6]

〈표 1〉에 따르면 남북한은 '디지털 경제 및 사업 분야'와 '사회적 참여'의 하부 요소인 '인터넷 연결도'에서 차이가 크다. 이처럼 경제적 측면을 비롯해 여러 면에서 차이가 큰데도 사이버공간에서의 군(military) 역할에는 양측의 차이가 전혀 없다는 점은 정책 대안을 마련하

표 1. 남북한의 사이버 성숙도

	1. 거버넌스				2. 군	3.디지털 경제 및 사업		4. 사회적 참여		총점
	조직 구조	입법	국제적 참여	사이버 안보지원 서비스	사이버 공간에서 군의 역할	정부-비즈니스 대화	디지털 경제	대중의 인지도	인터넷 연결도	가중치를 둔 총점
한국	7	6	7	8	7	8	8	9	9	75.5
북한	3	1	2	0	7	1	2	1	1	20.7

는 데 반드시 주목해야 할 대목이다.

북한은 디지털경제의 발전에는 큰 관심이 없으며 민심 이탈을 막기 위해 바깥 세상과의 인터넷 연결을 차단하고 자유로운 정보의 유입을 계획적으로 막고 있지만 군사적 목적으로는 사이버 공간을 적극 활용하고 있다.

북한은 남북의 현저한 비대칭성을 중요한 대남 공격포인트로 인식할 것이다. 사이버공격·사이버전으로 갈등이 고조될수록 사이버공간에서 우리의 피해는 기하급수적으로 증가하지만 북한의 피해는 제한적일 수밖에 없다. 남북의 공격과 방어가 사이버공간에만 벌어진다면 북한으로서는 잃을 것이 없는 승리의 공간인 셈이다. 사이버공간은 평시 우리의 전략적 자산이지만 방치하면 전시에는 엄청난 취약점이 돼 북한은 목적 달성을 위해 작전을 펼치고 협박하기 쉬운 공간으로 간주, 집요하게 공격해 올 것이다.

셋째, 디지털 경제규모와 인터넷 연결의 차이로 만들어진 비대칭적 취약점은 우리의 사이버전 능력을 현저하게 떨어뜨리는 요인이 되고 있다. 남북 간의 사이버전 능력을 비교하는 자료를 찾기 곤란하지만 단순한 지표를 활용해 주요국 간을 비교하는 공개 자료는 있다. 이 중 가장 단순하고 흥미로운 Clarke와 Knake의 비교 표를 제시하면 〈표 2〉와 같다.[7]

〈표 2〉에서는 사이버 의존성이 낮을수록 점수가 높게 표시되는데 이는 사이버전 능력이 강하다는 의미다. 이들은 사이버전 능력을 1) 공격, 2) 의존성, 3) 방어 세 범주만으로 평가했기 때문에 단순한 평가라는 비판을 받는다. 그러나 사이버 의존성이 낮은 북한이 사이버전 능력은 오히려 높게 평가되기 때문에 북한은 전세계 유력 저널리스트들이 관심을 끄는 대상이 됐다. 사이버 의존성을 과대 평가하는 측면은 있지만 이 문제는 사이버전략 구축에서 반드시 고려해야 할 중요한 요소임을 보여준다.

표 2. 각국의 사이버전 능력 비교

	사이버 공격	사이버 의존성	사이버 방어	총점
미국	8	2	1	11
러시아	7	5	4	16
중국	5	4	6	15
이란	4	5	3	12
북한	2	9	7	18

4. 소니 해킹사건과 미국의 대응(보복)조치가 주는 교훈

2014년 11월 24일 소니사 직원들의 컴퓨터 화면에 붉은 해골과 함께 회사 정보를 유출하겠다는 경고 메시지가 팝업으로 떴다. 이 사이버공격은 시스템을 파괴하고 개인 정보를 빼갔을 뿐 아니라 미개봉 영화 파일도 유출해 실질적인 경제적 피해를 일으켰다.[8] 소니라는 민간회사에 대한 공격이었지만 '북한 소행'이라는 FBI의 발표 직후 오바마 미 대통령은 이를 '사이버 파괴주의(cyber vandalism)'로 규정하고 "미국이 선택하는 장소와 시간 및 방법에 따라 비례적으로 대응하겠다"라고 천명했다. 소니 사건과 이에 대한 미국의 대응은 '앞으로 있을지 모를' 북한의 사이버공격에 우리가 어떻게 대처해야 하는지에 대해 교훈을 주고 있는데 이 중 우선 몇 가지를 소개하면 다음과 같다.

(1) 소니 사건의 교훈

소니 사건은 북한의 김정은을 희화하고 암살 계획도 보여주는 코미디 영화 '더 인터뷰(The Interview)'에 대한 보복이라고 단순화하기엔 결과가 너무 심각하고 엄중했다. 소니에 1,500만 달러(약 165억 원)로 추정되는 경제적 손해를 입힌 파괴적 공격이었다.[9] 이번 공격은 향후 북한의 사이버공격·사이버전 전개와 관련해 다음과 같은 중요한 방향을 시사한다.

첫째, 전시가 아닌 평시에 발생한 파괴적 행위로 공격 방식이 꾸준히 진화하고 있음을 보여준다. 전시 사이버공격의 양상은 이미 다양한 형태로 공개됐다. 그러나 평시에 발생하는 대다수 사이버공격과 사이버전은 전모를 전혀 보여주지 않는 시범(trial run)에 불과했다. 예를 들어 보통 평시에 사이버공격·사이버전을 하는 국가들은 단순한 DDoS 공격으로 타깃 사이트의 작동을 일시 중지시키는 선에 그쳤다. 2007년 에스토니아, 2008년 조

지아에 대한 러시아의 사이버공격처럼 며칠에 걸쳐 대대적으로 DDos 공격을 한 사례도 있다. 그러나 이 경우에도 '산출 가능한 경제적 피해'를 야기하는 직접적이며 파괴적인 공격은 아니었다. 사실 전시가 아닌 평시에는 DDoS 공격만으로 존재감을 드러내는 소위 전시효과(demonstration effect)를 충분히 거둘 수 있다. 그런 점에서 소니사에 대한 공격은 사이버공격·사이버전의 능력을 과시하는 정도를 넘어 정치적 목적에 따른 것이란 평가가 가능하다.

북한도 사이버전 초기에는 전시효과를 염두에 둔 듯한 DDoS 공격을 했다. 그 단적인 예가 바로 2009년 7월에 한국과 미국에서 발생한 DDoS 공격이었다. 2009년 5월 북한은 2차 핵실험을 했고, 같은 해 7월 4일 미국 독립 기념일에는 미사일 7발을 발사했다. 그런데 7월 4일부터 9일까지 3차례에 걸쳐 미국 정부와 한국에 대대적인 사이버 공격이 발생했다는 사실은 많이 알려져 있지 않다. 7월 4일의 DDoS 공격은 미 백악관과 펜타곤이 주 타깃이었다.[10] 일련의 치밀한 행동계획을 통해 전시효과를 극대화한 것이다. 그런데 2013년 3월 20일 공격 때는 파괴적 행위가 크게 늘더니 2014년 소니 사건에서는 지적재산을 유출하는 행위까지 저질렀다.

둘째, 공격대상이 민간으로 무차별하게 확대됐다. 북한이 사이버 공격을 자제해야 하는 타깃 목록을 보유하고 있지 않음을 의미한다. 2009년 사이버공격의 대상은 미국의 경우 백악관, 펜타곤 등 정부 사이트였다. 2013년 3월 한국에 대한 사이버공격의 대상은 기간방송사와 금융기관 등 국가의 중요한 인프라[11]로 사실상 정부가 타깃이었다. 그런데 2014년의 대상인 소니사는 정부도 중요 인프라도 아닌 민간회사였다. 이는 북한이 평시에도 민간을 공격 대상에서 배제하지 않는다는 것을 뜻한다.

사이버공격과 사이버전 능력을 갖춘 국가들은 긴장의 확산을 막기 위해 소위 '유보적 공격대상(withhold target set)'을 사전에 설정, 공격을 자제하고 평시에는 특히 더 엄격하게 금한다. 그 대상엔 앞서 예로 든 중요 인프라와 민간인이 포함된다. 이런 대상이 공격을 받으면 단호히 보복하고 특히 중요 인프라를 공격하면 이를 국가 차원의 전쟁 행위로 간주한다는 지침도 갖고 있다.

한편 전쟁법이 적용되는 전시에는 국제관습법인 차별주의가 적용되는데 이에 따르면 민간에 대한 공격은 금지된다. 지침에 불과하지만 '탈린 매뉴얼(Tallinn manual)'의 Rule 37도 민간에 대한 사이버공격을 금지하고 있다.[12] 북한이 2010년 11월의 연평도 포격이 민간인을 의도적으로 공격한 것이 아니라고 발뺌해도 2013년 3월 20일의 공격에 이어 발

생한 소니 사건은 민간을 의도적으로 공격한 것이란 점에서 북한이 관련 국제규범을 모두 무시하는 것은 물론 유보적 공격 대상도 설정하지 않고 있음을 재확인해준다.

(2) 미국 대응(보복)조치의 교훈

첫째, 미국 정부는 소니 사건에서 행위의 귀속(attribution)문제를 신중히 확정한 다음 곧바로 엄중한 대응(보복)조치를 취하겠다고 발표했다. 우선 사건 20여 일 만에 FBI는 북한에 책임이 있다는 발표부터 했다.[13] 이러한 귀속 가능성 발표 직후 오바마 대통령은 CNN 방송과의 인터뷰에서 "미국이 선택하는 장소와 시간 및 방법에 따라 비례적으로 대응할 것"이라고 말했다.[14] 이를 두고 일부 전문가들은 "미국이 자위권을 행사한 것"이라고 했지만 이는 잘못된 평가다. 민간회사에 대한 사이버 공격은 국가에 대한 무력공격과 달리 자위권으로 대응할 수 없기 때문이다. 국제법상으로도 자국민보호를 위해서 자위권 개념을 원용할 수 없다. 미국의 조치를 '굳이' 국제법적 관점에서 보면 자국민의 권리 침해를 구제하는 대응조치나 보복조치에 해당한다.

둘째, 오바마 대통령은 북한의 사이버공격이 전쟁 행위가 아니라는 점도 분명히 했다. 영화 상영을 막을 목적으로 사이버공격을 감행했다하더라도 이는 미연방수정헌법이 최고의 덕목으로 여기는 표현의 자유를 침해하기 때문에 미국의 가치를 훼손하는 행위임에는 분명하다. 그러나 공격 대상이 국가나 국가 기간산업, 중요 인프라도 아닌 민간회사라는 점은 전쟁행위로 볼 여지를 주지 않는다. 오바마 대통령은 사이버테러(cyber terror)라는 용어도 쓰지 않았고 사이버 파괴주의(cyber vandalism)라는 새로운 용어를 사용했다. 이는 미국 정부의 신중한 태도를 반영한다. 테러와 관련한 국제조약은 14개나 있지만 '국가간에 합의된 테러에 대한 정의'는 없다. 또 14개 조약 모두 테러 행위의 주체를 비국가행위자(non-State actor)로 한정할 뿐 국가는 포함시키지 않는다. 이는 국제법상 국가테러리즘(state terrorism)이라는 관념이 존재하지 않는다는 의미다. 국가는 '국가지원테러(state-sponsored terrorism)'라는 개념으로만 다뤄지며 따라서 테러지원국이라는 비난만 받을 수 있다. 북한이 사이버 공격을 해도 국제법에 따르면 국가테러리즘이 성립하지 않기 때문에 테러행위라고 비난할 수 없다. 그러나 한국의 헌법은 북한을 반국가단체나 테러집단으로 규정하고 있으므로 북한의 사이버공격으로 남측 민간에 공포심이 야기되면 북한을 사이버테러의 주체로 꼽아도 무방하다. 그러나 다른 나라에 이를 주장하고 설명할 때는 용어에 주의할 필요가 있다.

셋째, 이번 미국정부의 대응은 공공-민간 파트너십(public-private partnership)이 원활하게 이뤄졌음을 보여주는 대표적 사례다. 사태 초기에 소니는 협박에 굴복, 영화 배포와 상

영 계획을 취소했지만 오바마 대통령이 유감을 표시하자 이를 철회했다. 이는 민관이 적절한 대화를 통해 공동 대응한 좋은 사례로 꼽힐 수 있을 것이다. 그리고 이러한 민-관 파트너십은 비슷한 사이버환경과 법제를 가진 우리에게도 위기에 대응하거나 사이버 공격을 억지하는 데도 중요한 선례가 될 수 있다.

넷째, 공격행위의 귀속문제를 확정하는 데 한미공조가 한 몫 했다. FBI는 "북한에 책임이 있다"고 발표하면서 공격에 동원된 수단이 2013년 3월 한국의 은행과 미디어에 대한 공격 당시와 유사하다고 지적했다. 수사단계에서 한미 간에 디지털 증거와 관련한 원활한 사법공조가 이뤄졌음을 암시한다. 다만 우리에게는 다소 부담이 되는 측면도 존재한다. 필자는 앞에서 2013년 3월 20일의 공격을 북한 소행으로 규정한 우리 정부가 무슨 대응 조치를 했는지 알 수 없다고 지적했는데, FBI가 '북한의 3월 20일 사이버 공격'을 재확인함으로써 '한국 정부는 앞으로 북한에 대해 어떤 조치를 취할 것인가'라는 의문을 거듭 갖게 만들었다.

다섯째, 미국은 2015년 1월 2일 북한 무기산업에 대한 금융제재 조치를 발표하면서 '보복의 첫 조치(first step in retaliation)'라고 표현했다.[15] 2014년 12월 23일 이후 며칠간 북한의 인터넷망이 마비되거나 불안정해지는 일이 벌어졌고 12월 27일 저녁에는 3G 이동통신망이 4시간 이상 완전 마비되거나 불통 상태가 됐다. 미국의 '동일 보복 조치(retaliation in kind)'에 따른 사태로 보였지만 미 정부는 이를 공식 확인해 주지 않았다.

금융 제재는 사이버상의 '동일 보복 조치'와 성격이 다른 별도의 교차보복조치(cross-retaliation)로 보인다. 이는 북한의 열악한 인터넷 상황과 사이버 의존성을 감안할 경우 북한의 사이버공간에 취해지는 동일 보복조치는 효율적이지 못하고 제한적이기 때문에 다른 종류의 보복조치인 교차보복조치가 고려된 것이다.

여섯째, 미국은 '사상 최초로 미국 영토에서 벌어진 파괴적 사이버공격'이라는 위기 의식에 기초해 '단호하고 즉각적인' 조치를 취했다. 이 같은 '단호함과 즉각성'은 억지력의 바탕이 되기도 한다. 위기의식은 2015년 2월 26일 미국 국가정보국 제임스 클래퍼 국장의 상원 증언에 잘 나타나 있다. 그는 "2014년은 다른 나라가 주도하는 파괴적 사이버 공격이 미국 영토에서 벌어진 최초의 해"라면서 이란의 2014년 2월 Las Vegas Sands Casino사 공격과 북한의 11월 소니 공격을 예로 들었다.[16] 여기엔 아마도 2009년 북한의 미 정부사이트 DDoS공격 때 '파괴적 공격도 아니고 귀속문제도 확정할 수 없다'는 이유로 강력히 대응하지 못한 데 대한 전략적 고려가 반영돼 있다고 볼 수 있다. 자국 영토 내에 벌어진 외국의

파괴적 사이버 공격으로 자국 민간 기업이 피해를 입은 사태로 국민 보호에 철저한 나라로 여겨졌던 미국의 자존심은 바닥으로 떨어진 상태였다. 급기야 4월 1일 오바마 대통령은 사이버 공격을 국가안보에 심각한 위협을 초래하는 국가비상상황으로 규정하고 사이버 범죄 주체에 대해 미국 내 자산동결 등 경제제재 조치를 취할 수 있는 행정명령에도 서명했다.[17] 2009년 단호하고 즉각적인 대응(보복)이 억지와 연결돼 있음을 간과한 미국은 2014년 큰 대가를 치른 셈이다.

5. 우리 정부에 대한 정책 제언

사이버공격을 100% 완벽하게 방어할 수는 없다. 이점을 고려해 Clarke와 Knake가 언급한 사이버전 능력의 세가지 구성 요소인 '공격력·방어력·의존성'을 중심으로 정부에 다음과 같은 제언을 한다.

첫째, 남북의 사이버 성숙도와 의존성의 차이로 발생하는 비대칭적 취약점을 보완하고 북한이 사이버공격을 하려는 유혹을 못 품게 하려면 가장 먼저 사이버 방어력을 최대한 강화해야 한다. 공격력을 키우는 방식으로 사이버전 능력을 향상하려면 남북 간의 '사이버 긴장'을 충분히 통제할 수 있을 만큼 압도적인 공격력을 가져야 하는데 그게 어렵기 때문이다.

북한의 사이버공격으로 긴장이 고조되면 우리의 사이버 대응 공격만으론 상황을 종결할 수 없다. 북한의 사이버 인프라와 사이버 환경은 아주 열악하며 외국 네트워크와 연결도 잘 안돼 있고, 국가가 망을 소유하고 운영하기 때문에 한국이 1차 대응 공격을 해도 북한은 즉시 외부와의 연결을 차단해 피해를 최소화할 수 있기 때문이다.

그러나 한국은 그렇게 할 수 없다. 디지털경제가 활성화된 우리 사회가 사이버 의존성을 줄이는 것은 시대의 흐름에도 역행해 거의 불가능할 뿐 아니라 경제에도 커다란 타격이 온다. 결국 북한의 사이버전 능력이나 사이버공격에 대한 최선의 대응은 방어력을 높이는 것뿐이다. 비대칭적 취약성 때문에 한국이 상황을 통제할 수 없는 상황에서 공격력을 강화하면 오히려 북한의 공격을 유도할 수도 있다.

둘째, 사이버 방어력 강화와 병행해 억지전략을 마련해야 하며 사이버전과 관련한 명확한 교리와 태세도 확립해 공개해야 한다. 오는 5월에 발표될 것으로 보이는 사이버 국가안보전략은 이 점을 분명하게 제시해야 한다. 북한이 1차 공격을 할 경우 우리가 선택할 보복

조치를 명확히 밝혀야 억지력은 확충된다.

셋째, 억지력 향상에 더해 복원력을 강화하는 전략도 사이버 국가안보전략에 반드시 담겨야 한다. 사이버공격을 100% 막기 어렵기 때문에 공격으로 인한 피해를 얼마나 빠르고 원활하게 복구할 수 있는지도 매우 중요하다. 경제적 피해가 가장 큰 관심사인 민간부문에는 복원력이 매우 중요한 쟁점이므로 명확한 입장과 비전을 제시하면 민간의 신뢰를 얻는 데도 보탬이 된다. 결국 우리의 대북 사이버전 대응력은 방어력, 억지력과 복원력에 있음을 염두에 두고 사이버 국가안보전략은 이 세 요소를 어떻게 증강할 것인지에 대한 로드맵을 보여주는 것이 돼야 한다.

넷째, 새로 임명될 사이버안보비서관은 기술적 방어 능력 향상은 물론 사이버전략에 관한 명확한 입장과 비전도 제시해야 한다. 관련 국제규범을 발전시키는 데도 적극 참여해야 하며 전략 개발을 총괄해야 한다. 민-관 파트너십 형성을 위해 민간과의 대화에도 시간을 많이 할애하는 전략적 마인드를 가져야 한다. 국제공조도 매우 중요하기 때문에 국제적 감각도 갖춰야 한다. 이런 인사를 구하기 힘들면 어느 한쪽이라도 제대로 갖춘 인사를 임명한 뒤 시간을 두고 두 덕목을 모두 갖출 수 있게 기다려주고 또 이를 위해 투자해야 한다.

다섯째, 청와대 국가안보실은 사이버전과 관련, 비전통안보라는 전략적 담론 차원의 논의를 펴면서 대비책을 마련해야 한다. 사이버공간이 약점이 아니라 장점이 될 수 있게 해야 하며 사이버안보를 군사적으로만 접근하지 말고 인간안보(human security)차원에서 운용할 수 있는 계획을 마련해야 한다. 예를 들어 인간안보와 관련된 인권문제 역시 사이버공간에서 활용될 수 있다.

1. 사이버안보(cyber security)와 관련해서는 행위와 침해유형 등에 따라 여러 가지로 구분해 볼 수 있는데, 사이버심리전, 사이버첩보(cyber espionage), 사이버범죄(cyber crime), 사이버테러(cyber terror)와 사이버전(cyber warfare) 등이 있다. 이 글은 국가전체에 단계에 이르는 공격(state-level attack)을 일컫는 사이버전과 거기에는 미치지 못하는 사이버공격에 집중해서 논의하고자 한다.
2. 마스터부트레코드란 운영체계가 어디에 어떻게 위치해 있는지를 식별하여 컴퓨터의 주기억장치에 적재될 수 있도록 하기 위한 정보를 의미한다.
3. 볼륨부트레코드는 NTFS 구조에서 가장 앞부분에 위치하는 영역으로 파티션되지 않은 장치의 시동 섹터이다.
4. KAIST 정보보호대학원 임채호, 김명철 교수 등이 계산한 것으로 시스템 복구 비용, 매출이익 손실, 생산효율 저하 등 직접 피해액은 1,361억 원으로 조사됐고, 사이버 테러 예방을 위한 투자비용 등 간접 피해액은 6,600만 원, 이미지 손상, 신뢰도 하락, 주가 하락, 법적 보상 등 잠재적 피해액은 7,310억 원으로 집계된 바 있다. 중앙SUNDAY, "피해액 8,672억 --- 정부 민간 컨트롤타워 구축 시급" (2013.9.7) 참조. http://sunday.joins.com/article/view.asp?aid=31373.
5. ASPI, Cyber Maturity in the Asia-Pacific Region 2014 (April 2014)
6. Ibid., p. 11.
7. Richard A. Clarke & Robert K. Knake, Cyber War (2012), p. 148.
8. 소니 해킹사건과 관련한 법적 평가는 신창훈, "소니 해킹사건의 국가안보적 함의", 북한 사이버테러 위협과 대응전략 (국가안보전략연구원, 국가보안기술연구소 공동 학술회의 자료집, 2015), pp. 51~66 참조.
9. 1,500만불은 소니가 추정한 피해액으로 자세한 내용은 "$15 Million: Cost Of Damages Following Massive Sony Pictures Hack", *Tech Times* (2015.2.5) 참조. http://www.techtimes.com/articles/30801/20150205/15-million-cost-of-damages-following-massive-sony-pictures-hack.htm.
10. Richard A. Clarke & Robert K. Knake, Cyber War (2012), pp. 23~25.
11. 중요 인프라에 대한 정확한 정의를 찾을 수는 없지만 일반적으로 전력망(power grid), 교통체제, 금융기관 등을 의미한다.
12. Tallinn Manual on the International Law Applicable to Cyber Warfare, p. 124 참조. 당해 매뉴얼은 http://nuclearenergy.ir/wp-content/uploads/2013/11/tallinn_manual.pdf에서 다운로드 할 수 있음.
13. 이러한 결론에 대해 FBI는 세가지 근거를 제시하고 있다. 첫째, 이번 공격에 사용된 데이터 삭제 악성코드의 기술적 분석 결과 북한의 행위자가 이전에 개발한 것으로 FBI가 알고 있는 다른 악성코드와 연결돼 있다는 것이 밝혀졌다. 예를 들어 코드의 특정 라인, 암호화 알고리즘, 데이터 삭제 방법 및 감염된 네트워크에 유사성이 존재했다. 둘째, 이번 공격에 사용된 인프라와 미국 정부가 이전에 북한에 직접적으로 연결시킨 다른 악의적 사이버 행위 간에 중요한 중첩을 발견했다. 예를 들어 FBI는 몇몇 IP주소가 이번 공격에 사용된 데이터 삭제 악성코드에 변경이 곤란하게 기록된 IP주소와 통신한 북한 것으로 알려진 인프라와 연계돼 있다는 사실을 발견했다. 셋째, 별개로 소니 공격에 사용된 수단이 지난 해 3월 북한이 수행한 한국의 은행과 미디어에 대한 사이버공격과 유사성을 지

니고 있다. http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation 참조.

14. 인터뷰 내용은 http://cnnpressroom.blogs.cnn.com/2014/12/21/cnns-candy-crowley-interviews-president-barack-obama/에서 볼 수 있다.
15. Carol E. Lee and Jay Solomon, "U.S. Targets North Korea in Retaliation for Sony Hack: New Sanctions Target Individuals Working for Arms Industry," *Wall Street Journal* (3 January 2015).
16. 2015년 2월 26일자 증언의 원고는 http://www.dni.gov/files/documents/2015%20WWTA%20As%20Delivered%20DNI%20Oral%20Statement.pdf에서 다운로드 받을 수 있다.
17. "북 사이버공격은 미 국가비상상황", 문화일보 (2015.4.2), 1면 및 3면 참조.

신창훈 박사는 아산정책연구원 연구위원으로 국제법 및 분쟁해결센터장을 맡고 있다. 서울대에서 전기공학사, 법학 석사, 영국 옥스퍼드 대학에서 법학 박사를 수여 받았다. 주요 연구분야는 국제법 일반이론, 해양법, 분쟁해결절차, 국제환경법, 국제인도법, 대량살상무기 관련 국제조약 등이다. 2010년부터 2013년까지 국제해사기구(IMO)에서 투기에 의한 해양오염방지를 위한 런던의정서에 의해 설립된 준수그룹의 위원으로도 활동한 바 있다.

94340
9 791155 701003 비매품
ISBN 979-11-5570-100-3
ISBN 978-89-97046-06-5(세트)

WWW.ASANINST.ORG