제4차 산업혁명시대의 사이버안보위기 대응책

유현국
(예비역 준장)

1. 들어가는 글

추석명절 연휴 기간 중 모처럼의 여유 시간에 영화 〈남한산성〉을 보았다.

많은 사람들이 이 불행한 역사 속 상황을 두고 여러 가지 문제점들을 지적하는데, 필자는 우리 선조들이 이전에 경험하지 못한 치욕의 아픔을 겪을 수밖에 없었던 가장 큰 이유는 한 마디로 '준비 부족'이라고 생각한다.

우리는 역사의 교훈을 바탕으로 과거의 잘못을 되풀이 하지 않으면서 안정적이고 지속적인 발전을 도모하기 위해 많은 노력을 기울이고 있다. 그러나 현재를 제대로 읽지 못하고 미래를 내다보지 못하는 방향성 없는 노력, 무엇이 정말 중요한 것인지 우선순위를 제대로 판단하지 못하고 주변의 각양각색의 소리에 중심을 잃고 전략적 판단 없이 눈앞의 실리들을 좇는 보여주기식 노력은 결국 위기를 자초하는 지름길이 될 것이다.

'강자가 살아남는 것이 아니고 살아남는 자가 강자'라는 말이 있다. 오래 살아남으려면 매사 미래에 대한 준비가 잘 되어야 한다. 즉 국가 차원에서 볼 때, 위기(crisis)를 대비하여 미연에 방지하고, 위기가 발생할 때는 조직적이고 효과적인 대응 및 조치로 그 피해와 영향을 최소화함으로써 조기에 위기 이전의 상태로 복구할 수 있는 위기관리(crisis management) 능력을 평소에 갖추어야 강한 국가가 될 수 있는 것이다.

한 국가가 위기관리 능력을 잘 갖추려면 국가자원의 원활한 운용을 담당할 조직과 이를 뒷받침하는 법령 등의 마련이 선행되어야 한다. 특히 북한의 직접적인 위협과 직면해 있고 주변국들의 이익이 첨예하게 대립하고 있는 우리나라의 상황 하에서는 안보 위기에 관한 한 보다 세심하고 면밀한 대비가 요망된다.

우리는 현재 전쟁양상의 변화에 따라서 국가안보 환경이 전통적 의미의 군사적 위기는 물론 국가의 지속 가능한 발전을 위협하는 모든 비군사적 위기를 망라하여 이로부터 국민과 영토, 주권, 핵심기반의 안전을 보장해야 하는 '포괄적 안

보(comprehensive security)'의 시대에 살고 있다. 특히 우리가 비전통적인 위기에 관심을 가져야 할 이유는 컴퓨터와 인터넷의 급속한 발전에 따른 새로운 위기 환경의 등장 때문이다.

따라서 이 글에서는 비전통적 · 포괄적 신안보위협인 '사이버 안보'에 대한 이해를 돕는 한편, 국가 사이버 안보 강화를 위한 소견을 간략히 제시하고자 한다.

2. 평시의 전쟁, 사이버전과 사이버 안보에 대한 올바른 인식

초연결(hyper-connectivity) 사회로 대표되는 제4차 산업혁명시대가 도래함에 따라 보다 더 지능화, 고도화 되고 있는 '사이버 위협'은 국민의 재산과 기본권뿐만 아니라 국가 안보와 직결되는 양상을 보이고 있는 실정이다.

컴퓨터와 인터넷이 유례없이 빠른 속도로 발전하면서 예기치 못한 다양한 혜택과 더불어 부정적인 측면에서의 영향력이 크게 확산되어 전 세계 500대 기업 중 97%가 해킹을 당했으며, 100개 이상의 정부가 온라인 영역에서의 전쟁을 준비하는 시대가 되었다.

2000년대 들어 우리나라에서도 공공 부문은 물론 민간 부문에 대해서까지 대상을 가리지 않고 무모하게 감행되고 있는 북한의 사이버 공격이 국가적으로 심각한 위협으로 인식되면서 조속한 대응능력 및 '사이버 안보' 위기관리 능력 구비의 필요성에 대한 요구가 커지고 있다.

흔히들 사이버전을 '사이버 공간에서 이루어지는 전쟁'으로 단순하게 정의를 내리거나, 심지어 군사작전의 보조적 기능 정도로 인식하는 사람들도 있다. 다시 말해 기존의 지 · 해 · 공중전에 더하여 새로운 공간에서의 전쟁이라는 전장의 개념으로 국한하거나, 전쟁의 새로운 수단 정도로 이해하는 경향이 있다.

하지만 현실은 그렇지 않다. 사이버전은 이미 지금 이 시간에도 치열하게 벌어지고 있는 상시 전쟁이 되어 있다. 급속한 정보화의 이면에 우리 사회 전반에 걸쳐 존재하는 사이버 분야의 취약성은 국가 안보의 안정적 관리 능력에 대한 재정비와 보완을 요구하고 있다. 세계 정보통신기술(ICT)을 선도하고 있는 우리나라에 구축된 정보통신기반이 사이버 공격의 표적이 되기에 이르렀고, 사이버 공간에서의 단순한 피해가 아니라 국가적 차원의 실제적 물리적 피해로 연결되어 단 한 번의 공격으로도 국가 전체의 안보 기반을 붕괴시킬 가능성이 높아지고 있는데다가, 이로 인하여 국가 간에 직접적인 무력 충돌로 이어질 개연성도 배제할 수 없게 됨으로써 국가 안보에 심대한 영향을 미치는 매우 중요한 국가 위기 요소가 되었다.

과거와 달리 사이버 영역과 수단이 대부분의 국가안보 구성요소와 연결 또는 중첩되어 상호 의존적으로 작용하고 있다. 그리고 사이버공격 또한 해킹, 악성코드 유포, DDoS 공격 등의 다양한 유형이 존재하고 있는데다가 스턱스넷(Stuxnet)과 같이 공격대상에게 물리적 피해를 가할 수 있는 사이버무기체계까지 등장하였으며, 사이버 위협의 주체도 국가의 단위를 넘어서서 불법테러조직, 개인에 이르기까지 주체의 범위가 넓어지는 등 사이버 안보의 개념이 확장되고 있다. 이러한 현실을 고려할 때 사이버 안보는 국가의 총력적 안보역량 차원에서 심도 있게 다루어지고 준비되어야 한다. 특히 점차 광범위해지고 있는 북한의 사이버 공격뿐만 아니라 새로운 위협이 될 것으로 예상되는 국제적

적대세력에 의한 사이버 공격까지도 대비할 수 있는 능력의 확보에 실기하지 않기 위한 국가적 노력이 절실히 요망된다.

3. 국가 사이버 안보 능력 강화를 위한 제언

가. 사이버 안보 관련 기본 법률 제정

세계 각국이 사이버 위협의 심각성을 인지하고 경쟁적으로 사이버전 수행능력을 증강시키는 요즘, 어느 나라보다도 사이버 위협에 대한 노출 수준이 높은 우리나라도 사이버전력 증강을 위해 많은 노력을 기울이고 있으나, 아직도 제도적, 법적 기반이 미흡하여 위기 발생 시 마다 수세적 후속조치 차원의 대처에 머무르면서 근본적인 대안을 마련하지 못하고 있는 실정이다. 특히 우리는 사회 전 분야에서 정보통신기술(ICT), 사이버 인프라에 대한 의존도가 높은 반면 상대적으로 낮은 보안의식 등으로 인하여 사이버 위협에 치명적인 약점을 상시 노정하고 있으므로 이를 극복하기 위한 법제도의 마련이 시급하다.

사이버 위기관리 체제를 구축해오는 과정에서 컨트롤 타워를 설치하고 사이버사령부 창설 및 사이버 전문인력 양성 방안 시행 등의 노력을 해왔지만, 법률이 일률적이지 않고 산재되어 있어 중복 규정, 모순 규정이 발생하는 등 다양한 비효율을 초래하고 있다.

일례로서 사이버안보를 담당하는 주요기관을 보면, 우선 인터넷침해대응센터는 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 그 설립근거를 두고 있고, 국군기무사령부 예하 국방정보전대응센터는 국군기무사령부령 제1조에서 정보통신기반보호법 제8조의 규정에 의하여 지정된 주요정보통신기반시설에 대한 기술적 지원 가운데 국방분야에 관한 사항을 관장하기 위해 국군기무사령부를 둘 수 있도록 하고 있어서 이를 근거로 설립되었으며, 국가정보원 내 국가사이버안전센터는 국가사이버안전관리규정(대통령훈령 제222호)에 그 근거를 두고 있다. 이렇게 사이버안보 관련 주요기관들이 각기 다른 법적 근거 하에 존재함으로써 역할과 책임이 충돌하고 사각지대가 발생하는 등 다양한 비효율이 초래되고 있다.

이 외에도 사이버 안보와 관련하여 주요 실무기구들의 법적 활동 근거가 미비하거나 위기 상황 또는 이슈 발생 시 즉흥적인 법률 제정 관례로 인하여 법체계상 통일성이 결여됨에 따라 효과적인 사이버 대응업무 수행 및 조율에 어려움을 겪게 되는 경우가 발생하고 있다.

따라서 이런 문제점들을 해소할 수 있도록 사이버 안보에 관한 전체를 아우를 수 있는 기본 법률의 마련이 필요하다. 우리나라는 지난 10여 년 간 국가 차원의 사이버 위기 대응을 위한 법 제정 논의를 통하여 많은 전문가들이나 국민들이 그 필요성에 공감을 하고 있으며, 지금 국회에는 정부 입법안인 '국가사이버안보법'과 의원 입법안인 '국가사이버안보에 관한 법률안'이 제안되어 있다. 해를 거듭하면서 문제점으로 대두된 부분들에 대한 다각적 논의를 거쳐 수정 · 보완한 안으로 제안되었지만 결론적으로 국가정보원에 권한이 쏠리는 것에 대한 불안과 우려로 인하여 여전히 사이버 안보법 제정이 쉽지 않은 상황이다. 이러한 상황에서는 오로지 국가의 이익과 미래의 번영에 초점을 맞춘 정치적 리더십 차원의 결단과 우려를 불식시킬 수 있는 장치 마련을 위한 합의가 필요하다.

문재인 대통령도 국정원의 사이버 보안 업무에

대하여 국회 통제 장치를 강화하겠다고 밝힌 바 있다. 국회의 통제 강화를 통해 사이버 안보에 관하여 국내는 물론 국제 협력의 대표 기관으로서의 역량을 갖추고 있는 국정원에 대한 불신을 해소하는 것이 유용한 해법일 수 있을 것이다. 국정원 스스로도 국민의 신뢰를 얻기 위하여 노력해야 함은 물론이다. 한편으로는 국가정보원이 아닌 행정안전부 또는 과학기술정보통신부 등을 주무부처로 하는 방안도 고려할 수 있을 것이다. 이러한 과정을 통해 조속한 법제화를 실현시켜 관련 기관의 권한과 책임을 확정하고 감시 체제를 갖추는 등 사이버 안보 기능의 법적 기반을 마련할 수 있기를 기대한다.

나. 사이버 안보 협력체계 구축

사이버 위협은 앞에서 살펴본 바와 같이 그 확장성과 치명성으로 인해 국가 안보기관 단독 능력이 아니라 공공과 민간을 망라한 전 영역에서의 책임 있는 관계자들의 역량을 결집할 때 비로소 효과적인 대응이 가능한 것이다.

우리나라는 2000년대 초반부터 국가 차원의 사이버 위협 대응역량을 구축하기 위한 정책을 지속적으로 추진해 오면서 국가사이버위기관리매뉴얼 수립, 국가사이버안전센터 설립을 통한 정부 기관 간 협업체제 구축, 관계부처 합동으로 "국가 사이버 안보 마스터플랜" 수립 및 민·관·군 합동대응팀 구성을 통한 국제협력 강화 등 5대 전략 20개 추진과제 선정, 청와대 안보실이 사이버 위기 발생 시 컨트롤 타워 역할을 하고 국정원이 실무총괄을 담당하며 국방부 등 관계 중앙부처가 소관분야를 전담하는 대응체계 구축, "국가 사이버안보 종합대책" 마련 및 그 후속조치로서 분야별 세부대책인 "정보보호산업 발전 종합대책"과 "금융전산 보안강화 종합대책" 시행 등 다양한 노력을 기울여 왔으며, 특히 한수원 해킹 사건을 계기로 수립된 국가 사이버안보태세강화방안은 국가적 역량 결집에 관하여 중대한 전환을 맞이하였다. 기존 전략들이 정보와 대응역량의 중앙 집중적 체계 수립 및 강화에 중점을 뒀던 반면, 태세강화방안은 각급 공공기관과 주요 민관기관의 자체 보안역량 강화를 바탕으로 국가가 이들 간의 신속한 협력을 가능하게 하는 관리·조정 기능을 담당하도록 하는 것이었다.

그러나 이러한 시도에도 불구하고 사이버안보를 위한 협력체계는 아직도 다양한 이해당사자간의 역량이나 인식 차이, 그리고 각급 기관과 주체들의 역할과 권한이 불명하여 체계가 완전히 자리잡지 못하였고, 이를 위한 제도적 뒷받침이 충분히 이루어지지 않고 있다. 이에 따라 사이버 안보 위해의 예방, 탐지, 대응, 조사 각 단계에서 기관 간의 역할이 불명하여 역량의 중복, 대응 수단과 주체의 판단 지연, 민-관 및 정부기관 간 정보공유 실패와 같은 문제들이 지속적으로 발생하고 있으며, 정보공유나 협력의 필요성에 대한 공감대가 충분히 형성되지 못하여 상시적 협력체계가 원활하게 작동하지 못하고 있는 실정이다.

따라서 국가 차원에서 일원화된 사이버 안보 위기관리 절차(예방-탐지- 대응-복구)를 수립하고 각 단계에서 사이버공간에서의 위협과 테러, 그리고 전쟁 상황 등에 효과적으로 대응 할 수 있는 민 · 관 · 군 · 경의 각 구성 요소의 역할과 총체적 협업 관계를 설정하여 보다 체계적이고 합리적인 업무수행을 가능케 함으로써 평시 예방활동으로부터 유사 시 피해 확산을 방지할 수 있는 체계를

구축해야 할 것이다.

4. 맺는 글

거부할 수 없이 새로운 물결로 우리에게 다가온 제4차 산업혁명시대에 살아가면서 구시대의 틀로 급변하는 안보 환경에 대응하는 것은 적절하지 않다. 우리 생각부터 획기적으로 바꾸고 새로운 안보 환경에 부합하는 제도와 조직의 틀을 갖춰 신속하고 융통성 있는 대응이 가능한 정책 수립을 통하여 사이버 안보를 강화해야 한다.

앞서 제시한 사이버 안보 관련 기본법 제정과 새로운 개념의 민 · 관 · 군 · 경이 함께하는 협력 체계 구축도 중요하지만, 사이버 안보 업무체계를 강화하기 위한 획기적인 개혁과 함께 국가 차원의 전 국민 통합 대응을 위한 '사이버 리더십' 또한 대단히 중요한 부분이다. 지속적으로 발생되는 사이버 문제는 관심 소홀, 특히 조직의 최고위 리더들의 무개념과 무방비에서 비롯되는 경우가 대부분을 차지한다. 리더로부터 모든 구성원들이 사이버 안보에 대하여 정확하게 인식하고, 불편하더라도 세부적으로 대비하는 행동이 절실히 요구되며, 아울러 우리가 일상적으로 사용하는 사이버 공간을 전 국민이 국가 주권을 수호하기 위한 전장으로 인식하고 각자 사이버전사로서의 역량을 갖추도록 관심을 가져야 할 시기이다.

끝으로, 국가는 국가 차원에서 사이버 안보 관련 미래로드맵을 설계하여 공동기술 연구 및 개발과 관련 산업의 육성 및 인재 양성 등에 주력하고, 이러한 내부적 역량 구축을 넘어 국제 협력 및 정책 공유 체제를 구축하는 등 제4차 산업혁명시대 안보 환경에 적합한 사이버 안보 위기 대응능력을 철저하게 '준비'함으로써 조속히 미래 강한 국가로서의 기틀을 마련하기를 소망한다.

글 | 유현국

필자는 예비역 육군 준장(육사35기)으로서, 현역 복무 기간 중 다양한 부대에서 지휘관 및 참모 직위를 역임하였으며, 군 발전과 국가 안보에 기여한 공을 인정받아 보국훈장천수장과 보국훈장삼일장 등 주요 훈장 및 표창을 수상하였고, 전역 후 국가위기관리실 정보분석비서관으로서 대통령을 보좌하여 국가위기관리업무를 수행하였으며, 현재 단국대학교 국가위기관리연구소 자문위원과 사단법인 미래안보산업전략연구원 이사장으로 사회 공헌을 위한 노력을 지속하고 있음.