안보정책의 새로운 과제와 과학기술의 대응

2014. 05. 14

홍 현 익
(세종연구소 수석연구위원)

순서

1부 안보정책의 새로운 과제

2부 북한의 WMD 및 무인기 위협

3부 북한의 사이버 위협 대응

1부: 안보 정책의 새로운 과제

1. 전통적 안보 과제

- 국가를 기본단위로 국외적 위협, 주로 군사적 침략 및 위협으로부터 국가와 국민을 보호.

- 가상적국의 군사공격 억지를 위한 세력균형과 동맹, 그리고 군사적 우위 확보를 위한 군비 강화와 상호간 군비통제 및 군축.

1부: 안보 정책의 새로운 과제

- **2. 탈냉전기 안보개념의 확대 : 인간안보**
- (human security)

- 냉전 종식으로 군사안보의 중요성 약화.

- 안보대상을 국가에서 개인으로 전환 : 경제적 고통, 기아, 에너지 부족, 환경 파괴, 마약거래 등 초국가적 범죄, 인권침해, 불법 이민도 개념에 들어옴.

- 그간 등한시되었던 경제·식량·자원·환경·인구·건강·개인·공동체·정치 등 비군사적 영역의 위협 부각.

1부: 안보 정책의 새로운 과제

- **3. 네트워크 국제관계와 안보**

- 국제정치의 기본 구조를 국가 및 비국가행위자 등 행위자를 중심으로 보기보다는 이들간의 복합적인 연결망(네트워크)으로 보아야 한다는 것.

- 행위자 중심으로 안보를 본 국가안보나 글로벌안보보다 국제(international)안보를 중시 : 특히 탈냉전기 가장 두드러진 위협이 테러인데, 테러조직의 활동이 다국적 네트워크에서 이루어짐.

1부: 안보 정책의 새로운 과제

- **3. 네트워크 국제관계와 안보**

- 초국가적 네트워크 속에서 만들어지는 환경과 생태적 위기, 복합적 금융위기, 테러위협 등은 과거보다 더 불안정하고 불확실한 세계위험사회(world risk society)를 예고.

- 글로벌 차원의 안보 공공재 문제를 해결하는 과정에서 구성원들이 항의(voice)나 충성(loyalty)과 같은 전통적 참여방식보다 이탈(exit)의 대안을 선호하는 새로운 딜레마 발생.

1부: 안보 정책의 새로운 과제

- **3. 네트워크 국제관계와 안보**

- ‘예측’과 ‘통제’라는 근대적 사고방식에 입각한 기대(anticipation)전략(위험회피전략)보다 조직능력, 지식, 경제적 부, 에너지, 커뮤니케이션 등을 축적하는 등 능력을 배양해 적극적으로 대처하는 탄성(resilience) 전략 필요.

- 세계화 및 네트워크화로 인한 국가의 ‘공동화(hollowing out)’ 현상을 다국적, 초국적, 지역적 거버넌스로 보완해야 함.

2부: 북한의 WMD 및 무인기 위협

- **1. 핵 개발**

- 북한이 1980년대 말부터 핵 개발에 박차를 가해 2006년, 2009년에 이어 2013년 2월 핵실험을 감행하였고, 현재 4차 핵실험 감행 동향을 보이고 있음.

- 이미 세 차례의 핵 실험으로 1.5-3t 정도의 핵탄두를 만들 능력은 보유했을 것으로 추정. 4차 핵실험을 감행할 경우 1t 이하 무게의 핵탄두를 만들 가능성이 있음.

- 플루토늄을 30-50kg 보유한 것이 확실한 북한은 2,000개 이상의 원심분리기를 가동하여 연간 40kg의 고농축우라늄도 생산하고 있을 것으로 추정됨.

2부: 북한의 WMD 및 무인기 위협

- **1. 핵 개발**

- 고농축우라늄으로 핵 탄두를 만들면 시험이 필요없을 정도로 폭발력이 좋고, 북한에 2,600만t 정도의 풍부한 우라늄이 매장되어 있으므로 중장기적으로 대량생산이 가능.

- 미국이 현재 북한의 핵 보유를 결코 용인하지 않겠다고 하지만, 수년 후에는 이미 사실상 가져버린 것을 어떻게 하겠느냐고 하면서 핵 확산 자제와 사실상의 핵 보유 인정을 교환할 가능성이 있음. 1994년 처럼 미국이 영변의 핵시설을 공습하겠다고 나설 경우에도 한국은 안보딜레마에 빠질 것임.

2부: 북한의 WMD 및 무인기 위협

- **2. 미사일 개발**

- 북한은 이미 부산까지 가격할 수 있는 800기 이상의 미사일을 보유하고 있음.

- 각각의 미사일은 750kg 정도의 탄두를 운반할 수 있으므로 북한이 남한 전역을 가격할 수 있는 500기 이상의 핵미사일을 보유하는 시점이 임박함.

- 또한 미사일을 이동해서 어디서나 발사할 수 있는 이동용 발사대도 200대가량 보유하고 있음.

2부: 북한의 WMD 및 무인기 위협

- **3. 북한의 핵미사일에 대한 한국의 대응: 북한 핵 보유에 대비한 대북 억제력 강화 방안**

- **1) 한국의 핵 개발?**
- **2) 미국의 전술핵 재배치?**
- **3) 미국의 동북아 MD에 참여?**
- **4) 대북 선제타격 전략?**
- **5) 현실적인 대안**

2부: 북한의 WMD 및 무인기 위협

- **3. 북한의 핵미사일에 대한 한국의 대응**
- **1) 한국의 핵 개발?**
- 기술적으로 가능하지만 대가가 너무 커 실현가능성 희박
- 한·미동맹에 심각한 위기 초래
- 한국 경제에 심각한 타격 불가피
- 북한의 핵 개발을 저지할 명분을 포기하는 것을 의미.
- 중국도 용인하지 않을 것

2부: 북한의 WMD 및 무인기 위협

- **3. 북한의 핵미사일에 대한 한국의 대응**

- **2) 미국의 전술핵 재배치?**
- 고려될 수는 있지만 실현 가능성은 그다지 크지 않음.
- “핵없는 세상”을 주창하여 노벨 평화상을 받은 오바마.
- 북한의 핵 개발을 막기 어렵게 됨.
- 중국과 러시아의 반발
- 대미 의존 증대로 한국의 자주성 저하

2부: 북한의 WMD 및 무인기 위협

3) 미국의 동북아 MD에 참여?

- 손실이 더 큼. 한국형 MD 체제를 강화하는 것이 더 나을 것.
- 미사일이 남한에 도착하는 데 3-4분. 효과적인 작동 어려움.
- 북한의 미사일이 적어도 500기 이상; 우리의 요격 미사일 숫자는 한정되므로 MD에 과도한 기대를 가지는 것은 부적절.
- 미·중 대결에 한국이 희생될 수. 물론 미·중 정면 대결시에는 당연히 미국의 MD에 전면적으로 참여해야 할 것임.
- 전면 참여시 한·중 대립구도 형성에 따른 불이익을 감수해야.
- 막대한 비용 : 현재로서는 그 비용으로 대북 억지력 강화를 위한 헬리콥터나 정밀타격무기를 구입하는 것이 더 효과적.

2부: 북한의 WMD 및 무인기 위협

- **4) 대북 선제타격 전략?**
- 북한의 도발에 대해 강력히 경고하고 임전무퇴와 초전박살의 결의를 표명한 것. 북한의 핵공격 임박이 100% 확실하다면 옳은 판단과 각오.
- 대북 억제 군사전략으로 채택하는 것은 신중히 고려해야.
- 전쟁에 대한 결정권은 국군최고통수권자인 대통령 권한.
- 북의 동향이 대남 공격인지를 100% 확실히 판단할 수 있느냐의 문제(인공위성 등 정밀 감시능력 보유 필요).
- 북한 핵무기 여러 개, 이동용 차량에서 발사 가능: 위치 파악 어려움. 전면전으로 이어질 가능성. 북한 핵무기를 모두 일거에 제거할 수 있을 정도로 선제공격이 100% 완벽하지 않다면 매우 위험할 수.

2부: 북한의 WMD 및 무인기 위협

- **5) 현실적인 대안**

- 한·미동맹 강화로 확장억제에 의한 핵 억제력 확보; 북한의 핵공격시 자동적으로 평양에 미국의 핵폭탄이 투하되도록 보장받아야.

- 대량확증파괴능력을 갖춰 북한 핵 공격시 북한을 확실히 전멸시킬 수 있음을 보여줌. 대북 공격 능력 제고: 800km 사거리 탄도미사일 조기 배치; 벙커버스터 등 강력한 공격무기 확충; 정밀유도무기 체제 강화.

- 반민족적 대량살상행위인 북한의 대남 핵공격을 억제하려면 우리도 북한에서 가장 소중한 가치로 여기는 김정은 일가에 대한 정밀 타격준비를 갖추고 북한 지도부가 이를 인지하도록 해야 함.

2부: 북한의 WMD 및 무인기 위협

- **4. 북한의 무인기 위협과 한국의 대응**

- **1) 문제점**

- 2014년 3월 24일 파주, 31일 백령도, 4월 6일 삼척에서 연속적으로 북한의 무인정찰기 발견. 모두 우리 군에 발각되지 않고 주민들의 신고로 발견. 군 방공방의 허점이 노정되었고, 파주 무인기는 발각되지 않은채 상공에서 청와대를 촬영하였으며, 백령도 무인기도 군의 주요시설을 촬영하였음.

- 영상 송수신 장치는 탑재되지 않았지만 사전에 입력된 좌표 상공에서 사진을 촬영하고 발진지점으로 복귀하는 기본 기능 구비. 시속 90km의 속도로 3-4시간 비행 가능하여 최대 423km 비행.

2부: 북한의 WMD 및 무인기 위협

- 문제는 날개폭과 길이가 2m 이내이므로 현재 우리 군 레이더에 포착되지 않음. 초보적인 정찰기능만 수행하는 것으로 평가되지만, 전자 제어장치를 장착하면 자폭기능을 추가할 수 있고, 복귀 연료를 빼고 3-4kg의 생화학무기나 핵물질을 가공한 Dirty Bomb을 적재하면 자폭 테러용으로 쓰일 수도 있다는 데 있음.

- 북한이 중동을 통해 밀수입해 5기 정도를 보유하고 있는 미국제 MQM-107D ‘Streaker’는 시속 925km, 상승 고도 12km로 휴전선에서 청와대까지 2분 40초면 도착해 타격을 가할 수 있다고 우리를 위협하기도 했음.

2부: 북한의 WMD 및 무인기 위협

2) 한국의 대응

- 우리 군은 이스라엘 라다의 RPS-42 저고도레이더(탐지거리 30km, 소형무인기는 10km) 10대를 연내 도입, 청와대 등 국가 중요시설과 서부전선의 주요 축선에 배치 예정. 전방 경계강화 위해 차기 열상감시장비(TOD)도 보강할 예정.

- 요격 : 낙탄·파편 피해를 고려, 독일 라인메탈사의 레이저무기 도입 검토. 대도시 이외 방어거점에는 벌컨포 등 기존 대공화기와 자주 대공포체계인 '비호'(K-30)에 휴대용미사일 '신궁'을 결합한 유도탄탑재 복합대공화기 배치 방안 검토 중.

- 우리 군도 4t의 폭탄을 장착하고 16시간을 비행할 수 있는 MQ-9 'Reaper' 같은 무인기를 개발·배치한다면 북한의 각종 도발을 억지할 수 있을 것임.

3부: 북한의 사이버위협 대응

- **1. 개념 정의와 북한의 위협 유형**

- 사이버공간 : 물리적인 위치와 관계없이 컴퓨터 네트워크 위에 구축된 가상의 활동 공간. 여기서 개인과 사회, 정보인프라와 실생활에 영향을 주는 정보의 작성, 수집, 처리, 전달, 사용 및 축적이 이루어짐.

- 사이버 위협의 분류 : 조셉 나이는 국가가 주체가 되는 사이버전, 경제염탐, 그리고 주로 비국가행위자가 가하는 사이버범죄와 사이버테러로 분류. 경제염탐을 사이버분쟁으로 대체할 수 있음.

3부: 북한의 사이버위협 대응

- 사이버범죄(cybercrime) : 외화벌이 수단으로 컴퓨터 네트워크에서 자행하는 범죄: 2011년 북한의 해커부대가 중국을 거점으로 한국의 게임사이트 등을 부정조작하여 수십억원의 전자머니 탈취.
- 사이버테러 : 컴퓨터체제와 정보통신망을 교란해 불특정 다수에게 대규모 피해를 주고 사회를 혼란시킴 : 2011년 4월 농협 서버 공격, 은행계좌 관련 파일 삭제; 2009-2011 한국의 민간, 정부, 군 사이트에 여러 차례 Ddos 공격을 가해 접촉불능 사태 초래.
- 사이버분쟁 : 2010년 11월 북한군의 연평도 포격 직전 전자교란(재밍)을 통해 우리 군의 대포병레이더를 무력화시킴.
- 사이버전 : 정보전(Information warfare)의 일환으로 국가나 이에 준하는 집단 사이에 사이버 공격과 방호를 수행하는 전쟁에 준하는 행위.

3부: 북한의 사이버위협 대응

- **2. 북한의 사이버 공격 능력**

- 북한의 사이버전 방호능력은 취약, 공격능력은 한국을 능가. 케빈 콜만 (미 테크놀리틱스 연) : 사이버전 의지는 러시아에 이어 중국, 미국과 같은 세계 2위, 공격능력 6위, 사이버정보평가 7위.

- 인프라 : 인터넷과 인트라넷의 이중화, 정보통신 인프라 부족과 국가독점 및 국가통제. 중국 단둥과 신의주를 잇는 광통신망을 통해 중국 차이나텔레콤으로부터 회선을 할당받아 중국 IP를 통해 인터넷을 이용. 중국 필터링 정책에 의해 걸러진 인터넷 콘텐츠에만 접근 가능. 북한 내부 인터넷 사용은 소수에 의해 독점·통제됨.

- 지도층의 관심과 투자 : 김정일 시대부터 사이버전력에 높은 관심과 지원. 김정은이 사이버전과 전자전을 직접 지휘. 국가전략 차원에서 사이버전 조직 관리.

3부: 북한의 사이버위협 대응

- 사이버 무기 체계와 기술 능력 : 전자적·논리적·심리적 무기체계를 고루 갖추고 다양한 공격 능력 확보 : 전자적 무기체계로 전자장치를 무력화시키는 EMP, GPS 신호를 교란시키는 GPS 재머(최대교란거리 100KM)를 개발하거나 이미 보유; 논리적 무기체계로 디도스 공격, 악성코드 개발, 역추적 방지 및 공격 우회기술, 해킹통신 암호화, 흔적 삭제 등 진화된 공격기술 구비.

- 사이버전 인력 양성 : 매년 미림대가 100명 이상 양성해 전원 인민무력부 정찰총국에 배속. 김일성군사대 매년 1,000여명 컴퓨터교육. 사이버전 관련 인원 3,000-30,000명 추산. 중요한 점은 최고 수준의 대우를 받아 인재들이 모인다는 것.

- 연구 개발 : 국방과학원 산하 정보전연구중심, 미림대학 정보전 연구센터, 제2경제위원회 연구부서들이 협동해서 정보전 수행에 필요한 각종 무기체계 연구·개발.

3부: 북한의 사이버위협 대응

- 수행 조직 체계 : 국방위 정찰총국에 해킹과 사이버전 전담하는 사이버전지도국(121국), 총참모부 직속 지휘자동화국(해킹·군관련·지휘통신 프로그램 개발)과 적공국(한국군 상대 사이버심리전), 통일전선부 소속 사이버 전담부서, 노동당 225국(옛 대외연락부) 소속 사이버 전담부서. 일선부대도 사이버전 능력 보유. 특히 전자전 부대는 평양권에 1개 연대와 전방군단에 각 1개 대대 배치.
- 사이버전 정책 : 이중적 태도 : 자기 공격 숨기고 외국 공격은 비난.
- 전략전술 : 기습·위장·기만·정보·심리·은폐·파괴 전술
- 국제협력 : 북한의 배후에 중국 사이버부대 넷포스와 협력 추정

3부: 북한의 사이버위협 대응

- **3. 사이버전에서 남한의 불리함**

- 북한의 사이버 공격 역량은 매우 위협적 : 북한은 비대칭전력으로 '사이버전력' 집중 육성. 한국은 IT 의존도가 높고, 남북한이 동일 어를 사용.

- 사이버전시 우리 피해가 더 심각할 가능성 : 북한은 폐쇄적인 정보통신망 운영, 컴퓨터 보급률 저조, 인터넷 감시·통제가 강하므로 북한 전산망 침투·공격이 어려움.

- 사이버 공격의 실체를 밝히기가 어렵다는 익명성 : 주로 중국에서 공격을 수행하므로 공격 역추적과 원점 식별 및 타격이 어려움.

- 대상과 범위 확대 추세 : 교통·통신·금융·전력망 등 기반시설 공격 가능성 증대.

3부: 북한의 사이버위협 대응

- **4. 한국의 사이버안보 현황**

- 한국은 IT 선진국 : 국내 인터넷 인구 3,400만명으로 세계 9위, 인구 비례 세계 5위. 초고속인터넷 가입자가 1,500만여명을 돌파하여 가입율 세계 4위. IT 조사자의 인원과 수준에서도 세계적인 경쟁력.

- 역설적으로 적대세력으로부터의 사이버공격에 취약성.

- 사이버전 대응체계 : 2005. 1. '국가 사이버안전 관리규정' 제정시부터 사이버안보에 대해 국가 차원의 대응 개시.

3부: 북한의 사이버위협 대응

- 대통령직할 국가사이버안전전략회의와 국가사이버안전대책회의, 국정원의 국가사이버안전센터, 국방부의 국방정보전대응센터, 미래창조과학부(옛 정통부)의 인터넷침해사고대응지원센터, 경찰청의 사이버테러대응센터. 그리고 부처별 사이버전 전담조직 보유.

- 국정원은 2009년 사이버전 전담조직 창설 : 당시 국정원, 방송통신위원회 등 15개 유관부처 합동으로 '국가 사이버안보 마스터플랜' 수립하고 '민▪관▪군 합동 사이버 위협 대응팀' 운영.

- 국방부 사이버사령부는 전문인력 500명. 고려대에 사이버국방학과 개설해 사이버보안 전문장교 육성.

- 2013년 방송사와 금융기관에 대한 '3▪20 사이버테러' 계기로 청와대가 직접 컨트롤타워 역할을 맡기로 함.

3부: 북한의 사이버위협 대응

- **5. 한국의 사이버안보 전략 추진방향**
- **1) 소극적 사이버방호 능력 구축**
- 국내 사이버 공간 침투 방지 및 침투시 피해 최소화하는 방호능력
- 주요기관 보안 전문인력 확충
- 사이버 위협에 대한 정보 공유와 사이버보안 교육 활성화
- 국가 주요 시설에 대한 망 분리 확대 및 의무화
- 사이버감내부대(Cyber Resilient Forces) 확보·편성
- 백신프로그램의 취약점 관리 및 철저한 검증
- 국가 보안정책의 거시적인 대응과 국민 개개인의 보안의식 제고를 통한 철저한 컴퓨터 관리.

3부: 북한의 사이버위협 대응

- **2) 적극적 사이버방호 능력 구축**
- 해외 사이버공격 거점을 색출, 해당국 정부에게 폐쇄를 요청하는 등 북한의 사이버공격을 능동적이고 원천적으로 차단.
- 북한의 사이버공격이 해외거점에서 수행되거나 해외망을 이용해 이루어지므로 공격에 이용된 IP를 추적하고 인적 정보(HUMINT)를 활용하여 사이버 공격 거점을 확인.
- '사이버안보 컨트롤타워'를 구축해야 함. 2013년 3·20 사이버테러 이후 청와대가 컨트롤타워 역할을 자임했는데, 전문 인력과 예산으로 이를 뒷받침해야 함.

3부: 북한의 사이버위협 대응

- **3) 사이버공격 능력 확보**
- 사이버공격으로 우리나라 국가기간 망이 파괴되고 인적·물적 피해가 발생한 경우 공격 주체 색출해 적절한 대응공격을 가해야.
- 미 국방부는 국가기간망을 흔드는 외부 사이버공격을 전쟁행위로 간주해 미사일공격 등으로 대응한다는 방침을 공표함.
- 지정학적 여건상 북한에게 군사 보복이 어려우므로 사이버공격 무기체계를 개발하여 우리가 피해를 받은 만큼 '비례성의 원칙'에 입각해 사이버 대응공격을 가하는 방법 고려.
- 국가사이버연습장을 설치해 사이버전의 종합연습, 장비 점검, 교육훈련 등을 실시해야 함.

3부: 북한의 사이버위협 대응

- **4) 사이버안보 기반 구축**
- 사이버방어 중심 전략에서 벗어나 사이버공격작전의 비중 강화. 북한 인트라넷에 대한 대응 공격 전략·전술 개발.
- 사이버전사 양성 : 교육훈련체계와 사이버병과체계, 공공과 민간의 사이버인력 활용체계 마련하고 합당한 대우와 보상체계 제공.
- 사이버전 연구 및 획득 체제 확립 : 사이버국방과학연구소 같은 사이버전 전문 연구기관 설립. 필요한 사이버공격·방어무기를 신속하게 충당하는 획득체제 구축.
- 민·관·군 정보 공유 및 상시적 협력 강화
- 국내 사이버 법체제 정비 : '국가사이버위기관리법' 제정.

3부: 북한의 사이버위협 대응

- **5) 국제협력**
- 국제적 차원의 사이버안보 규범 형성 노력 참여 및 주도.
- 북의 사이버 공격에 대한 대응공격을 위한 국제법적 근거 마련 및 국제 합의 도출.
- 한·미동맹의 사이버안보 협력 강화 및 사이버안보관련 다국 공동훈련 참가.
- 중국의 국제 사이버범죄 방지조약 가입 유도.
- 한·중간 사이버 수사 공조와 사이버안보 협력 방안 수립.
- 북한을 사이버 국제규범 논의 테이블로 유도.

3부: 북한의 사이버위협 대응

- **6) 기술적 대응전략**
- 논리적·전자적·심리적 공격·방어 기술 연구·개발
- 근원지 역추적 기술 연구·개발
- 사이버게놈기술 등 공격자 신원 확인을 위한 기술 연구·개발
- 사이버 공격 증거 확보를 위한 사이버포렌식기술 연구·개발
- 공격원점 사이버 타격기술 연구·개발
- 인터넷-인트라넷 망분리기술 연구·개발
- 인트라넷 침투 및 공격 기술 연구·개발 **–끝-**