Jeju Peace Institute
제주평화연구원

JPI 정책포럼

발행인 | 문태영 · 주소 | 제주특별자치도 서귀포시 중문관광로 227-24 (697-120) · Tel: 064)735-6500 · Fax: 064)738-6522 · www.jpi.or.kr

No. 2012-13

사이버 무기와 국제안보

장노순 (한라대학교 교수)

국제안보 및 평화구조에 도전할 수 있는 위협 요인은 확대·심화되고 있다. 하지만 무기 발전과 무력 위협은 여전히 국제안보의 불안 요소로 계속해서 작용하고 있는 당면한 문제이다. 핵무기의 도래가 강대국 간 평화를 보장했지만, 정보통신기술의 발전과 인터넷의 상호연계성은 국가와 비국가 행위자에게 사이버 공간에서 공격과 방어의 새로운 사고를 요구하고 있다.

2010년 중반 이후 이란의 핵시설이 Stuxnet 사이버 무기의 공격을 받았고 일정 수준의 피해가 발생했다. 사이버 공간에서의 안보위협은 결코 최근 등장한 안보 이슈가 아니지만, Stuxnet은 과거와 전혀 다른 특징을 보여주었다. 이는 국제안보구조와 국가안보전략 측면에서 변화의 불확실성과 불안전성을 고조시키고 있다.

국가가 주도적으로 사이버 무기를 개발하고 적대세력의 산업시설을 공격하면서 나타난 결과는 이전과 성격이 다른 사이버 무기의 등장, 다른 유형의 전쟁 가능성, 국가와 비국가 행위자의 결합, 방어전략의 수단과 실행의 애매성, 사이버 무기의 확산과 통제 등이다. 본고는 이에 관한 문제를 이해하고 국제질서의 안정화 방향을 고민하고 있다.

* JPI정책포럼 세미나(2012. 10. 12) 발표자료임.

목 차

1. 문제제기

○ 국가 차원에서 사이버 전쟁(cyber warfare)을 시도했던 사례가 외부에 드러난 적은 거의 없었음.[1] 그러나 지난 수년간 국가가 주도했거나 국가 차원의 지원 및 방조 속에서 상대국가에 대한 사이버 공격의 사례가 발생하고 있음. 최근 이란의 우라늄 농축시설을 공격하는데 이용된 Stuxnet이라는 사이버 무기는 '군사용 사이버 미사일(military-grade cyber missile)'로 비교될 만큼 국제안보와 평화에 새로운 패러다임의 전환을 요하는 것으로 평가되고 있음.

– 이란의 핵개발을 저지하기 위해 이스라엘의 공중 폭격에 대한 대안으로 사이버 무기 개발과 사이버 공격의 전략이 마련되었음.

○ 이는 기존의 사이버 공간(cyber space)에서 벌어진 사이버 공격과 근본적으로 성격이 다르다는 특징을 갖고 있음. 기존 사이버 공격의 행위자는 해커와 범죄 집단 혹은 특정한 비정부 세력들로 금전적 목적이나 자기 과시적인 이유 그리고 정보를 수집하려는 목적으로 행해졌음. 그러나 Stuxnet은 국가가 주도하거나 제3의 세력을 지원하여 상대국가의 정보통신시스템을 공격하여 무력화하거나 파괴하려고 시도하였음.

– 사이버 공간은 인간 노력의 산물, 역동성, 신속성, 경계 불확실성, 저비용의 진입, 급성장, 다양한 형식의 변화 등을 특징으로 보여줌.

○ 국가의 주도적인 계획과 의도가 반영된 사이버 공격은 사이버 전쟁이라고 할 만큼 공세적인 안보위협이고, 국제안보질서의 불안정성과 분쟁 가능성을 새로운 형태와 방향으로 변화시키고 있음. 이는 기존의 안보구조 및 특성과 전혀 다르기 때문에 사이버 안보전략과 사이버 위협에 관한 국제규범을 조정해야만 하는 환경을 조성하였음.[2]

2. 사이버 공격의 최근 경향

가. 사이버 전쟁의 사례

1) 2007년 4월 에스토니아(Estonia)에 대한 디도스(DDoS: Distribute Denial of Service, 분산서비스 거부) 공격

○ 구소련의 연방에 속했던 에스토니아는 2007년 4월 27일 단순한 사이

버 수단을 동원한 사이버 공격을 받기 시작하였고, 30일에는 좀비 컴퓨터를 활용한 정교한 공격을 당하였음. 즉, 디도스 공격의 규모가 더욱 증가하였고, 공격의 시점에 대한 조율도 나타나기 시작하였음. 에스토니아 디도스 공격은 많게는 85,000여 대의 컴퓨터가 동원되었고 3주간이라는 유례없는 장기간에 걸쳐 계속되었음. 러시아의 2차 세계대전 전승기념일인 5월 9일 디도스 공격이 최고조에 이르렀음. 이 시기에 58개의 에스토니아 주요 웹사이트가 서비스를 중단하였고, 에스토니아 최대 은행이 이틀에 걸쳐 90분 그리고 2시간 정도 온라인 서비스를 제공하지 못했음. 사이버 공격은 5월 19일 종료되었음.

- 에스토니아는 전체 인구의 2/3가 인터넷을 활용하고 있고 은행거래의 95%가 인터넷을 통해 이루어질 만큼 세계에서 인터넷의 사회적 연계망이 잘 구축된 국가임.
- 2차 세계대전 당시 히틀러에 대한 러시아의 전승을 기념하기 위해 에스토니아 수도 탈린(Tallinn)에 러시아의 무명용사 동상이 건립되어 있었음. 에스토니아 정부는 이 무명용사 동상을 도시 외곽으로 이전하기로 결정하였고, 이에 대해 에스토니아의 친 러시아 주민들과 러시아는 분노하였음. 이는 거리 시위로 발전하여 1,300여 명이 체포되고 100여 명이 부상당했으며, 1명이 사망하는 격렬한 폭동 시위로 발전하였음.

○ 에스토니아에 대한 디도스 공격은 장기간에 걸쳐 정부와 민간 및 기업을 망라한 대상을 포함하고 있고, 에스토니아 사상 최악의 사이버 공격이었지만 피해와 사회적 후유증이 심각하지 않았음. 또한 나토(NATO)는 회원국으로서 에스토니아의 지원 요청에 대해 이번 사이버 공격이 군사대응을 요하는 범주에 들어가지 않는다고 규정하고 지원을 거부하였음.

- 그러나 사이버 공격이 종결된 이후, 나토는 사이버 방어를 지원하기 위한 상설 부서(the Cooperative Cyber Defence Centre of Excellence)를 에스토니아에 설치하였음.
- 에스토니아는 디도스 공격의 주체를 파악하는 데 실패하였음. 러시아 정부가 배후에 있을 것이라는 심증이 있었지만, 러시아 정부의 개입을 확증하는 증거를 확보하지 못했음. 유럽위원회(European Commission)와 대서양 동맹국들(Atlantic Alliance)의 전문가들도 공격의 배후 세력을 밝히지 못했음.

국가 차원에서 사이버 전쟁(cyber warfare)을 시도했던 사례가 외부에 드러난 적은 거의 없었음. 그러나 지난 수년간 국가가 주도했거나 국가 차원의 지원 및 방조 속에서 상대국가에 대한 사이버 공격의 사례가 발생하고 있음

2007년 4월 에스토니아에 대한 사이버 공격이 종결된 이후, 나토는 사이버 방어를 지원하기 위한 상설 부서(the Cooperative Cyber Defence Centre of Excellence)를 에스토니아에 설치하였음

2) 2008년 7월과 8월 조지아(Georgia)에 대한 러시아의 디도스 공격

○ 지리적으로 러시아의 남쪽에 위치하고 구소련 연방의 일원이었던 조지아는 2008년 8월 러시아와 영토를 둘러싸고 군사충돌이 있었음. 조지아는 러시아와 접경 지역인 오세티아(Ossetia) 분리주의자들에 대한 군사공격을 가했으며 러시아는 하루 뒤에 조지아 군에 반격을 가함으로써 군사충돌이 발생하였음.

○ 러시아의 조지아에 대한 사이버 공격은 군사충돌이 발생하기 열흘 전쯤인 7월 말 시작되었고 대규모 사이버 공격은 군사충돌이 일어나는 8월 8일에 일어났음. 조지아에 대한 사이버 공격이 무력충돌과 병행해서 이루어졌다는 점이 특징임. 7월 1차 사이버 공격은 미국 소재의 상업 웹주소를 둔 컴퓨터를 이용한 조지아 대통령의 웹사이트 공격이었음.

- 러시아로부터의 디도스 공격은 조지아의 웹사이트를 압도하였지만, 공격자의 신원을 파악하지는 못하였음. 그러나 조지아 디도스 공격에 사용된 'Machbot' DDoS Controller는 러시아 해커들이 즐겨 사용하는 것이었기 때문에 사이버 공격이 러시아와 연계되어 있을 것으로 추정하였음.
- 조지아에 대한 1차 사이버 공격은 규모, 양태 및 결과를 보면 사이버 전쟁보다는 사이버 범죄로 평가되는 것이 더 적합한 판단임. 따라서 군사 조직에 의한 군사적 대응이 적절하지 못하다고 여겨질 수 있음.
- 인터폴(Interpol) 혹은 미국의 입장에서 보면 FBI가 수사하여 처벌하는 접근 방식이 군사 대응보다 타당할 수 있음을 의미하는 것임.

○ 2008년 8월 8일, 조지아에 대한 2차 디도스 공격은 1차에 비해 훨씬 광범위하게 이루어졌음. 특히 2차 디도스 공격은 러시아군이 남부 오세티아 지역으로 진입하는 작전과 함께 발생했다는 점에서 전례가 없는 새로운 방식의 사이버 공격이었음. 일부에서는 사이버 공격이 재래식 군사공격과 병행해서 일어난 최초의 사례로 평가됨.

○ 조지아에 대한 러시아 소재 비정부 조직들의 사이버 공격은 크게 세 가지 방식으로 이루어졌음.

- 첫째, 조지아의 주요 웹사이트를 공격하여 조롱하는 것임. 조지아 국립은행이나 외교부의 웹사이트에서 조지아 대통령과 히틀러를 동시에 게시하여 정부의 위신을 실추시키려 했음.
- 둘째, 정부와 주요 민간 웹이사트를 공격하여 기능을 마비시키는 디도스 공격을 실행하였음.

- 셋째, 조지아를 전 방위로 공격하기 위해 악성 소프트웨어를 배포하여 인터넷을 이용하는 일반 시민들로 하여금 조지아를 공격하도록 유도하였음.

○ 조지아에 대한 사이버 공격의 진상을 조사하기 위해 미국의 정부와 민간인 전문가들은 '그레이 구스(Grey Goose)' 프로젝트를 진행하였음. 이들은 조지아 공격에 대한 사이버 공격이 러시아의 해커, 정부의 지원을 받은 요원들, 사이버 시위자들이 합세하여 일어났다고 결론을 내림.

- 조지아 사이버 공격은 일종의 핵티비즘(hactivism)으로 평가되기도 함. 집단적인 시민운동으로 정치적 목적을 위해 컴퓨터를 활용하는 형식이고, 평범한 컴퓨터 이용자들이 사이버 공격을 주도했음을 강조하는 것임.

○ 조지아는 사이버 공격을 받고 정부의 공식 웹사이트가 제 기능을 발휘하지 못하고 국민과의 정보교류가 정상적으로 이루어지지 않는 상황에 처하게 되면서, 미국의 TSHost와 Google에 조지아의 인터넷 역량을 재구축하는 '사이버 피난(cyber refuge)'을 감행하였음. 미국 정부의 공식적인 지원과 협력 없이, 조지아 정부는 미국의 인터넷 기업과 상호 협력 체제를 구축하여 사이버 공격에 맞서는 전략을 마련하였음. 이들 미국의 인터넷 회사에 대한 러시아의 사이버 공격이 시도되었으나, 조지아의 사이버 시스템은 보호되었음.

3) 2010년 이란에 대한 Stuxnet Worm 공격

2008년 8월 조지아에 대한 2차 디도스 공격에 대해 일부에서는 사이버 공격이 재래식 군사 공격과 병행해서 일어난 최초의 사례로 평가함

○ 2010년 6월, 미국의 주요 언론과 세계적인 인터넷 보안업체들은 이란을 겨냥한 새로운 형태의 사이버 공격이 있었음을 보도하기 시작하였음. 벨라루스의 한 컴퓨터 보안회사는 특정 유형의 ICS(산업제어시스템)를 공격하기 위해 고안된 악성 소프트웨어 Stuxnet 웜(worm)을 발견하였음.

- Stuxnet의 공격 대상인 ICS는 원자력 발전소 혹은 우라늄 농축시설을 제어하는 컴퓨터 시스템임. SCADA(Supervisory Control and Data Acquisition, 감시통제 및 데이터요구 시스템)의 일종이 ICS임.
- Stuxnet의 목적은 독일 지멘스(Siemens)사가 만든 ICS가 활용하는 마이크로소프트 윈도우를 기반으로 응용되는 프로그램을 공격하고 파괴하려는 것임. 이 웜 바이러스는 인터넷과 차단된 네트워크에서 USB 혹은 CD를 통해 감염되었고, 나중에는 인터넷에 연결된 컴퓨

터를 감염시켜 확산되었으며, 보안프로그램에 의해 감지되는 것을 피할 수 있는 역량을 갖추고 있음.

2010년, '세계 최초의 정밀유도 사이버 무기'로 평가되는 Stuxnet이 이란 주요 핵시설을 공격하였음. 미국과 이스라엘은 Stuxnet 공격의 책임을 공식적으로 인정하지 않았지만, 전문가들과 언론은 이들 국가들이 개발하여 사이버 공격을 실행하였다고 판단하고 있음

○ Stuxnet은 '세계 최초의 정밀유도 사이버 무기'로 평가되지만, 이 웜을 개발했다고 주장하는 주체가 없음. 그럼에도 불구하고, Stuxnet은 국가 차원에서 개발되고, 실행에 옮겨진 것으로 간주되는 이유는,
- 이를 개발하는 데 소요되는 막대한 비용을 뒷받침해야 한다는 점
- 기술적으로 정교한 웜 개발은 다양한 컴퓨터 전문가와 기술을 필요로 한다는 점
- 사이버 공격의 대상이 되는 시설과 시스템에 대한 정확한 정보를 파악하고 있어야 한다는 점
- 새로 개발된 웜 바이러스를 통한 사이버 공격의 효과를 검증하는 실험을 실행할 수 있어야 한다는 점
- 사이버 공격의 목적이 정보절취, 금전적 이익이 아니라 산업통제시스템을 목표로 설정하고 이를 마비시켜 파괴하려고 했다는 점 임.

○ 미국과 이스라엘은 Stuxnet 공격의 책임을 공식적으로 인정하지 않았지만, 전문가들과 언론은 이들 국가들이 개발하여 사이버 공격을 실행하였다고 판단하고 있음.[3)]
- 오바마 행정부는 이란의 핵시설에 대한 이스라엘의 공습이 불확실한 결과를 가져오고 지역의 불안이 고조된다고 판단하여 이스라엘의 지원 요청을 거부하였음. 그러나 이에 대한 대안으로 사이버 무기 개발과 사이버 공격을 장기간 계획을 세워서 추진하였음.
- 이스라엘은 1981년 이라크의 오시락(Osirak) 핵시설과 2007년 시리아의 핵시설을 공습하여 파괴하는 데 성공하였음.

○ 테러조직은 국가의 기간시설이나 산업시설에 대해 사이버 공격을 감행할 충분한 동기가 있고, 이를 공격하고자 하는 확고한 의지도 있음. 그러나 이런 산업통제시스템을 공격할 수 있는 역량을 갖추지 못했음. 또한 정교한 보안기술을 보유하고 있는 다른 조직과의 필요한 연대 관계를 아직까지는 구축하고 있지 못한 것으로 평가됨.

○ Stuxnet 공격으로 2010년 말 현재 6,000여 대의 컴퓨터가 감염되었고, 이 중 3,000여 대의 컴퓨터가 이란에 소재한 것으로 추정됨으로써 이번 사이버 공격의 주된 목표는 이란이라는 것이 전문가들의 일치된 견해임. Stuxnet은 주로 나탄즈(Natanz) 소재의 컴퓨터들을 감염시켰

음. 일부 전문가들은 Stuxnet의 공격목표가 우라늄 농축시설이었다고 지적하고 있기 때문에, 나탄즈의 우라늄 농축시설을 파괴하려는 것이 목적이라고 분석함.

- Stuxnet의 주요 공격 대상으로는 이란의 주요 핵시설이 있는 나탄즈와 부쉐르(Bushehr)로 추정됨. 나탄즈는 우라늄을 농축하는 시설이 있고 부쉐르는 원자력 발전소가 있는 장소임. 나탄즈에서의 핵활동을 제어하는 산업제어시스템(ICS)은 독일 지멘스사 제품이고, 반면 부쉐르 원자력발전소는 러시아가 원료를 공급하여 건설을 맡고 있음.
- 이란 고위 관리들은 Stuxnet 사이버 공격으로 이란의 피해가 미미하다고 주장하고 있지만, 국제원자력기구와 미국 CIA의 분석에 따르면 적어도 이란의 핵활동을 2년 정도 지연시키는 효과를 얻은 것으로 평가됨.

○ 이란 원자력 시설에 대한 사이버 공격 계획은 오바마 행정부 내내 지속적으로 발전되어 왔지만, 시작은 부시 행정부의 마지막 시기에 '올림픽 게임(Olympic Games)'이라는 비밀 프로젝트로 추진되었음. 오바마 대통령은 이스라엘이 요구하는 이란 핵시설에 대한 공중 폭격이 초래할 위험과 문제점을 극복할 수 있는 대안으로 사이버 공격을 준비하였음.

4) 기타 사이버 무기의 사용

○ 2010년과 2011년 Google은 중국 정부가 수백 명의 구글 이용자의 비밀번호를 절취하여 이메일을 감시하려고 시도했다고 주장함. 중국 정부는 사이버 공격의 배후와 관련이 없다고 부인함.

- 정보 획득을 위한 사이버 공격은 미국의 행정부 고위인사, 중국 재야 정치인사, 아시아 국가들의 고위인사, 군인사 혹은 언론인들을 대상으로 삼았음.
- 사이버 공격은 비교적 단순한 방식을 사용하였지만, 이메일 계정을 가로채기 위해 선별된 목표물에 대해 공격의 공조체제, 공격의 규모, 공격의 시발점은 국가 차원의 주도적인 역할이 있을 것으로 추정됨.

Stuxnet의 이란의 주요 핵시설에 대한 공격으로 이란의 핵활동은 적어도 2년 정도 지연되는 효과를 얻은 것으로 평가됨

○ 2012년 3월, 리비아에서 민주화 운동이 있고 정부군과 반군 사이의 내전 양상으로 발전하면서 반군을 지원하려는 서방은 리비아 정부군에 대한 공중포격전략을 세웠음. 그리고 미국은 카다피의 친위 방공망을 무력화하기 위해 사이버 공격을 시도할 것인지 여부에 오바마 행정부 내에서 논쟁이 있었음.

- 사이버 전쟁 혹은 사이버 공격에 대한 대통령 권한의 범위와 한계가 분명하지 않고, 안보전략적 중요성이 크지 않은 상황에서 미국의 사이버 공격 능력을 과시함으로써 노출되는 전략적 위험부담으로 인해 사이버 공격 계획은 실행에 옮겨지지 못함.

Stuxnet 공격은 지금까지 국가 차원에서 가장 체계적이고 조직적이며 치밀한 사전 계획과 준비 과정을 통해 이루어진 사이버 공격임

3. 사이버 무기와 국제안보

가. Stuxnet과 국제안보적 의미

○ Stuxnet 공격은 지금까지 국가 차원에서 가장 체계적이고 조직적이며 치밀한 사전 계획과 준비 과정을 통해 이루어진 사이버 공격임.
- 막대한 재정적 지원, 공격대상이 되는 외국의 산업시설에 대한 정확한 정보활동, Stuxnet 공격의 효과에 대한 사전 실험을 통해 정확한 공격목표를 최적의 효과를 거둘 수 있는 시점에 공격을 감행할 수 있도록 하였음.
- Stuxnet 공격 이후, Flame, Stars, Duqu 웜의 공격이 계속해서 이루어짐.

○ 산업시설을 운영하는 컴퓨터 시스템을 공격하여 시설을 마비시키고 파괴하려는 목표는 과거의 위협과는 목표가 전혀 달랐음. 또한 인터넷으로 연결되어 있지 않은 시스템(air gap)을 공격하는 방식도 기존의 공격 형태와 다름.
- Stuxnet 공격은 산업시설에 대한 방해와 파괴(sabotage)가 목적이었고, 과거의 주된 목표는 정보수집을 추진하는 간첩활동(espionage) 혹은 기존의 정권이나 권위를 와해시키려는 전복활동(subversion)이 주된 것임.
- 컴퓨터의 개인용 데이터 저장장치를 이용해서 사이버 무기를 옮기는 과정은 인터넷을 이용해서 사이버 공격을 감행한 방식과 다름.

○ Stuxnet 공격은 이스라엘, 미국, 독일 지멘스사, 영국 등의 국제 협력으로 이루어졌음.
- 이스라엘과 미국은 이란의 핵시설에 대해 사이버 공격을 위한 계획과 실행 과정에서 매우 긴밀한 협력을 유지했고, 독일과 영국의 지원도 있던 것으로 보임. 웜 바이러스의 효과를 실험하는 과정에서 이스라엘의 핵시설과 미국의 인터넷 보안 연구소 및 핵시설을 활용하였음.

○ Stuxnet 공격은 국가 차원의 사이버 공격이 공식적으로 활용되는 선

례를 만든 경우에 해당함. 미국과 이스라엘 정부 차원에서 준비되고 실행에 옮긴 사이버 공격은 사이버 무기를 이용하여 타국을 공격하는 위협 행위에 대해 정당성을 확인해주는 선례로 작용하고 있음. 이는 향후 이란과 기타 세력 그리고 중국과 러시아가 사이버 무기를 개발하고 공격의 수단으로 적극 활용하더라도 용인될 수 있는 상황에 들어선 것임.

- 실제로 이란은 Stuxnet 사이버 공격을 받은 이후, 미국 내 혹은 해외에서 미국의 국익을 위협하는 공격을 적극적으로 추진할 의지가 있음을 드러내고 있음.
- 2012년 미국의 주요 은행들은 중동지역에서 시작되는 사이버 공격을 과거에 비해 월등히 빈도수가 높게 받고 있고, Google 역시 국가 차원의 사이버 공격이 이루어지고 있음을 경고하였음.

○ 사이버 공격에 따른 부차적인 피해와 영향이 있었음.

- 이란의 핵시설을 운영하는 SCADA 시스템의 오염을 알지 못한 이란 과학자의 개인 컴퓨터 접속이 확산의 요인이 되었음. Stuxnet은 이란을 넘어서 파키스탄, 인도네시아, 미국, 독일, 한국 등에 소재한 컴퓨터를 오염시켰음. 2012년 6월 공격의 효력이 종료되었으나, 사이버 공격의 수단을 설계하는 방식과 예측하기 어려운 과정에 따라 피해의 규모와 확산의 속도를 예측하기 쉽지 않음.

○ 국가안보 차원의 사이버 전쟁과 치안 차원의 사이버 범죄를 주도하는 주체와 행위자들 간의 경계가 모호해짐. 조직 범죄와 사이버 범죄 집단은 좀비 컴퓨터(bonet)를 대여하거나 악성 소프트웨어를 만들어 사이버 공격의 수단으로 활용될 수 되도록 판매하는 암시장(black market)을 형성할 수 있음. 비국가적 행위자(non-state actor)의 안보 위협과 범죄 행위를 구분하는 기준이 현실적으로 모호해지고, 초국가적 행위자는 사이버 공격 수단을 사이버 범죄조직으로부터 구매하면 되기 때문에 공격의 방법과 과정이 다양하게 구사될 수 있음.

- 2011년 전 세계 사이버 범죄 시장은 120억 달러 규모로 추산되고, 이 중 1/3 규모를 러시아 범죄조직이 장악하고 있는 것으로 추정됨.[4]
- 미국 국방부는 2007년 43,880회, 2008년 54,640회, 2009년 상반기 43,785회 사이버 공격을 국방부가 받았다고 보고함.[5] 또한 미국의 네트워크에서 발견된 악성 소프트웨어의 규모는 2009년에 비해 2011년 3배 이상 증가하였고, 매일 6만 개 이상의 컴퓨터 파괴 소프트웨어가 발견되고 있음.[6]

Stuxnet 공격은 국가 차원의 사이버 공격이 공식적으로 활용되는 선례를 만든 경우에 해당함

나. 사이버 공격과 사이버 전쟁

사이버 무기와 사이버 공격에 대한 국제적 합의와 규범적 행동의 기준을 마련하는 것이 시급함

1) 국제안보 차원의 이슈

○ 사이버 무기와 사이버 공격에 대한 국제적 합의와 규범적 행동의 기준을 마련하는 것이 시급함.
- 사이버 공격에 대한 규정, 사이버 무기에 대한 규정, 사이버 공격과 국가의 대응 수준에 대한 수용 여부가 중요한 요소가 될 것임.
- 국제법적으로 다른 주권 국가에 대한 무력 '공격(aggression)'의 범주에 사이버 공격이 포함되는지를 결정하는 문제가 어려움. 또한 '무기(weapon)'의 범주를 어떻게 규정할 것인가도 사이버 무기와 사이버 공격에 대한 대응전략을 마련하는 데 핵심적인 요소가 됨.[7)]

○ 사이버 위협과 공격에 대해 군사동맹체제가 무력 공격으로 간주되고 동맹국을 지원할 수 있는지를 수용할 한계선(red line) 설정이 필요함.
- 에스토니아는 사이버 공격을 받았을 때, 나토의 회원국으로서 나토의 지원을 요청하였으나 나토는 군사적 혹은 사이버 대응 차원에서 지원을 거부함. 그러나 2차 사이버 공격을 당한 조지아는 사이버 피난을 시도했고, 미국의 인터넷 기업들은 조지아의 피난과 지원 요청에 적극적으로 협력하였음.
- 사이버 범죄와 사이버 전쟁의 애매한 경계는 사이버 공격을 안보 차원에서 대처하기에 기존의 국제규범과 제도를 약화시켜야 하는 부작용이 있음. 특히 에스토니아와 조지아에 대한 1차 사이버 공격처럼 전쟁의 범주로 분류하기 어려운 상황에서 국제사회의 적극적인 지원은 근본적인 한계가 있음.[8)]

○ 사이버 무기는 공격형 무기로 활용하기가 훨씬 용이하여 국제분쟁을 유발하는 결과를 초래할 수 있음. 사이버 무기는 성격상 방어용으로 활용되기보다는 공격용이고, 과거 어떤 무기보다 극히 짧은 극 초단위 시간에 공격이 이루어지기 때문에 방어보다 예방이 훨씬 중요하게 여겨짐.
- 국제정치의 공수이론(offense-defense theory)은 공격형 무기와 방어형 무기의 발전 시기에 따라 국제안보 질서의 안정성과 전쟁 발생 가능성이 밀접하게 연관성을 갖고 있다고 주장함.

○ 사이버 군비 경쟁(cyber arms race)이 나타날 가능성이 있음.
- 국제협력과 제도를 통해 사이버 무기를 통제하기 어려운 장애요인

들이 있음. 일반적으로 군비통제는 무기체계의 신고, 사찰, 검증과 협약 준수의 과정을 통해 이루어지고 있지만, 사이버 무기는 국가와 비국가 행위자들의 경계가 모호하고 사이버 무기의 사용이 시작된 지리적 공간에 대한 한계도 분명하지 않은 상태에서 재래식 무기와 같은 감시와 통제가 가능할지 의문임.

- 기존의 국가 간 관계는 사이버 우호관계(cyber relationship)와 사이버 적대관계(cyber belligerents)의 동맹체제로 강화되고 발전할 여지가 있음.

2) 국가안보 차원의 이슈

○ 사이버 안보(cyber security)는 공공부문뿐만 아니라 민간부문에서도 국가안보 차원의 심각성과 중요성을 갖고 있음. 국가의 안보와 안전 그리고 정부의 기본적인 활동이 방해받고 중단되며 물리적 피해가 발생한다면, 국가안보를 책임지고 있는 정부의 역량에 대해 국민의 신뢰성이 약화될 것임. 또한 국가의 경제활동과 안보 위상은 심각하게 침해받을 수 있음.

- 미국의 국토안보부는 2009년 오로라 프로젝트(Aurora Project)를 통해 미국의 발전소를 제어하는 SCADA에 대한 사이버 공격의 취약성을 평가하는 모의실험을 하였음. 그 결과 취약점을 발견하였고, 다른 부문의 기간 시설에서도 미국의 경제에 영향을 주고 물리적 피해를 초래할 수 있는 취약성이 있다고 지적하였음.

사이버 안보(cyber security)는 공공부문뿐만 아니라 민간부문에서도 국가안보 차원의 심각성과 중요성을 갖고 있음

○ 전쟁(무력위협) 관련 어떤 법률이 사이버 공격에 대한 대응전략을 결정하는데 적용되는지 국내제도와 규정이 보완되어야 함.

- 행정부의 무력사용 혹은 사이버 공격을 결정하는 권한은 의회와의 관계에서 통제될 수 있는 범주인지를 명확하게 규정하고 있지 못한 실정임.
- 사이버 공격에 따라 사이버 반격이 요구되는 시점은 언제인가?
- 사이버 공격(혹은 반격)을 결정하는 권한은 누구에게 있는가?

○ 사이버 공격으로 입게 되는 부차적인 피해를 최소화하는 방법은 무엇인가? 예컨대, 사이버 공격으로 민간병원의 전력이 중단되는 사태가 발생하는 경우에 행정부의 대응 조직과 제도적 뒷받침은 되어 있어야 함.

- 최근(2012년 8월) 미국은 정부뿐만 아니라 민간 기업이 관리하는 국가 주요 기간시설에 대한 사이버 공격에 대처하기 위해 정부의 엄격한 안보기준을 마련하여 입법화하려고 하였으나 상원에서 부결되었음.

○ 전력 생산, 식수 공급, 하수 처리, 가스 공급 등 주민의 생활에 필요한 주요 서비스를 제어하고 관리하는 SCADA 시스템에 대한 공격은 국가안보 차원으로 다루어지고 있는 경향이고 이를 보호하기 위한 대책 마련에 나서고 있음.

- 2008년 한 해 미국의 인터넷 관련 손실은 420억 달러이고 전 세계적으로 1,400억 달러의 손실을 입은 것으로 추산됨. 또한 전 세계적으로 민간 기업은 자료 절취로 1조억 달러의 지적재산권에 손해를 입고 있는 것으로 추산됨.[9] 미국의 정유와 가스 시설에 대한 사이버 공격으로 일일 최대 630만 달러의 손실이 발생할 수 있다는 평가도 있음.
- 조직의 가외성(resilience)과 유연성(flexibility)은 사이버 위협에 대비하는 조직의 특성임.

핵무기 혹은 재래식 무기의 억지전략은 선제 군사 공격을 감행한 국가에게 엄청난 보복을 통해 선제 공격 국가가 얻을 수 있는 이익보다 손실이 크다는 인식을 심어줌으로써 무력 공격을 단념시키는 것임. 결국 억지전략의 성패는 응징역량과 응징의지에 달려 있음

4. 사이버 무기와 안보전략

가. 사이버 억지전략

○ 핵무기의 도래는 기존의 전쟁에 대한 패러다임을 변화시켰음. 전쟁은 승리를 목적으로 무력 사용을 결정했지만, 핵무기를 보유하는 국가들은 전쟁의 승리보다는 전쟁의 예방이 주된 안보전략의 목표가 되었음. 이런 인식을 배경으로 미국과 소련이 전략적 사고와 판단으로 억지전략(Deterrence)을 채택하여 냉전시기 동안에 적용하였음.

- 억지전략은 거부(denial)와 응징(punishment)의 두 가지 방식으로 상대방의 공격을 예방함.[10] 공격에 기대한 효과를 거두지 못하도록 방어하는 것은 '거부' 방식이고, 엄청난 비용을 부담하도록 하는 방식이 '응징'임.
- 전략적 공군력 이론(Strategic Airpower Theory)은 재래식 억지전략을 적용한 논리이지만, 효과적인 안보전략이었는지는 의문임.

○ 핵무기 혹은 재래식 무기의 억지전략은 선제 군사 공격을 감행한 국가에게 엄청난 보복을 통해 선제 공격 국가가 얻을 수 있는 이익보다 손실이 크다는 인식을 심어줌으로써 무력 공격을 단념시키는 것임. 결국 억지전략의 성패는 응징역량과 응징의지에 달려 있음.

- 응징역량은 핵무기라는 확실한 파괴력을 보장하는 무기를 통해 응징능력을 과시했고, 응징의지는 선제 공격 국가가 반격하는 국가가 보복하겠다는 의지를 신뢰함으로써 결정되는 것이기 때문에 좀 더 많은 장애요인을 안고 있음.

- 억지전략은 확장 억지전략(extended deterrence)과 누적 억지전략(cumulative deterrence)으로 전략의 적용 범위와 방식을 넓혀갔음. 확장 억지전략은 냉전시기에 미소 강대국은 자국의 동맹국에 대한 다른 국가의 군사안보 위협을 예방하기 위해 미소 양국의 강력한 무력 보복을 다짐하는 군사안보전략이었음. 누적 억지전략은 이스라엘이 테러단체의 공격을 예방하기 위해 이들 테러 행위에 대한 보복으로 주변 국가들의 근거지를 무력 보복하는 전략이었음.

○ 냉전시기에 안보전략의 근간을 이룬 억지전략을 사이버 위협과 공격에 대해서도 적용할 수 있을지 회의적임. 사이버 위협에 대한 억지전략은 크게 두 가지, 공격자의 신원 혹은 속성(attribution)과 비대칭성 때문에 분명한 한계를 지니고 있음.

- 첫째, 사이버 공격자에 대한 응징은 공격자의 신원이나 소재를 분명하게 파악하고 있어야 가능하지만, 사이버 공격자는 사이버의 속성 때문에 자신들의 신원을 숨길 수 있음. 수십억 개의 IP 주소와 PC가 인터넷을 통해 연결되어 있는 인터넷의 연계성은 자신의 신상을 은폐하기가 매우 용이함.
- Stuxnet 웜의 개발과 공격 주체로 이스라엘과 미국을 대체로 지목하고 있지만, 이스라엘은 공식 부인하고 있고, 미국은 공식 대응을 전혀 하지 않고 있는 상태에서 아무도 이들 국가가 진범이라고 단정적인 증거를 제시하고 있지 못함.
- 둘째, 사이버 공격에 대한 억지전략은 사이버 공격자와 비대칭적 특성으로 인해 적용되기 어려움. 설령 테러단체의 공격자를 파악했다고 하더라도 이들의 지리적 소재와 응징 대상이 될 만한 목표물이 없는 경우가 흔하기 때문에 응징하는 것이 불가능할 수 있음.

냉전시기에 안보전략의 근간을 이룬 억지전략을 사이버 위협과 공격에 대해서도 적용할 수 있을지 회의적임. 사이버 위협에 대한 억지전략은 공격자의 신원 혹은 속성(attribution)과 비대칭성 때문에 분명한 한계를 지니고 있음

○ 사이버 공격에 대한 응징 수단으로 무력 사용에 대한 논의가 필요함. 사이버 공격에 대한 무력 보복은 군사력 사용의 기준으로 '비례성(proportionality)'에서 쉽게 수용하기 어려울 것임. 즉, 보복은 공격의 수준과 피해의 결과에 상응한 정도에서 이루어져야 한다는 것임.

- 지금까지 가장 일반적으로 나타나는 사이버 무기는 디도스 공격으로 국가 공공기관이나 주요 민간 기업에 대해 정상적인 활동을 방해하려는 목적에서 사용되었음. 따라서 인명이나 시설물 피해가 발생하기보다는 국가와 민간부문에서 경제적 손실이나 신뢰성 약화가 주된 피해 결과였음. 이런 수준의 사이버 공격에 대해 무력 보복은 국제법적 합법성과 윤리적 문제의 측면에서 정당성을 인정받기 어려울 것임.

- 사이버 공격에 대한 대응 수단과 범위는 사이버 공격이 발생한 상황과 결과에 의해 영향을 받을 것으로 보임. 만약 사이버 공격으로 인명 피해가 발생한다면, 무력 공격의 위협으로 간주될 여지가 높아지는 것임. 하지만 무력 응징의 정당성이 높아졌다고 하더라도, 무력 보복은 추가적인 장애요소를 극복했을 때만이 가능할 것임.

사이버 무기의 빠른 확산과 이를 이용한 사이버 안보위협의 현실화 가능성이 증대함에 따라 국가 간 협력을 통해 국제안보 질서의 안정성을 확보하려는 시도가 이루어지고 있음

○ 사이버 공격에 대응하려는 목적으로 사이버 국력(cyberpower)을 활용한 보복 행위는 여전히 현실적으로 실행에 옮기는 데 장애물이 있음.
- 첫째, 비대칭적인 수준에 있는 적대 국가를 응징하기 위한 사이버 무기를 사용하는 것이 어려움.
- 둘째, 사이버 무기를 동원한 사이버 응징은 공격 목표물을 겨냥하지만, 통제하기 어려운 사이버 무기는 병원, 상수원 등 다른 시설물에 대해서도 공격하여 인명을 살상하는 피해를 줄 수 있음.

나. 사이버 무기통제의 국제협약

○ 사이버 무기의 빠른 확산과 이를 이용한 사이버 안보위협의 현실화 가능성이 증대함에 따라 국가 간 협력을 통해 국제안보질서의 안정성을 확보하려는 시도가 이루어지고 있음.
- 사이버 범죄 유럽협약(Council of European Convention on Cyber Crime)
- 사이버 무기 통제를 위한 군비 통제와 사이버 공격을 예방하기 위한 국제적 노력은 국내 사법적 법집행기관과 국가안보기관이 국제적으로 상호 협력해야 하는 중층적 복잡성을 띠고 있음.
- 주권의 제약 조건, 공격의 불확실한 지리적 공간, 위협의 예방과 범죄 처벌에 따른 다른 법률적 제약과 절차 등 사이버 무기에 대한 국내 법집행기관이 전담하기에 충분치 못함.

○ 사이버 무기를 통제하기 위한 국제협력과 제도화는 핵무기, 화학무기, 미사일제한 협정과 같이 선례를 적용하는 데 한계가 있음.
- 러시아와 중국은 오랫동안 미국에게 사이버 무기 통제를 위한 국제협약을 체결하자고 노력하였지만 미국의 거부로 진척이 없었음. 미국은 러시아에 비해 군사력 우위를 유지하고자 했고, 러시아는 이를 견제하려는 외교적 목적에서 추진하였던 것임. 미국은 사이버 무기 개발과 로봇 기술에서 러시아와 중국보다 월등히 우위에 있고 이런 상대적 우위성이 통제되는 것을 거부했음.
- 미국의 오바마 행정부는 자국의 사이버 안보를 확보하고 사이버 국력

의 절대 우위를 유지하기 위한 국제안보전략을 추진하고 있음. NPT(핵확산금지조약)와 PSI(핵확산방지구상)의 국제협력체제는 사이버 안보를 위한 안보전략으로 목표와 과정에 대한 전략적 고려에 의해 다른 방향에서 고려될 수 있지만, 국제협력체제의 가능성과 그에 따른 추진 과정은 다음 행정부에서 훨씬 분명하게 나타날 것으로 보임.

5. 한반도의 안보정책적 의미

○ 사이버 안보의 중요성은 최근에 부상한 것은 아니지만, 새로운 유형의 사이버 무기와 사이버 공격의 방식은 한반도의 안보와 밀접하게 연관되어 의미를 갖고 있음. 2009년 7·7 디도스 공격, 2011년 3·4 디도스 공격으로 남한의 주요 정부와 민간 사이버 공간이 위협을 받았음.

- 정부와 민간부문에서 자료 절취와 훼손 그리고 국가의 정상적인 기능을 마비시키려는 시도가 있었으나, Stuxnet과 같이 특정 산업시설을 파괴하는 사이버 공격의 심각한 위협이 발생하지는 않았음.

○ 이란의 핵시설에 대한 사이버 공격에서 드러났듯이, 북한의 핵시설에 대한 사이버 공격이 불가능할 이유는 없음.

- 남한의 개입 여부에 상관없이 북한의 핵시설에 대한 사이버 무기 개발과 공격 계획이 현실화될 가능성은 항상 열려 있음. 미국은 유사한 전략적 목표를 갖고 있다고 알려져 있지 않지만, 향후 사이버 국력과 충분한 동기를 갖춘 국가는 사이버 무기 개발과 외교와 군사수단의 중간 단계로 고려할 수 있다는 것은 분명함.

이란의 핵시설에 대한 사이버 공격에서 드러났듯이, 북한의 핵시설에 대한 사이버 공격이 불가능할 이유는 없음. 이에 대해 남한은 법률적, 조직적, 전략적 준비가 필요함

○ 만약 북한의 핵시설에 대한 사이버 공격이 이루어진다면 남한은 법률적, 조직적, 전략적 준비가 필요한데,

- 첫째, 남한은 미국과 공조 체제를 마련해야 하는가? 미국과 이스라엘의 협력은 안보전략적으로 불가피한 결과이기도 하고, 이스라엘은 미국보다 우위를 보여줄 수 있는 정보환경적 강점으로 협력함.
- 둘째, 남한은 북한의 대응 공격에 방어할 수 있는가? 정부의 기능은 국가 주요 기간시설에 대한 보호와 민간부문이 담당하고 있는 주요 시설에 대해 방어할 수 있는 법적 제도와 협력관계가 갖추어져야 함.
- 셋째, 북한의 사이버 반격에 방어하는 조직체계는 구축되었는가? 안보담당 부서와 치안담당 부서의 역할 분담과 협력체제를 총괄하는 조직과 제도적 준비가 되어 있어야 할 것임.

저자 약력

▌장노순

現 한라대학교 경찰행정학과 교수. 한국외국어대학교 영어과를 졸업하고, 미국 Florida State University에서 정치학 석사와 박사학위를 취득하였음. 주요 경력으로 국정홍보처 전문위원을 역임했음. 주요 저서로 『국가정보학(공저)』, 『테러리즘(공역)』 등이 있고, 논문으로 「테러와 정보의 억지전략」, 「정보실패와 미 의회 정보감독의 정파성」 외 다수가 있음.

기획 및 감수: 이성우 (제주평화연구원 연구위원)
편집: 이지영 (제주평화연구원 연구원)
강지혜 (제주평화연구원 인턴)

주석

1) Nielsen(2012), pp.336-240.

2) 사이버 전쟁(cyber war)의 개념은 학자마다 다른 의미로 사용되고 있고, netwar, cyber warfare, electronic warfare, information warfare 등 유사한 용어들이 있음. 본 연구에서는 사이버 전쟁의 요건으로 (1) non-kinetic 수단을 이용한 컴퓨터 네트워크 공격(CNA)과 방어(CND), (2) 심리전의 목적에서 사이버 공간(cyberspace)을 이용하는 활동 배제, (3) 직접적인 정치 및 군사적 목적을 위한 컴퓨터 네트워크 공격과 방어 등으로 한정하였음(Liff, 2012: 404). 이 정의는 개인이나 집단의 사이버 범죄와 심리전 목적의 컴퓨터 네트워크 활동(CNO)을 배제시킴으로써 국가가 주도하는 국가안보와 분쟁에 초점을 맞추는 데 유리함. 또한, 최근 사이버 전쟁의 의미를 명확히 하는 장점이 있음. 이런 개념 규정은 인터넷을 기반으로 하는 포괄적인 위협, 범죄 혹은 군사적 활동을 강조했던 초기의 연구들과 구분이 됨(Ryan and Peartree, 1998; Schwartau, 2000; Arquillad Ronfeldt, 2001).

3) Raviv and Melamn(2012) and Sanger(2012).

4) Kramer and Perlroth(2012).

5) US-China Economic and Security Review Commission, 2009 Report to Congress (November 2009), p.68.

6) Rid(2012).

7) 유엔은 1974년 총회 결의안으로 '공격'을 한 국가의 군대가 다른 국가의 영토에 대해 폭격하거나 "다른 국가의 영토에 대해 한 국가가 어떤 무기의 사용"이라고 규정하였음. 미국 공군은 무기란 "사람을 살상하거나 거동을 못하게 하고, 혹은 자산에 피해를 입히고 파괴하기 위해 고안된 도구"라고 정의하였음. 산업시설이 '영토(territory)'에 해당되는지 그리고 사이버 무기는 무기에 관한 기존의 규정에 부합하는지에 관한 명확한 설명과 합의가 있어야 함.

8) Rid(2012) and Korns and Kastenerg(2009).

9) Buennemeyer(2011), pp.48-49.

10) Snyder(1961) and Jervis(1989). 억지이론에 바탕을 둔 억지전략은 미소 양극체제의 국제안보질서하에서 가장 합리성과 현실성을 인정받은 안보전략이었음. 핵무기와 재래식 군사력은 억지력의 신뢰성을 얻기 위한 기본 요소이기 때문에, 국가의 안보정책은 군사력 증강 그리고 상대국가와의 균형에 방향이 모아짐. 하지만 새롭게 등장한 초국가적 행위자의 안보위협과 안보위협 수단의 변화는 억지전략의 근간 유지 가능성을 지지하는 입장과 안보전략의 패러다임적 전환을 요구하는 입장으로 나누어놓고 있음.

참고문헌

Arquilla, John and David Ronfeldt, eds. *Networks and Netwars* (Rand, 2001).

Berman, Ilan. "The Iranian Cyber Threat to the U.S. Homeland," Statement before the U.S. House of Representatives Committee on Homeland Security (April 26, 2012).

Brown, Michael E. et al. *Offense, Defense, and War* (The MIT Press, 2004).

Broad, William J., John Markoff and David E. Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times* (January 15, 2011).

Clayton, Mark. "Stuxnet Malware Is 'Weapon' out to Destroy Iran's Bushehr Nuclear Plant?" *Christian Science Monitor* (September 21, 2010).

Farwell, James P. and Rafa Rohozinski. "Stuxnet and the Future of Cyber War," *Survival*, Vol.53, No.1(2011), pp.23-40.

Henry, Ryan and C. Edward Peartree, eds. *The Information Revolution and International Security* (The CSIS Press, 1998).

Jervis, Robert. *The Meaning of the Nuclear Revolution* (Cornell University Press, 1989).

Klimburg, Alexander. "Mobilising Cyber Power," *Survival*, Vol.53, No.1 (February-March 2011), pp.41-60.

Korns, Stephen W. and Joshua E. Kastenberg. "Georgia's Cyber Left Hook," *Parameters*, Vol.38(Winter 2008/09), pp.60-76.

Kramer, Andrew E. and Nicole Perlroth, "Expert Issues a Cyberwar Warning," *New York Times* (June 4, 2012).

Liff, Adam P. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *The Journal of Strategic Studies*, Vol.35, No.3(2012), pp.401-418.

Nielsen, Suzanne C. "Pursuing Security in Cyberspace: Strategic and Organizational Challenges," *Orbis*, Vol.56, No.3(Summer 2012), pp.336-256.

Raviv, Dan and Yossi Melman. *Spies Against Armageddon* (Levant Books, 2012).

Rid, Thomas. "Think Again: Cyberwar," *Foreign Affairs*, Vol.91, No.2(March/April 2012).

Rustici, Ross M. "Cyberweapons: Leveling the international Playing Field," *Parameters*, Vol.41(Autumn), pp.32-42.

Sanger, David E. "Mutually Assured Cyberdestruction?" *New York Times* (June 2, 2012), p.SR4.

Schwartau, Winn. *CyberShock* (Thunder's Mouth Press, 2000).

Sheldon, John B. "Deciphering Cyberpower: Strategic Purpose in Peace and War," *Strategic Studies Quarterly* (Summer 2011), pp.95-112.

Snyder, Glenn. *Deterrence and Defense* (Princeton University Press, 1961).

Sterner, Eric. "Retaliatory Deterrence in Cyberspace," *Strategic Studies Quarterly*, Vol.5, No.1(Spring 2011), pp.62-80.

US-China Economic and Security Review Commission, *2009 Report to Congress* (November 2009).

평화와 번영을 위한 제주포럼 2013에 초대합니다

평화와 번영을 위한 제주포럼은 2001년 한반도와 동아시아 지역의 평화와 공동번영을 모색하기 위한 역내 다자협력 논의의 장으로 출범, 외교 · 안보 · 경제 · 환경 · 여성 · 지역개발 등 다양한 분야의 최고 전문가들이 참여하여 매회 그 규모와 질적 성장을 거듭하고 있는 국제종합포럼입니다.

2013년 5월 개최 예정인 제8회 평화와 번영을 위한 제주포럼에 많은 관심과 참여 바랍니다.

평화와 번영을 위한 제주포럼 2013

- 주 최 제주특별자치도, 국제평화재단, 동아시아재단, 중앙일보
- 주 관 제주평화연구원
- 일시 및 장소 2013년 5월 29일(수)~31일(금), 제주도

2012 05.31~06.02
제7회 평화와 번영을 위한 제주포럼
"새로운 트렌드와 아시아의 미래"
김황식 총리, 오무르벡 바바노프 키르기즈스탄 총리, 폴 존 키팅 전 호주 총리, 람베르토 자니에르 OSCE(유럽안보협력기구) 사무총장, 한승수 전 총리, 스티브 워즈니악 애플 공동창업자 등 36개국 3,100명 참석

2011 05.27~29
제6회 평화와 번영을 위한 제주포럼
"새로운 아시아: 평화와 번영을 위하여"
글로리아 마파카발 아로요 전 필리핀 대통령, 김황식 총리, 자오지청 중국 인민정치협상회의 외사위원회 주임 등 23개국 1,880명 참석

2009 08.11~13
제5회 제주평화포럼
"상생과 공영의 동아시아 질서: 공동의 비전을 향하여"
반기문 유엔사무총장, 한승수 총리, 존 하워드 전 호주 총리 등 13개국 650명 참석

2007 06.21~23
제4회 제주평화포럼
"동북아시아 평화와 번영: 유럽 경험의 탐색"
노무현 대통령, 가이후 도시키 전 일본 총리, 예브게니 프리마코프 전 러시아 총리 등 13개국 500명 참석

2005 06.09~11
제3회 제주평화포럼
"동북아시아 공동체의 건설: 평화와 번영을 위하여"
이해찬 총리, 무라야마 도미이치 전 일본 총리, 첸치첸 전 중국 부총리 등 10개국 500명 참석

2003 10.30~11.01
제2회 제주평화포럼
"동북아 평화공동체의 건설: 도전과 새로운 비전"
노무현 대통령, 예브게니 프리마코프 전 러시아 총리 등 8개국 450명 참석

2002 04.12~13
세미 제주평화포럼
"21세기 세계 평화의 재검토와 평화의 확산"

2001 06.15~17
제1회 제주평화포럼
"동북아시아 공동평화와 번영"
김대중 대통령, 윌리엄 페리 전 미국 국방장관 등 9개국 350명 참석

평화와 번영을 위한 제주포럼

제주평화연구원 제주포럼기획단
제주특별자치도 서귀포시 중문관광로 227-24, 697-120
T. +82 (0)64 735 6531 | F. +82 (0)64 738 6539 | E-mail. jejuforum@jpi.or.kr
www.jejuforum.or.kr

제주특별자치도 서귀포시 중문관광로 227-24 (697-120)
전화: 064)735-6500 팩스: 064)738-6522
E-mail: policyforum@jpi.or.kr http://www.jpi.or.kr

『JPI 정책포럼』에 게재된 의견은 필자 개인의 의견으로,
제주평화연구원의 공식입장과는 무관함을 알려드립니다.

ISSN: 2005-9760