

발간등록번호
11-1290000-000272-09

ISSN 1739-9653
군비통제연구 52(2012. 12)

한반도 군비통제

특집 논문 - 제1회 서울안보대화(SDD)

동북아시아 내 WMD 확산 도전 : 북한에 대한 대응

사이버 위협의 실태와 대응 방안

일본의 사이버 보안과 정보활동 : 동아시아의 새로운 위협에 대한 대응

러시아 군의 현대화 : 21세기 전략을 찾아서

미국의 역내 존속과 유럽의 개입 도모 : 아태 지역의 전략적 영향력 행사를 위한 스마트 국방

대한민국 수호자 우리국군



한반도 군비통제



국 방 부

발간사

2012년의 국제정세는 우리나라를 비롯해 한반도 주변 4대 강국의 지도부가 모두 교체된 정치권력 변화의 해로 요약할 수 있겠습니다. 버락 오바마 미국 대통령은 재선에 성공했고 중국은 시진핑 총서기 시대를 열었습니다. 블라디미르 푸틴 러시아 대통령은 대통령, 총리에 이어 또다시 대통령에 당선되었고, 아베 신조 일본 자민당 총재는 2006년 이후 두 번째로 총리직을 맡았습니다. 우리나라도 지난 12월 19일 열린 제18대 대통령 선거에서 박근혜 후보가 당선됨으로써 헌정 사상 최초로 여성 대통령 시대를 열었습니다.

한편 김정은 집권 시대를 연 북한은 김정은 지배 체제의 안착을 위해 내부 결속을 강화하고 있습니다. 또한 북한은 유엔 안보리 결의를 무시하면서 지난 4월에 이어 12월 12일 다시 한 번 장거리 미사일 발사를 감행함으로써 한반도의 안보와 국제평화를 위협하고 있습니다.

이처럼 북한의 핵·미사일 개발 및 사이버 공격 등에서 보듯이 최근의 안보 위협은 그 외연이 포괄적으로 확장되고 있습니다. 따라서 한 나라가 단독으로 대응하기 어렵고 복잡해진 초국가적·비군사적 위협에 대처하기 위해서는 다자간 대화와 협력이 그 어느 때보다 더욱 중요해지고 있습니다.

이러한 상황에서 대한민국 국방부는 ‘아·태지역의 안보와 평화를 위한 협력’을 목표로 미·일·중·러를 비롯한 아·태지역 14개 국가들과 EU, NATO 등 국제기구의 차관급 국방관료와 민간 안보전문가가 함께 참여하는 다자안보대화체인 서울안보대화(SDD : Seoul Defense Dialogue)를 창설하여 금년 11월에 제1회 회의를 개최하였습니다.

「더욱 안전한 아·태지역을 위한 협력 : 과제와 해법」을 주제로 한 제1회 회의에서는 ‘공동안보 도전과 WMD 확산 대응’, ‘사이버 위협의 실태와 대응’, ‘국방운영 효율화’ 등 3개의 소주제로 나누어 심도 깊은 논의 및 토의를 진행하였으며, 이번 제52번째 「한반도 군비통제」에는 제1회 회의에서 역내 명망 있는 민간 안보전문가들이 발제한 5편의 논문을 수록하였습니다.

첫 번째 논문에서 미국 국방대 James Przystup 박사는 아·태지역 내 WMD 확산으로 인한 공동안보 위기와 관련하여 특히 북한 핵 문제에 대한 국제사회의 노력을 고찰하고 이에 대한 대응방안을 설명하였습니다. 고려대 정보보호대학원장 임종인 교수는 두 번째 논문에서 사이버 위협의 실태와 사이버전의 특징에 대해 고찰하면서 이에 대응하기 위한 국가적 노력 및 초국가적 협력 방안을 제시하였습니다. 이어서 일본 게이오대 Motohiro Tsuchiya 교수는 2009년 미국과 한국을 대상으로 벌어진 대규모 사이버 공격 과정에서 일본 정부의 대응을 분석하고 새로운 위협으로 등장한 사이버 공격의 심각성과 이에 대한 대비책을 면밀하게 분석하였습니다. 러시아의 카네기 모스크바 센터장 Dmitri Trenin 박사는 네 번째 논문에서 최근 러시아 군이 단행한 일련의 개혁조치에 대해 평가하고 새로운 안보환경 시대를 맞아 러시아 군이 나아가야 할 방향에 대해 역설하였고, 마지막으로 독일의 Sandfire AG 대표이사 Heiko Borchert 박사는 최근 전 세계적인 경기침체로 인해 재정적으로 어려움을 겪는 국가들이 늘어남에 따라 방위역량에 대한 국가 간의 통합과 공유, 즉 스마트 국방 도입의 필요성을 강조하면서 아·태지역 국가에 대한 스마트 국방의 적용 가능성을 연구 하였습니다.

이상과 같은 현상의 예리한 분석과 유용한 정책 방향을 제시한 이번 연구들이 아·태지역의 안보와 평화를 증진하고 역내 국가 간 신뢰와 협력을 강화하는 데 유용한 참고가 되기를 기대합니다.

끝으로, 서울안보대화가 아·태지역을 대표하는 권위 있는 다자안보대화체로 자리매김하여 한반도와 동북아시아의 긴장을 해소하고 항구적인 평화를 정착시켜 나가는 협력의 장이 되기를 기원합니다.

2012년 12월 31일



국방부 정책기획관 육군 소장 연 제 옥



아·태지역 다자안보의 중요한 근간이 될 서울안보대화(SDD)의 성과와 발전 방향

대한민국 국방부가 주관한 제1회 서울안보대화(SDD : Seoul Defense Dialogue)가 2012년 11월 14일부터 16일까지 서울 신라호텔에서 아·태지역 15개국과 EU, NATO 등 국제기구의 차관급 국방관료가 참가한 가운데 성공적으로 개최되었다.

최근의 국제 안보상황은 개별국가 차원에서 대응하기 어려운 포괄적, 비전통적 위협이 증대되고 있어 다자 간 협력이 활성화되는 추세이다. 더욱이 우리나라는 북한의 군사적 위협은 물론, 남북관계의 안정적 관리와 평화적 통일의 달성을 위해 국제사회의 이해와 협력이 필요한 상황이다.

이에 ‘안보와 평화를 위한 협력(Cooperation for Security & Peace)’을 슬로건으로 출범한 SDD는 한반도 평화와 아·태지역 안정에 기여하고 변화하는 국제 안보환경에 적극적으로 대응하기 위하여 추진되었다. 제1회 대화는 ‘더욱 안전한 아·태지역을 위한 협력 : 과제와 해법’을 주제로 ①아·태지역 공동안보 도전과 WMD 확산 : 대응과 협력방안, ②사이버 위협의 실태와 대응방안, ③국방운영의 효율화 : 성공사례 및 방안 등 3가지 의제로 진행되었다.

이러한 서울안보대화가 갖는 의미는 다음과 같이 정리할 수 있겠다.

첫째, 대한민국 국방부가 주관한 우리나라 최초의 고위급 다자안보대화체이다.

최근 아·태지역에서는 안보현안에 대한 다자주의적 접근 경향에 따라 ARF, TDF, 상그릴라 대화, JIDD 등 많은 다자안보대화체들이 창설, 운영되고 있으며, 이들 대화체에 우리나라도 적극적으로 참가하고 있다. 이번에 우리나라가 주관하는 다자안보대화체로서 SDD가 새롭게 출범한 것은 대한민국이 국제안보 이슈와 의제를 창출하고 안보와 평화를 증진하기 위한 대화·협력을 선도하는 역할과 위상을 갖게 됐다는 의미가 있다.

둘째, 민족의 분단과 군사적 대치 속에서 가장 첨예하게 안보가 위협받고 있는 한반도, 즉 대한민국에서 연례적으로 SDD가 개최된다는 것은 그 자체만으로도 한반도 평화와 안정에 기여할 것이다.

SDD는 역내 국가 간 대화와 신뢰구축을 통한 분쟁의 예방과 평화적 해결을 목적으로 역내·외 주요 국가 및 권위 있는 국제안보기구의 고위급 국방관료들이 머리를 맞대는 자리이다. 냉전의 고도로 남아있는 한반도에서 이러한 SDD가 개최됨으로써 자연스럽게 한반도의 안보 현실을 올바르게 인식하고 해결방안을 모색하는데 관심이 제고될 것이다. 북한도 SDD에 참여하여 국제사회의 책임 있는 일원으로서 역내·외 안보·평화를 위한 협력에 동참해 오길 기대한다.

셋째, 정무적 성격과 아울러 실무를 겸비하고 있는 각국의 차관급 국방관료들이 대표로 참여하는 SDD는 국제안보 이슈에 대한 논의와 함께 국방당국 간 교류협력을 증진시킬 수 있는 대화체이다.

즉, 차관급은 정무적 성격이 강한 장관급과 실무적 성격의 국장급을 이어주는 장점이 있다. 따라서 의제 선정에 있어서도 포괄적 안보현안과 아울러 구체적이고 실질적인 사안을 다룰 수 있는 융통성을

가지고 있다.

이번 제1회 서울안보대화는 다음과 같은 성과를 거둔 것으로 평가된다.

첫째, 아·태지역 내 의미 있는 고위급 다자안보대화체로 성공적으로 발족함으로써 한반도 안정과 역내 국가 간 군사적 신뢰구축을 도모할 수 있는 효과적인 대화의 장을 마련하고, 아울러 다자안보협력 분야에서 대한민국의 국제적 위상에 걸맞은 기여를 할 수 있는 기반을 마련하였다.

둘째, 제1차 회의임에도 불구하고 내실 있으면서도 품격 있는 행사로 진행되었다. 각국 대표의 50%가 차관보급 이상이었으며, 내빈의 대부분이 주한 외교관·무관, 전직 장·차관 및 안보문제전문가 등 안보관련 국내외 영향력 있는 인사가 참석하였다. 각국 대표와 참석자들은 토의 의제 등 행사 내용은 물론, 의전·경호 등에 대해 최고의 찬사와 함께 서울안보대화 창설에 대한 부러움과 기대를 표시하였다.

셋째, 각국이 공통적으로 관심을 갖고 있는 사항을 주제로 선정·토의함으로써 SDD의 실효성을 제고하였다. 세션 1에서는 북핵문제 해결을 위한 현실적 대안을 지속 논의할 수 있는 기반을 마련하였으며, 세션 2에서는 사이버 위협과 관련하여 국제공조를 위한 실무그룹 구성·운영 필요성에 공감하여 향후 이의 구체적 실행을 위한 계획을 수립해 나갈 예정이다. 세션 3에서는 차기 회의 시에도 각국의 성공사례를 공유할 수 있도록 지속적인 논의 필요성에 대한 공감대를 형성하였다.

이제 새롭게 아·태지역의 다자안보대화체로 발족한 SDD가 보다 권위 있는 다자안보대화체로 발전해 나가기 위해서는 많은 노력을 기울여야 한다.

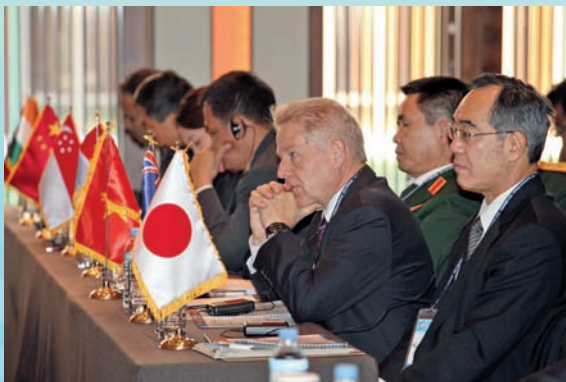
먼저 제1회 대화의 성공적인 개최를 계기로 모든 ASEAN 국가들뿐만 아니라 유럽의 주요 국가 등으로 참가국을 확대해 나갈 필요가 있다. 앞으로 한반도를 비롯한 아·태지역의 안전 보장과 새롭게 등장하고 있는 안보위협에 효과적인 대응을 위해 제1회 대화에는 참가하지 못한 브루나이, 캄보디아, 라오스, 미얀마를 비롯한 모든 ASEAN 국가는 물론, 영국, 프랑스 등 UN안보리 상임이사국, 독일과 몽골, 그리고 UN기구 대표를 초청할 계획이다.

둘째, 참가국 대표들 간에 심도 깊은 토의가 이루어지고, 이를 바탕으로 실효성 있는 협력 방안이 도출될 수 있도록 의제 선정이나 토의 방식 등의 세밀한 검토가 필요하다. 우선 의제는 ①아태지역 공동안보, ②사이버 위협, ③국방운영 세션별로 의미 있고 구체적인 토의가 가능한 의제를 선정하여 추진할 필요가 있다. 특히 지난 제1회 회의에서 사이버 위협 관련 실무그룹 구성 및 운영에 대해 다수가 공감대를 형성하였고 현재 이를 추진 중에 있다. 토의 방식에 있어서도 모든 참가자들이 주의를 집중하고 생산적인 토의가 이루어지도록 개선하고 국내외 저명인사를 사회자, 발제자, 토론자로 섭외하여 국제적인 행사에 걸맞도록 준비해야 할 것이다.

SDD는 가장 민감한 안보위협 지역인 한반도에서 역내·외 국가 및 국제 안보기구의 고위급 국방관료들이 국제 안보현안을 협의하고 상호 신뢰와 협력을 증진할 수 있는 대화의 장이다. 마침 2013년 새롭게 출범한 박근혜 정부는 '동아시아 평화와 유라시아 협력 추진'을 목표로 '동북아 평화·협력 구상'과 '서울 프로세스'를 추진한다는 외교정책 방향을 제시하고 있다. 이에 따라 SDD가 더욱 품격 있고 권위 있는 국제 다자안보대화체로 자리잡아 신정부의 외교 전략을 구현하는데 일익을 담당할 것으로 기대된다.

행사사진









Contents (2012. 12)

특집 : 제1회 서울안보대화(SDD)

- 1 동북아시아 내 WMD 확산 도전 : 북한에 대한 대응(한/영)
| James J. Przystup | 1
- 2 사이버 위협의 실태와 대응 방안 | 임종인 | 24
- 3 일본의 사이버 보안과 정보활동 : 동아시아의 새로운 위협에
대한 대응(한/영) | Motohiro Tsuchiya | 40
- 4 러시아 군의 현대화 : 21세기 전략을 찾아서(한/영)
| Dmitri Trenin | 101
- 5 미국의 역내 존속과 유럽의 개입 도모 : 아태 지역의 전략적
영향력 행사를 위한 스마트 국방(한/영) | Heiko Borchert | 123

이 책에 게재된 논문의 내용은 집필자의 개인적인 견해로서 국방부의 공식 입장이 아님을 알려드립니다.

동북아시아 내 WMD 확산 도전 : 북한에 대한 대응

James J. Przystup¹ || 美 국방대학교 국가전략연구소 선임연구원

목 차

- I. 서 론
- II. 제1부 : 도전의 정의
- III. 제2부 : 우발 사태

I 서 론

본 논문에서는 아시아·태평양 지역 내 대량살상무기(WMD)의 확산과 관련된 공동 안보 문제를 다루고자 한다. 이러한 동북아시아의 도전은 그 근원을 북한에 두고 있다.

본문에서는 우선 오늘날의 확산 문제를 점검한 후 단·중기적 미래 전망에 대해 살펴볼 것이다. 이는 김정은 정권을 다루는 문제를 포함한다. 제2부에서는 가능성이 낮지만 그럼에도 불구하고 여전히 발생할 가능성이 존재하는 북한에서의 정권 붕괴 사태가 야기할 수 있는 확산 문제에 중점을 둘 것이다.

1) 제임스 프리스텝(James J. Przystup) 박사는 현재 美 국방대학교 국가전략연구소 산하의 전략연구본부에서 선임연구원을 역임하고 있다. 본 논문의 내용은 저자 개인의 의견이며 美 국방대학교 또는 미국 정부의 정책을 반영하고 있지 않다.

II 제1부 : 도전의 정의

오늘날 북한은 확산과 관련하여 뚜렷하며 상호 연계된 두 가지의 도전을 지속적으로 제기하고 있다. 첫 번째는 외부적 도전으로서 북한 핵무기 프로그램과 이에 수반하는 한반도 내 WMD의 확산 위협으로부터 발생하는 문제이다. 동 위협은 핵 관련 기술 및 생·화학전 관련 이중용도 기술의 확산, 그리고 탄도미사일 및 관련 기술의 확산 문제를 포함한다. 북한의 핵 프로그램과 확산 관련 활동은 정권의 생존문제와 직결되어 있다. 핵 프로그램이 북한의 전략적 억제책으로서의 역할을 하는 반면, 확산 활동은 경화를 확보함으로써 지도부가 당 충성 세력들에게 사치품과 특전을 제공하고 결속을 도모하려는 목적이 있다.

두 번째는 전적으로 내부적인 도전은 아니나 현재 북한 내 진행 중인 권력 이양과 이에 수반하는 불안정성 문제, 그리고 지도부가 WMD 무기고에 대해 통제를 잃게 되는 가능성에 의해 제기되는 도전이다.

미국, 한국, 일본, 중국 및 러시아는 1990년대 초반부터 제네바 기본합의, 페리(Perry) 프로세스, 3자 회담, 그리고 지금은 중단된 6자 회담 등과 같은 다양한 외교 채널을 통하여 북한의 비핵화를 실현하고 WMD 관련 활동을 중단시키기 위해 노력해왔다. 도널드 럼스펠드 前 미국 국방부 장관은 북한의 WMD 확산 문제를 미국의 안보 이익에 반하는 북한의 가장 큰 위협으로 규정한 바 있다.

본질적으로, 위와 같은 외교적 노력의 초점은 북한으로 하여금 핵무기 프로그램을 포기하는 대가로 국교 정상화를 포함하여 개혁·개방이 가져오는 경제적 이익을 선택하게 하는 시도, 즉 북한에 근본적인 전략적 선택을 제시하는 시도였다고 할 수 있다. 그러나 북한은 수 차례에 걸쳐 이 같은 선택을 거부하였으며 주로 중국으로부터의 경제적 원조 및 지원에 의존하는 한편 핵무기 프로그램을 확충해왔다.

북한이 2006년과 2009년도 두 차례에 걸쳐 수행한 핵 실험은 이 같은 현실을 반증해주고 있다. 또한 위성 발사(미사일 실험)에 실패했던 지난 4월 13일, 북한은 자국의 헌법을 수정하여 “핵보유국”으로서의 지위를 수립하였다. 단기적으로 볼 때 앞으로 북

한의 WMD 프로그램을 종결시킬 가능성은 매우 희박할 것이라 사료된다.

한편, 북한의 새 지도부는 심각한 경제적 도전에 직면하고 있다. CIA 보고서에 따르면 2010년과 2011년의 북한 주민 1인당 GDP는 미화 1,800불로 추산되었다. 따라서 새 지도부는 어느 정도 경제 개혁의 필요성을 인식하고 있는 것으로 보인다. 김정은은 북한 주민들에게 앞으로 “허리띠를 졸라맬” 필요가 없을 것이라고 안심시켰다. 또한 6·28 조치를 통해 경제 개혁 실험의 신중한 시작을 암시하였다. 그러나 2012년 9월 열린 최고인민회의에서는 경제 개혁 문제를 다루지 않은 채 폐회하였다. 지난 2002년과 2009년에도 이와 유사한 경제 개혁을 위한 초기 작업에 착수한 바 있으나 철회 또는 중단하였다.

새 지도부는 앞으로 다음 두 가지의 주요 문제를 다루어야 할 것이다: 북한이 경제 개혁 없이 강성대국의 목표를 달성할 수 있을 것인가? 그리고 정권을 유지함과 동시에 경제 개혁을 달성할 수 있을 것인가?

만약 북한의 새 지도부가 실제로 경제 개혁·개방에 대해 진정성을 보이고 있다고 한다면, 이는 중·장기적으로 국제 안정과 안보를 위협하는 확산 문제를 종결할 수 있는 열쇠를 쥐고 있는 것과 마찬가지로일 수도 있다. 중국과 베트남의 경우 오랫동안 지속되었던 미국과의 문제를 해결함으로써 경제 개혁과 성장에 박차를 가할 수 있었다. 현재 미-북 관계는 여전히 미해결 과제로 남아 있으며 그 사이에 우리는 지속적으로 북한의 확산 도전과 마주할 것이다.

핵 문제 : 대안

핵 및 WMD의 확산 위험을 다루기 위한 대안은 탐구 목적을 위해 크게 세 가지로 고려해 볼 수 있다.

첫 번째는 북한 핵 프로그램을 종결시키는 목적의 군사 전략이다. 이는 거의 완벽한 정보수집이 요구되나 현재 북한 전반에 대한 정보는 극히 제한적이다. 북한 핵 프로그램, 특히 고농축우라늄(HEU) 프로그램에 대한 정보는 더욱 제한적일 것이다. 더불어 관련 정보수집 작전을 수행하는 것은 대한민국, 일본뿐만 아니라 잠재적으로 미국, 괌, 알래스카에까지도 심대한 보복 위험을 초래할 수 있다. 미국이 북한의 보복을 막지 못한다면 이는 동북아시아 동맹 구조를 긴장시키거나 파열시킬 수도 있다.

두 번째로는 비핵화라는 정책적 목표가 현재 북한의 새 지도부 통치 하에서는 달성이 불가능하며 비핵화를 실현하고 확산 위험을 제거하기 위해서는 정책의 초점이 정권 교체에 있어야 한다는 전제에 기반을 둔 전략을 생각해 볼 수 있겠다. 이는 정책적으로 북한 정권 교체 또는 붕괴에 초점을 두고 유엔 안보리 결의안 1718호 및 1874호를 넘어서는 경제적·재정적 압력을 북한 당국에 가중시키는 것이다.

그러나 이를 성공하기 위해서는 중국의 전폭적인 협력, 즉 제재 조치를 고수하고 이를 강력히 시행하고자 하는 중국의 의지가 요구된다. 하지만 중국은 한반도의 안정이 자국의 주요 전략 이익이라는 것을 수 차례에 걸쳐 명확히 한 바 있다. 두 차례의 핵 실험, 미사일 실험, 천안함 폭침 및 연평도 포격도발 이후 북한이 실로 엄청난 행동을 자행하지 않는다면, 물론 중국 측의 판단이 어떨지는 알 수 없겠지만, 현재로서는 중국이 북한으로부터 이득을 취하며 보유하고 있는 경제적 수단을 전향하여 북한 당국을 압박하기 위해 이를 활용할 가능성은 낮다. 최근 왕자루이의 방북과 장성택의 방중은 중국이 북한의 새 지도부에 대해 정치적·경제적 지원을 보장하고 북한 내 안정을 위해 노력하고 있다는 사실을 반증하고 있다.

또한, 북한 정권을 교체하기 위해 정책적 노력을 집중하는 일은 한국의 대북정책과 관련하여 뿌리 깊게 지속되었던 국론 분열을 더욱 심화시킬 것이다. 그렇기에 전폭적인 지지를 얻기는 어려울 것이다. 그리고 만약 정권 교체 정책이 실제로 성공할 경우 미국은 한반도 및 동북아시아 내 문제들을 정리하는 데 있어 관여할 수밖에 없을 것이다.

세 번째 전략은 외교책으로의 회귀, 즉 어떻게 북한 당국과 대화하여 북한의 핵 및 WMD 프로그램을 종결하고 확산 위험을 제거하기 위한 조건을 협상하느냐이다. 이 과정에서는 6자 회담 등 외교적 오점을 남긴 지속되는 구조적 문제들을 검토하는 것이 중요하며 그리고 그 과정에서 향후 발전방향 또한 식별할 수 있을 것이다.

구조적 문제와 관련하여 첫 번째 문제는 공동 이익을 공유하지만 국가적 우선순위는 다르다는 현실을 들 수 있다. 미국과 현 한국 정부는 양국의 외교 우선순위를 비핵화로 두었다. 지난 4년 동안의 한-미 정책이 강력히 일치해왔던 것은 향후 양국 대신의 결과와 새 행정부 출범에 의해 영향을 받을 수 있다.

두 번째 구조적 문제는 중국이 무엇보다도 북한의 안정 및 국가유지를 중요하게 생각하며 그 다음으로 비핵화에 중점을 두고 있다는 점이다. 북한 내 잠재적 불안 또는 불안정에 대해 우려하고 있는 중국은 확산 관련 문제에 있어 북한 당국을 설득하려고

시도는 할 것이나 강압하지는 않을 것이다. 중국이 북한의 안정에 중점을 두고 있다는 사실을 강조하자면, 유엔 안보리 결의안 1718호의 서명 이후 중국의 대북 교역량은 2008년 사이 41% 증가하였으며 2009년 잠시 하락한 이후 지금까지 상승곡선을 그려왔다. 또한 중국은 북한-이란 간의 항공로 환승기점이기도 하다.

오랜 시간 동안 많은 중국 관료들과 분석가들은 북한을 미국과 동맹국인 통일·민주국가 한국이라는 세력에 대항하기 위한 “완충국”으로 간주해왔다. 또한 오바마 행정부가 아시아·태평양 지역에 대한 재조정 정책을 발표한 이후, 일부 중국 분석가들은 북한이 완충국의 역할을 할 뿐만 아니라 소위 말하는 미국의 중국 봉쇄 노력을 피하기 위한 “전략적 자산”이라는 의견을 내놓기도 하였다.

세 번째 구조적 문제는 핵 외교 관련 당사국들 간, 특히 미국과 북한 간에 신뢰가 거의 전무하다는 것이다. 이 같은 간극을 메우는 일은 핵 관련 현안들을 다룸에 있어 아마도 가장 힘겨운 도전일 것이다.

네 번째 구조적 문제는 핵보유국 지위에 대한 북한의 단호한 입장이다. 북한이 지속적으로 핵보유국 지위를 주장한다면 비핵화를 완전히 실현하기는 더욱 어려워진다. 또한 북한이 핵보유국으로서의 지위를 유지하는 한 확산의 위험은 계속될 수밖에 없다. 북한이 시리아와 핵 관련 협력을 진행하는 것을 단지 하나의 사례로만 보아서는 안 된다. 그리고 앞서 언급했듯이, 북한은 여전히 탄도미사일 및 이중용도, WMD 관련 기술 등을 수출하는 주요 수출 국가이다.

요약해 보면, 앞서 설명한 구조적 장애들은 북한 비핵화의 실현이 어느 정도 어려울 것이라는 점을 시사하고 있다. 비핵화의 과정은 지연될 것이며, 그동안 국제 사회는 북한으로부터의 지속적인 WMD 확산 위협에 직면할 것이다.

확산 위험에 대한 대응

그럼에도 불구하고 확산 위험에 대응하여 활용할 수 있는 조치들이 다음과 같이 존재하는데 대량살상무기 확산방지 구상(PSI) 강화를 통한 국제 협력 증진, 유엔 안보리 결의안 1718호 및 1874호에 의거 부과된 대북 제재 강화 시행을 위한 국제적 노력 지속, 그리고 북한 당국에 대한 외교 채널 개방 지속 등이 바로 그것이다.

압박과 회유는 성공적인 외교와 불가분한 것이다. 2003년에 출범한 대량살상무기 확산방지 구상(PSI)은 대량살상무기와 이중용도 기술의 운송을 차단하는 것에 목적을 두고 있다. PSI는 오늘날 100여 개국이 참여하고 있으며 “확산이 염려되는 운송을 차단하고, 정보 교환 촉진을 위한 절차를 발전하며, 차단을 돕기 위해 국가의 법적 권한을 강화하며, 차단 노력을 지원하여 특정 조치를 취하는²⁾” 노력을 한다.

2006년에 채택된 유엔 안보리 결의안 1718호와 2009년에 채택된 1874호는 북한의 확산 활동을 제재하는 것에 중점을 두고 있다. 동 결의안은 회원국들이 각국의 법과 사법 체계를 강화하여 확산 관련 활동을 억제하도록 촉구하고 있다. 이는 회원국들이 각국의 항만에서 북한 선박에 대한 수색작업을 수행하고 식량 및 연료 공급을 차단하도록 하는 조치를 포함한다. 동 결의안에 의거하여 많은 국가들이 북한 선박을 차단하고 적재되어 있는 금지된 화물을 압류한 바 있다. 2009년 태국 돈므앙공항에서 무기를 압류한 사건이 오늘날까지 항공화물 차단에 성공했던 유일한 사례로 기록되고 있으며, 북한이 고가치 확산 활동을 수행하고 제재를 피하기 위해 항공화물 수단을 활용하고 있다는 사실에 대해 우려의 목소리가 커지고 있는 실정이다.

유엔 제재위원회 전문가 패널은 일련의 보고서를 통해 북한이 화물 분류표 위조, 동아시아 내 환적 기점을 통한 문서 세탁, 해외기업 및 위장기업을 활용한 비공식 자금이체, 현금 밀수 및 바터 무역 등을 활용하여 제재를 교묘히 피하고 있는 사실을 지적하며 평양 당국의 불법 활동에 대응하기 위해서는 국제 협력을 강화해야 한다고 강조하였다.

전문가 패널은 유엔 안보리 결의안 1718호 및 1874호의 집행 강화를 위해 다음 조치들을 취할 것을 권고하였다 : 회원국들 간의 정보공유 증대, 회원국들에게 화물 표준 문서 및 해운·항공 화물에 대한 문서통제 지침 제공, 환적 기점에서의 경계 강화, 공항에서의 세관 경계 강화, 소화기 및 경화기의 정의, 유엔 안보리 결의안 1718호에 의거 금지된 사치품의 정의, 결의안 시행 조치와 관련하여 더욱 세부적인 보고서를 제공하도록 회원국들을 장려하는 것 등이다.

또한 전문가 패널은 연구 결과, 제재 조치에 대해 다음과 같은 평가를 내렸다.

- 과거 북한의 외화벌이 주 수입원이었던 무기 거래 및 수출 능력을 현저히 제한시켰다.

2) 美 국무부 웹사이트 참조. <http://www.state.gov/t/isn/c/10390.htm>

- 불법 이체의 비용을 가중시키는 동시에 이익을 줄임으로써 경제적 측면에서 성공을 거두었다.
- 북한 지도부에 “상당한 영향”을 끼쳤다. 즉 북한 일반 주민들이 겪고 있는 극심한 경제 사정이 북한 자체 경제정책의 결과로 발생한 것이라는 인식을 주었다.

전문가 패널은 유엔 안보리 결의안에 순응하지 않고서는 북한이 경제적 목표를 달성하기 어려울 것이라고 평가했으며 동시에 북한이 아직 비핵화를 실현하고 기존 WMD 및 탄도미사일 개발 프로그램을 중단할 조짐이 없는 것으로 보아 앞으로 북한이 유엔 안보리 결의안에 정면으로 대항하는 노력을 지속할 것으로 내다보았다.

과거 상황이 전초전 양상을 띠고 있었다면, 앞으로 북한이 제기하는 WMD 도전에 대응하는 일은 더욱 어려울 것으로 예상되며 문제의 근원인 북한의 핵 및 WMD 프로그램을 제거하는 우리의 목표에 미달할 가능성이 높다. 결국 북한에서 내부적 변혁이 일어나지 않는 한 도전은 지속될 것이다. 문제는 과연 우리가 성공적인 상황 관리를 위하여 협력해 나갈 수 있을지 여부이다.

더 나은 미래?

2012년 8월 31일, 북한 외무성은 성명을 발표하여 핵 능력을 유지하겠다는 의지를 천명하였다. 또한 8월 31일 성명을 통해 미국의 “적대적 정책”이 “핵 문제 해결에 있어 주요 장애물이다.”라고 언급하며 오랫동안 고수했던 정책적 입장을 반복하였고, 1954년 체결된 정전협정을 대체하여 “항구적 평화체제”를 수립할 것을 주장하며 북한은 “이미 완전한 핵보유국으로 부상”하였고 “북한의 강경 입장을 특정 전술로 보는 것은 오산”이라고 밝혔다.

북한의 8월 31일 성명과 지난 4년 동안의 사건에도 불구하고 외교의 문은 여전히 열려 있다. 이에 적용되는 적절한 사례로는 2012년 2월 29일에 발표된 미-북 합의를 들 수 있다. 2·29 합의를 통해 북한은 장거리 미사일 발사, 핵 실험 및 우라늄 농축 활동을 포함한 영변 핵 활동의 중단, 국제원자력기구(IAEA) 사찰단 복귀 및 영변 우라늄 농축 활동의 검증 및 감시 수용, 5-MW 원자로와 주변 시설의 불능화 등에 합의

하였다. 이에 대한 대가로 미국은 240,000톤의 인도주의적 식량 지원을 약속하였다.

그러나 본 합의는 북한이 지난 4월 13일 위성·미사일 발사를 감행함에 따라 무산되었다. 동 미사일 발사는 그동안 북한과의 대화를 주장해왔던 미국인들에게 신뢰를 무너뜨리는 조치였으며 미국 내 얼마 안 되는 북한 대화 세력들의 뒤통수를 치고 이들을 크게 망신주었던 행위였다.

2·29 합의가 무산된 이후 북한과 국제 사회 간의 불신의 골은 더욱 깊어져만 갔다. 그러나 국제사회는 다시 비핵화라는 최종상태를 위해 북한을 대화로 이끌어 내려는 시도를 하고 있다. 현재 북한과 아시아·태평양 지역 내 주변국들과의 안보 현안들을 고려해 볼 때 먼저 우리를 분열시키고 있는 각자의 문제를 해결하지 않고서는 이러한 불신의 골을 단번에 메울 수는 없을 것이다. 오늘 당장 평화협정을 체결한다고 해도 이는 단지 무의미한 종잇조각일 뿐이며, 한반도 평화 체제 수립이라는 궁극적인 목표를 달성할 수는 없을 것이다.

향구적인 평화를 가져올 평화협정을 체결하는 방법으로는 현재 불화의 근원이 되는 안보 및 외교 등의 어려운 현안들을 먼저 해결하는 것이다. 이 과정은 북한의 비핵화로부터 시작하며 이를 달성함으로써 끝내야 한다. 비핵화 없이는 한반도에 향구적인 평화를 정착시킬 수 없다. 동시에, 역사적인 1991년 남-북 기본합의서의 이행에 착수함으로써 남북 간 신뢰를 구축할 수 있는 조치를 취해야 한다. 이는 외교적으로 서로를 인정하는 것을 포함한다. 과거 북한이 오랫동안 한국 정부의 정당성을 인정하지 않는 노력을 해왔음에도 불구하고, 진정한 남북의 화해는 한반도에 평화 체제를 수립하는데 있어 주요 요소가 될 것이다. 마지막으로 정전협정을 정치적 합의서 또는 미국, 중국, 북한 및 한국이 서명하는 평화 조약으로 대체해야 할 것이다. 그때까지 북한은 비핵화를 실현함으로써 미국과의 국교 정상화 문을 열 수 있을 것이다.

종합하자면, 이 모든 과정들은 실질적 위협 감소에 초점을 두는 것이며 이들이 합쳐져야 평화 정착과 평화 체제 수립을 지원하게 되는 것이다. 덩 샤오핑은 돌을 두드려가며 강을 건너야 한다고 말했다. 물론 이러한 과정은 긴 과정이 될 것이며 그동안 지역 내 국가들은 협력해서 북한의 확산 위협에 대응함과 동시에 자체적으로 적절한 외교책을 강구하여야 한다. 또한 스포츠, 문화, 교육 분야에서의 교류를 발전시킴으로써 우리는 북한 주민들에 대한 악감정은 없으며 단지 북한 정권의 관행에 대해서만 깊은 우려를 갖고 있다는 인식을 심어주어야 한다.

Ⅲ 제2부 : 우발 사태

먼저 이 문제를 다루기 전에 본 논문은 미국의 국가 안보 이익이 북한의 안정에 있다는 것을 확실히 하는 바이다. 본 논문의 내용이 북한 정권을 지지하고 있다고 오해하여서는 안 되며 단지 불안정 사태로 인해 핵무기 및 물질에 대한 통제력이 상실되고 확산의 위험이 커질 수 있다는 점에 주목하고 있다.

그러나 북한의 경우, 경제 개혁은 새 지도부에게 힘겨운 정치적 도전을 제시한다. 안드레이 란코프 국민대학교 교수의 말처럼 개혁하는 북한은 매우 불안정하며 붕괴할 수도 있다. 또한 만약 장성택이 사망하거나 권력에서 물러나게 되면 어떻게 될 것인가?

필자는 美 국가전략연구소에서 18개월 동안 동료 연구원인 Ferial A. Saeed와 함께 북한 불안정 또는 정권 붕괴 사태에서의 안보 및 외교 도전에 대해서 연구를 수행한 바 있다. 동 연구의 중점은 북한 정권이 핵 무기고에 대해 통제를 잃는 상황과 이에 수반하는 확산 위험에 관한 것이었다. 그리고 2011년 9월, 美 국방대학교에서는 우리의 연구 결과를 “한국의 미래: 미국 외교에 대해 북한 정권 붕괴가 주는 도전”이라는 논문으로 발간하였다.

다음은 해당 논문의 일부 내용이다:

- 북한 정권이 급작스럽게 붕괴한다고 해도 적어도 단기적으로는 국가 붕괴로 이어지지는 않을 것이다. 중국은 미국과 동맹인 민주 자본주의 국가, 한국에 대항하기 위해 북한을 완충국으로 영속시키려 할 것이다.
- 중국은 북한 지도부 위기사태를 가장 먼저 감지할 것이며 후계 정권을 구성하기 위해 외교적으로 개입할 것이다.
- 국제 사회는 북한 주민 대다수가 지지하지 않는 한 북한이라는 국가를 종식시키는 것에 찬성하지 않을 것이다.
- 불안정 사태 발생 시 주요 정치적 결심은 다음과 같을 것이다: 개입을 할 것인지 여부, 누가 개입할 것인지, 인도주의적 지원, WMD 제거, 안정화 또는 통일 등

어떠한 명분하에 또는 어떠한 최종상태를 위해 개입할 것인지 등. 따라서 개입 및 최종상태를 결정하는 것이 중요하다.

- 미국의 국가 안보이익은 WMD 제거에 있으나 개입 문제는 동맹국들과 마찬가지로 현실적으로 어려울 것이며 정치적 문제의 소지가 있다. 인도주의적 지원, 안정화 또는 WMD 제거와 같은 목표를 달성하기 위해서는 개입에 있어서 북한 주민들의 협조가 요구될 것이다. 그러나 그들의 협조가 있을 것이라고 가정해서는 안 되며 개입 초기에는 협조가 제한될 가능성이 높다.
- 중국 또는 한-미가 선제적으로 개입할 가능성이 존재한다. 현재 안보 이익 및 국가 목표와 관련하여 소통이 부족한 점을 고려하면 북한 붕괴 시 계산 착오 위험성은 높을 것이다.
- 중국과 러시아는 WMD 제거보다 미국의 독자적 개입 문제에 더 큰 우려를 갖고 있으며 평화적인 비핵화 요구를 위해 2005년 공동 성명을 들며 비핵화 과정에 대해 국제적으로 감시하도록 압박할 것이다.
- 중국 또는 미국은 문제를 유엔 안보리에 제기하여 기타 국가의 행위를 제한하고 개입에 대한 정당성을 확보하려 할 것이다.

확산 위험과 국익 문제가 달려있는 점을 고려할 때 오늘날 미국, 한국, 중국, 일본 및 러시아는 북한 우발사태 발생 시에 야기되는 안보 및 정치 문제를 다루기 위한 준비가 극심하게 부족한 실정이다. 바로 지금이 조용하지만 적극적인 외교가 요구되는 시점이다.

Common Security The Proliferation Challenge in Northeast Asia; Dealing with North Korea

James J. Przystup¹ ||
Senior Fellow Institute for National Strategic Studies National Defense
University Washington DC

CONTENTS

- I . Preface
- II . Defining the Challenge
- III . Contingencies

I Preface

This paper seeks to address the common security challenge of WMD proliferation in the Asia–Pacific region. The critical source of that challenge

1) Dr. James J. Przystup is a Senior Fellow at the Center for Strategic Research, part of the Institute for national Strategic Studies at the National Defense University. Views expressed in this paper are those of the author alone and do not necessarily reflect the policies of the National Defense University, the Department of Defense or the United States Government.

in Northeast Asia rests in the Democratic People's Republic of Korea.

The paper will first take up the proliferation challenge as it exists today and, as it will likely exist in the near to mid-term future. That involves dealing with the Kim Jong Un regime. A second part will focus on the proliferation challenges posed in the event of an unlikely, but nevertheless possible, collapse of the regime in Pyongyang.

II Defining the Challenge

Today, North Korea continues to pose two distinct but interrelated proliferation challenges. The first is external; the challenge posed by its nuclear weapons program and the attendant risks of WMD proliferation from the Peninsula. This risk involves the proliferation of nuclear-related technologies, dual-use technologies related to chemical and biological warfare as well as the proliferation of ballistic missiles and ballistic missile-related technologies. North Korea's nuclear program and proliferation-related activities are directly related to regime survival. The nuclear program stands as a strategic deterrent, while the proliferation agenda is aimed at securing the hard currency that allows the leadership to incentivize party faithful to remain faithful with rewards of luxury goods and perks.

The second challenge is essentially, but not wholly internal the challenge posed by the on-going transfer of power in Pyongyang and the attendant risk of instability and potential loss of Pyongyang's control over North Korea's WMD arsenal.

Since the early 1990s, the United States, the Republic of Korea, Japan,

China and Russia, in various diplomatic constructs -- the Agreed Framework, the Perry Process, the Three Party Talks and the now suspended Six Party Talks -- have endeavored to effect the denuclearization of North Korea and a termination of WMD-related activities. Former U.S. Secretary of Defense Donald Rumsfeld defined North Korea's proliferation of WMD as the greatest threat posed by Pyongyang to U.S. security interests.

In essence, these diplomatic efforts have attempted to put before Pyongyang a fundamental strategic choice: the economic benefits of opening and reform, including normalization of relations in return for the abandonment of its nuclear weapons program. And repeatedly Pyongyang has refused to make a choice, relying on economic aid and assistance, mainly from China, while expanding its nuclear weapons program.

North Korea's nuclear tests of 2006 and 2009 serve to underscore this reality. And, on April 13, the day of the failed satellite launch/missile test, the DPRK's constitution was amended to establish North Korea as a "nuclear-armed nation." In the near-term, the prospect of ending North Korea's WMD program should be considered exceedingly remote.

Meanwhile, the new leadership in Pyongyang is faced with daunting economic challenges. The CIA Fact Book estimates per capita North Korea's GDP in 2010 and 2011 as \$1,800 USD. The new leadership appears to recognize the need for some form of economic reform. Kim Jong Un has assured North Korea's citizens that there should be no future need of "belt-tightening." The June 28 measures suggested the cautious beginnings of an experiment in economic reform. But the Supreme People's Assembly adjourned its September meeting without taking up issues related to economic reform. In 2002 and 2009, similar incipient steps were taken in the direction of economic reform only to be pulled back and suspended.

Looking ahead, the new leadership will have to address two key questions: can it attain the goal of becoming a Strong and Prosperous Nations absent

economic reform and can economic reform be pulled off without pulling down the regime?

If, in fact real, the commitment of the new leadership to economic reform and opening may, over the mid-to-long term, hold the key to ending the threat of proliferation posed by North Korea to international stability and security. For China and Vietnam, it was the resolution of long-standing issues with the United States that spurred economic reform and growth. For the DPRK and the United States that remains a proposition to be tested. In the meantime we will continue to be faced by the proliferation challenge posed by North Korea.

The Nuclear Challenge: Alternate Strategies

For heuristic purposes, three broad alternative strategies to address the dangers of nuclear and WMD proliferation can be considered.

The first is a military strategy that would aim to terminate North Korea's nuclear program. This would require near perfect intelligence, and intelligence on North Korean general is exceedingly limited. Intelligence on its nuclear program, in particular, the HEU program is likely even more so. Moreover, such an operation would pose significant risks of retaliation – to the Republic of Korea, to Japan and potentially to the United States, to Guam and even Alaska. Failure by the United States to prevent retaliation by the DPRK would strain, if not rupture, the alliance structure in Northeast Asia.

A second strategy would be based on the assumption that the policy goal of denuclearization is not be achievable even under North Korea's new leadership and that policy should be aimed at regime change in order to effect denuclearization and end the risks of proliferation. Policy would be

aimed at intensifying economic and financial pressure on Pyongyang beyond United Nations Security Council Resolutions 1718 and 1874, with the objective of forcing regime change or collapse.

Success, however, would require the complete cooperation of China – its willingness to adhere to and strictly enforce sanctions measures. Yet, Beijing has repeatedly made clear that stability on the Korea Peninsula is its core strategic interest. In the absence of truly egregious behavior on the part of North Korea -- and after two nuclear tests, several missile tests, the sinking of the Cheonan and the shelling of Yeongpyeong island -- it is difficult to imagine what Beijing's definition of egregious might be – it is unlikely that China will fully utilize the economic leverage it enjoys to pressure Pyongyang. The recent exchange of visits by Wang Jiarui to Pyongyang and Jong Song Taek to Beijing only serve to underscore China's commitment to the political and economic support of North Korea's new leadership and to stability in the North Korea.

Policy efforts directed at regime change in Pyongyang would also likely exacerbate the deep and longstanding divide in the Republic of Korea over policy to the North. Wholehearted support cannot be expected. And should a policy of regime change actually succeed, the United States would not be able to disentangle itself from sorting things out on the Peninsula and Northeast Asia.

A third strategy is a return to diplomacy -- how to engage Pyongyang and the terms and conditions for engagement toward ending its nuclear and WMD programs and removing the threat of proliferation. In the process, it is important to consider the enduring structural problems that have marked diplomacy, including the Six Party talks to date. In doing so, it is perhaps possible to discern a way ahead.

As for the structural problems, the first is the reality of shared common interests but different national priorities. The United States and the present

ROK government have made denuclearization the primary focus of their diplomacy. The strong concurrence of U.S. and ROK policy over the past four years may be affected by the results of presidential elections and new administrations in both countries.

A second structural problem is that China is concerned first and foremost, with stability in North Korea, the continuation of the North Korean state, and then with denuclearization. Concerned with the potential for unrest or instability, China will attempt to persuade Pyongyang on proliferation-related issues but it will avoid strong-arming it. Underscoring Beijing's focus on stability, after signing on to UNSC 1718, China's trade with North Korea increased at a rate of 41percent through 2008, and after a brief fall off in 2009, has since been on the rise. China also serves as an air-transit point for North Korean air traffic to and from Iran.

Many Chinese officials and analysts have long considered the DPRK to be a "buffer" at against the influence of a unified, democratic Korea allied to the United States. And, since the Obama administration announced its policy of rebalancing toward the Asia-Pacific region, some Chinese analysts have come to view North Korea not only as a buffer but also as a "strategic asset" in parrying, what they consider to be, U.S. efforts to contain China.

A third structural issue is the almost complete lack of trust among the parties involved in nuclear diplomacy, in particular between the United States and North Korea. Bridging this chasm is perhaps the most daunting challenge in addressing the outstanding nuclear-related issues.

A fourth structural issue is North Korea's resolute commitment to its nuclear status. The longer North Korea continues to assert its nuclear status as a nuclear-armed state, the more difficult it will be to realize complete denuclearization. And as long as North Korea maintains its status as a nuclear-armed state, the risks of proliferation will continue. North Korea's nuclear cooperation with Syria should not be considered a

singular case. And as noted above, North Korea continues to be a major exporter of ballistic missiles and dual-use, WMD-related technologies.

In sum, the above structural impediments speak to the degree of difficulty in realizing the denuclearization of North Korea. The process of denuclearization will be protracted. In the meantime, the international community will be faced with a continuing threat of WMD proliferation from North Korea.

Addressing Proliferation Risks

Nevertheless, there are steps that can be used to address the proliferation risks. These include; enhancing international cooperation in strengthening the Proliferation Security Initiative (PSI); sustained international efforts to enforce more strictly the sanctions imposed on North Korea under UNSCR 1718 and 1874; and keeping open the diplomatic track to Pyongyang.

Pressure and persuasion are intrinsic to successful diplomacy.

The Proliferation Security Initiative, launched in 2003 is aimed at interdicting shipments of weapons of mass destruction and dual-use technologies. Today, 100 countries have endorsed the initiative. In doing so, they commit to “interdict transfers... of proliferation concern...develop procedures to facilitate exchange information...strengthen national legal authorities to facilitate interdiction... and take specific actions in support of interdiction efforts.” U.S. Department of State. <http://www.state.gov/t/isn/c/10390.htm>

UNSCR 1718, adopted in 2006, and 1874, adopted in 2009, are aimed at constraining North Korea’s proliferation activities. The resolutions call on member states to strengthen their national laws and enforcement mechanisms to inhibit proliferation-related activities. This includes searching North Korea ships in their ports and denying provisioning and

fuel to North Korea ships calling at their ports. Acting under the resolutions, various states have interdicted and seized prohibited cargo on North Korea ships. To date, only the seizure of weapons at the Don Mung airport in Thailand in 2009 stands as a success in terms of air-cargo interdiction, and there are increasing concerns that North Korea has adopted air-cargo as the preferred means to engage in high-value proliferation activities and evade sanctions.

The United Nations Sanctions Committee Panel of Experts, in a series of reports, has called attention to North Korea's continuing efforts to circumvent sanctions -- the use of false labels; laundering documentation through trans-shipment points in East Asia; use of overseas entities and shell companies informal transfer mechanisms, cash couriers and barter arrangements -- and the need for enhanced international cooperation to deal with Pyongyang's illegal activities.

The Panel of Experts has recommended a number of steps to strengthen enforcement of UNSCR 1718 and 1874. These include: greater information sharing among member states; providing member states with guidelines on uniform documentation of cargo and documentation controls for both sea-borne and air cargo; greater vigilance at transshipment points; enhanced customs vigilance at airports; definition of small arms and light weapons; definition of luxury items banned under UNSC 1718, and encouraging member states to provide more detailed reports with regard to steps taken to implement the resolution.

Among its findings, the Panel has determined that sanctions:

“significantly constrained the DPRK's ability to market and export arms which had previously provided a significant source of the DPRK's foreign exchange...

succeeded in economic terms by raising the costs of illicit transfers while simultaneously lowering the returns...

had a “substantial impact” on North Korea’s leadership ... severe economic circumstances impacting the DPRK’s general population... are the result of the DPRK’s own economic policies...”

The Panel considered it “unlikely” that North Korean will attain its economic objectives “without complying with Security Council resolutions...” At the same time, the Panel found that Pyongyang continues “actively to defy” Security Council Resolutions and that “there are no indications, as yet that the DPRK is ready to move forward on denuclearization and its other existing WMD and ballistic missile development programs.”

If the past is, in any way prologue, the way ahead in dealing with the WMD challenge posed by North Korea, will be difficult and, in all likelihood, yield less than what we should aim to achieve – the elimination of the central source of that challenge, North Korea’s nuclear and WMD programs. In short, barring an internal transformation of the regime in Pyongyang, the challenge will continue. The issue is whether we can cooperate to manage it successfully.

A Better Future?

That depends...

On August 31, the North Korean Foreign Ministry issued a statement that makes clear North Korea’s intent to maintain its nuclear capabilities. The August 31 statement also reprises long-held policy positions: citing U.S. “hostile policy” as the “main obstacle to resolving the nuclear issues;” calling for a “lasting peace regime” to replace the 1954 Armistice and making clear that the DPRK has “already emerged as a full-fledged nuclear

weapons state” and that it “would be great mistake to regard our strong position as a kind of tactics.”

Notwithstanding the August 31 statement and the events of the past four years, the door to diplomacy has remained open. A case in point is the agreement reached between the United States and North Korea announced on February 29 of this year. In the agreement, North Korea agreed to implement a moratorium on long-range missile launches, nuclear tests and nuclear activities at Yong by on including uranium enrichment activities, to accept the return of IAEA inspectors to verify and monitor uranium enrichment activities at Yong by on, and to confirm the disablement of the 5-MW reactor and associated facilities. For its part, the United States agreed to provide 240,000 tons of humanitarian food aid.

Unfortunately, the agreement collapsed in the wake of North Korea’s April 12 satellite/missile launch. For an American colleague, who has long been engaged in efforts to engage North Korea, the missile launch after the 2/29 agreement, was a “confidence destroying measure,” one in which North Korea had blindsided/cut-off at the knees, the very few American supporters of engagement that it has.

In the aftermath of the collapse of the 2/29 agreement, the chasm of mistrust between North Korea and the international community has only widened. And, we find ourselves again looking for traction in efforts to engage North Korea toward the end state of denuclearization. Given the outstanding security issues that exist between North Korea and its neighbors in the Asia-Pacific region, it should not be expected that the chasm of mistrust can be crossed in a single leap without first resolving the individual issues that divide us. Signed today, a peace treaty would be a meaningless piece of paper and would not achieve the goal of establishing a peace regime on the Peninsula.

The way to conclude a peace treaty that will sustain peace is first to

resolve the difficult security and diplomatic issues that are the source of the present discord. This begins with, and should end in, the denuclearization of North Korea, without which lasting peace on the Peninsula is unattainable. At the same time, other steps need to be taken to build confidence between Seoul and Pyongyang, beginning with initiatives to implement the historic 1991 Basic Agreement. At the diplomatic level, this would be accompanied by cross-recognition -- despite North Korea's long efforts to de-legitimize the ROK, true South-North reconciliation is a key element in building a peace regime on the Peninsula. Finally, the Armistice would be replaced by political agreement or a peace treaty, to which the United States, China, North Korea -- and South Korea are signatories. Meanwhile North Korea's denuclearization would open the door to normalization of relations with the United States.

In sum, all steps are aimed at actual threat reduction; collectively, they realize a state of peace and support a peace regime. In the words of Deng Xiaoping, we should cross the river by feeling for stones. This process, of course, will be a protracted one, during which the region must cooperate in addressing the proliferation threat posed by North Korea, even as we explore modest steps to re-engage diplomacy. Sports, cultural and education exchanges should be advanced in a process of demonstrating that we bear no-ill will toward the North Korean people, only profound concerns with the practices of the regime.

III Contingencies

Before addressing this issue, this paper would argue that the United

States has a national security interest in the stability of North Korea. This should not be mistaken as support for the regime, but simply as recognition that instability could result in the loss of control over nuclear weapons and material and increase the risks of proliferation.

But, for North Korea, economic reform presents a daunting political challenge to the new leadership. As Andre Lankov recently observed, “a reforming North Korea will likely be very unstable and might collapse.” And what would happen were Jang Song Taek to die or be incapacitated?

At the Institute for National Strategic Studies, my then colleague Ferial A. Saeed and I conducted an 18 month research project on the security and diplomatic challenges involved in the event of instability or regime collapse in North Korea. A central focus of the study was Pyongyang’s potential loss of control over North Korea’s nuclear arsenal and the attendant risk of proliferation. The National Defense University published the results of our research in September of last year under the title “Korean Futures: Challenges to U.S. Diplomacy of North Korea regime Collapse.”

Below are some of our findings:

- Sudden collapse of the DPRK regime will not, at least in the short run, end North Korea as a state. China is likely to seek to perpetuate the North Korean state as a buffer against a democratic and capitalist ROK allied to the United States.
- China will be the first to perceive a leadership crisis in North Korea and will intervene diplomatically to structure a successor regime
- The international community will not endorse ending the North Korean state unless supported by a North Korean majority
- In the event of instability, key policy decisions will be: whether to intervene, who will intervene, under what auspices and for what ends – humanitarian relief, elimination of WMD, stabilization or reunification.

Decisions on intervention and end-states are critical.

- U.S. national security interests mandate WMD elimination, but intervention will be practically difficult and politically problematic, including for our allies. To attain its objectives – e.g. humanitarian assistance, stabilization or WMD elimination, any intervention will require North Korean cooperation. Cooperation can not be assumed and in early stages of any intervention is likely to be withheld
- Preemptive intervention is possible by either China or the United States and the ROK. The risk of miscalculation, given the present lack of communication on security interests and national objectives in the event of North Korean collapse, will be high.
- China and Russia are more concerned about preventing U.S. unilateral intervention than WMD elimination and will likely press for international monitoring of any denuclearization process, using the 2005 Joint Statement to demand peaceful denuclearization.
- China or the United States will move the issue to the UN Security Council in order to constrain the other's actions and to seek legitimacy for intervention.

Given the proliferation risks and national interests stakes involved, the United States, the ROK, China, Japan and Russia are today woefully ill-prepared to deal with the security and political challenges that such a contingency would pose. This is a time for very quiet but intense diplomacy.

사이버 위협의 실태와 대응 방안

임종인 || 고려대학교 정보보호대학원장

요약

정보통신 기술로 인해 우리의 일상은 하루가 다르게 변화하고 있다. 대화, 쇼핑, 뉴스 확인 등 일상적인 생활에서부터 업무처리, 금융거래, 민원 서비스 등 사회활동 전반에 걸쳐 정보통신 기술을 통하여 효율성을 높이고 있다. 하지만 이러한 정보통신 기술에 대한 의존도 증가는 사이버 위협의 증가와 피해의 증가로 나타나고 있는 것이 현재의 상황이다.

사이버 위협은 해킹, 크래킹 등 소극적 공격에서 금전적 목적을 위한 사이버 범죄, 사이버 첩보로, 더 나아가 사회혼란 유발을 위한 사이버 테러, 국가 안보를 위협하는 사이버전으로 진화하고 있다. 해킹 혹은 크래킹은 초기에는 장난, 실력 과시 혹은 대상 시스템의 보안 취약성을 알려주기 위한 화이트해킹으로 시작했다. 하지만 사이버 경제 활동이 증가함에 따라 금전적 이익 취득을 위한 사이버 범죄, 조직의 정보 및 기밀 탈취를 위한 사이버 범죄, 사이버 첩보와 같은 조직화된 범죄 형태로 진화하였다. 이러한 발전은 사이버에 대한 사회적 의존도가 증가함에 따라 최근에는 사이버 테러와 사이버전으로 진화하고 있다.

사이버 테러는 국가 기반시설을 비롯하여 사회적으로 중요한 시설 및 서비스에 대한 공격을 통해 혼란을 유발하는 목적의 행위를 의미한다. 사회적으로 정보통신 기술에 대한 의존도가 증가하며, 특히 제어시스템의 SCADA 시스템으로의 변화, 스마트 그리드의 추진에 따라 사이버 테러는 심대한 위협으로 다가오고 있다.

최근에는 해커 조직이 자신의 정치적 목적, 메시지 전달 등을 위하여 해당 기업, 조

직에 대하여 조직화된 사이버 공격을 하는 Hacktivism이 사이버 테러의 한 형태로 발생하고 있다. Anonymous, LulzSec 등 대표적인 해커 단체들은 WikiLeaks, 월가시위 등 정치적 사회적 현상에 대하여 자신의 의견을 피력하고자 정부 및 기업에 대한 해킹을 시도하고 있다.

이와 같이 사이버 위협이 국가 안보에 위협을 미칠 수 있는 수준의 공격으로 발전하며, 사이버상에서 국가 단위의 분쟁이 발생할 가능성이 나타남에 따라 전쟁 수준의 사이버 위협인 사이버전과 이를 가능하게 하는 무기인 사이버 무기에 대한 개념이 등장하였다. 사이버전의 개념과 정의는 아직 명확하게 이루어지지 않고 있으나, 일반적으로 사이버 공간 내·외부에서 수행되는 다양한 수준의 전투로 기존 네트워크전과 전자전을 포괄하는 개념으로 설명하고 있다.

2007년 발생한 러시아-에스토니아 분쟁에서 에스토니아에 대한 대규모 사이버 공격, 2008년 발생한 러시아-조지아 간의 남오세티아전에서 조지아에 대한 대규모 사이버 공격으로 그 가능성이 확인되었다. 두 사례에서 에스토니아와 조지아는 대규모 DDoS 공격과 해킹, 변조공격 등을 당하며 사이버 인프라의 마비와 사회적 혼란을 겪었다. 2010년 이란 부세를 원자력 발전소를 마비시킨 Stuxnet은 목표를 정하고 이를 마비시키기 위하여 정교하게 제작된 사이버 무기로 분석됨에 따라 사이버 무기의 현실화와 사이버전의 가능성을 국제 사회에 시사하는 중요한 사례가 되었다. 이러한 국가 안보를 위협할 수 있는 사이버전이 현실화됨에 따라 각 국가들은 사이버 사령부 창설, 인재 양성, 대응무기 개발 등 사이버전에 대한 대응을 시작하고 있다.

사이버전에 기존 방어 체계와 개념의 확장이 아닌, 새로운 접근이 필요한 것은 사이버 공간과 사이버전이 가지고 있는 특징에 기인한다. 사이버 공간은 현실 세계와 달리 영토의 개념이 희박하며, 연결되어 있으며, 정형화되어 있지 않거나 볼 수 없다는 특징을 가지고 있다. 사이버전은 이와 같은 사이버 공간에서의 전투들로, 기존의 재래식 혹은 현대식 전쟁과 차이를 보인다. 사이버전은 물리적 충돌 없이 승리할 수 있고, 적은 비용으로 최대한의 효과를 줄 수 있으며, 익명성이 보장되며 보복이 어려운 대표적인 비대칭전이다. 또한 누구나 사이버 공격 무기를 제작할 수 있어, 비국가주체(Non State Actor)에 의하여 수행될 수 있다. 또한 사이버 무기는 목표를 지정하기 어렵고 네트워크의 연결성으로 인하여 피해 양상과 피해대상 예측이 어렵다는 문제가 있다.

대한민국의 경우 2009년 발생한 7.7 DDoS공격, 2011년 3.4 DDoS 공격과 농협

전산망 테러, 그리고 2010년, 2011년, 2012년 발생한 GPS 교란 공격을 통하여 사이버전의 위협성과 특성을 몸소 경험하였다. 7.7 DDoS는 대한민국과 미국의 주요 웹 사이트를 대상으로 발생한 대규모 DDoS 공격이었다. 이 공격으로 인한 피해 금액은 최대 544억 원으로 추정되는데, 이는 2008년 대한민국의 풍수로 인한 재난 피해규모인 580억 원에 육박하는 금액이다. 3.4 DDoS는 7.7 DDoS와 동일한 공격자가 진화한 방식으로 수행한 것으로 추정되는 공격이었다. 7.7 DDoS 이후 대응책 마련을 통하여 큰 피해는 없었지만, 또다시 국가와 사회에 위협이 되는 대규모 DDoS 공격을 경험하였다는 측면에서 의미가 있다. 농협 전산 장애는 국가 정보통신 기반시설로 분류된 금융기관에 대한 사이버 테러로, 직원 노트북에 악성코드를 심어 전산서버 275대를 삭제한 공격이었다. 이로 인하여 농협이 정상화되기까지 2주 이상의 기간이 소요되는 등 큰 피해를 입었으며, 이는 한 국가의 경제안보를 위협할 수 있는 심각한 공격이었다. 이와 같은 공격에서 가장 큰 문제는 공격자를 식별하고 검거할 수 있는 방안이 없다는 것으로, 공격의 억제가 어렵다는 문제를 초래하여 향후 재발의 위험성이 있다.

2010년부터 매년 발생한 GPS 교란 공격 역시 주목해야 할 사례이다. 북한의 개성과 금강산 지역 등에서 발생한 것으로 추정되는 GPS 교란 전파는 군에는 대응책이 마련되어 있어 피해가 적었으나, 민간 항공기와 선박에 피해를 입혔다. 국제민간항공기구(ICAO)는 2011년 교란 공격의 중단을 촉구하는 서한을 발송하였으나, 2012년 또다시 GPS 교란 공격이 발생하면서 실효적인 대응이 되지 못했다. 또한, 민간인 보호를 위한 제네바 협약 Protocol 1의 위반 여부에 대한 논의 역시 제기되고 있으나, 실효적인 대안이 되지는 못하고 있다. 이러한 전자적 공격 역시 규제 및 억제가 어려우며, 기존의 전쟁법으로 해석하기 어렵다는 문제가 있다.

이와 같이 사이버 위협은 국가 안보에 대한 실질적인 위협으로 다가오고 있으며, 이에 대하여 기존의 방어체계와 전쟁법으로는 대응이 어렵다는 문제가 있다. 따라서 이에 대한 개별 국가 차원의 대응과 함께 국제적인 대응이 필요하다. 각 국가 차원에서는 사이버 안보와 관련된 조직의 역할과 책임을 명확하게 하는 거버넌스 체계 정립과, 민-관-군의 협력체계 마련, 사이버전 대응을 위한 기술 연구 및 개발, 전문 인력의 양성 방안과 훈련 계획 마련 등의 대응이 필요할 것으로 예상된다.

국제적 대응 방안은 사이버 공간과 사이버 위협의 특성을 고려할 경우 매우 중요하다. 재래식·현대식 전쟁과 대량살상무기 등은 국제 전쟁 협약을 통하여 효과적으로

규제되고 있는 만큼 사이버전에서도 역시 이러한 국제 협약 및 공동 대응 방안의 마련이 필요할 것이다. 사이버공간에 대한 국제 대응은 2011년 뮌헨 안보회의에서 그 필요성이 제기된 이후 2011년 런던 사이버스페이스 총회, 2012 부다페스트 사이버스페이스 총회, 그리고 2013년 서울 사이버스페이스 총회로 이어지고 있다. 2011년 런던 사이버스페이스 총회는 ‘사이버 공간에서 허용 가능한 행동에 관한 규범’을 주제로, 사이버 공간의 중요성과 사이버 공간이 당면한 문제를 해결하기 위하여 국가 간 협력과 국제행동의 필요성과 가능성을 확인하는 자리였다. 2012년 부다페스트 사이버 공간 총회는 ‘자유와 번영을 위한 신뢰와 안전’을 주제로 국제 협력과 공동 대응방안을 논의하였으나, 아직까지 사이버 공간 질서 수립에 대한 국가 간의 견해 차이만 확인하였다. 2013년에는 대한민국 서울에서 서울 사이버 공간 총회가 예정되어 있으며, 사이버 공간의 보호를 위한 다양한 논의들이 이루어질 것으로 기대하고 있다. 하지만 이러한 논의들은 사이버 범죄와 관련된 논의로 주로 외교적 차원에서 진행되고 있어, 사이버전 대응에 있어서는 한계가 있다고 본다.

사이버전 대응을 위하여 국제적으로는 사이버전 관련 국제협약 마련, 사이버전 국제 공조체계 마련, 사이버 안보 협의체계 운영 등의 노력이 필요할 것으로 보인다. 사이버 위협과 사이버 무기 개발의 억제를 위해서 사이버전 관련 국제협약은 가장 효과적인 해결책이 될 수 있다. 기존 전쟁 관련 협약의 사이버 공간에 대한 적용 및 확장 여부에 대한 논의와 사이버전의 속성을 고려한 새로운 협약의 필요성, 사이버 무기 통제를 위한 협약의 필요성 등을 검토하여 현실적이면서 사이버 위협을 억제할 수 있는 국제협약 마련을 위한 노력이 필요하다. 또한, 사이버 위협이 발생할 경우 이에 대응하기 위한 국제 공조체계의 마련 역시 중요한 과제이다. 사이버 위협은 네트워크의 연결성으로 인하여 한 국가만의 대응으로는 쉽지 않으며, 특히 비국가 주체에 의한 공격이 예상됨에 따라 억제를 위해서는 반드시 공격자 식별 및 제재가 필요하다. 이러한 사이버전 관련 국제협약과 공조체계 마련, 그리고 정보 공유 등을 위한 협의체계 운영도 필요할 것이다. 특히, 사이버전에 있어서 군사시설과 민간시설의 경계가 모호해짐에 따라 이 협의체계에는 학계, 기업, 국제기구 등 민간의 참여 역시 필요할 것으로 판단된다.

사이버 위협은 나날이 진화하여 국가 안보를 위협하고 있으며, 사이버전이 현실화되고 있는 상황이다. 반면 기존의 대응체계로는 이러한 사이버전에 대응을 할 수 없으

며, 사이버전에 대한 개별 국가와 국제적인 대응은 미비한 상황이다. 따라서 사이버전 준비체계 확립을 위한 노력, 특히 국제적인 노력이 필요한 시점이다. 사이버 위협에 대한 인식과 각 국가의 대응 현황 공유를 통해 인류의 새로운 소중한 공간인 사이버 공간을 지키기 위한 노력을 시작할 수 있을 것이라 생각한다.

Current Status of Cyber-Threats and Responses

Korea University Department of Cyber Defense
Graduate School of Information Security


Dean, Prof., PH.D. **Jongin Lim**





Contents

I	Current Status of Cyber-Threats	3 Page
II	Characteristics of Cyber Spaces & Warfare	8 Page
III	Ways to Respond Cyber Threats	13 Page
IV	Conclusion and Questionnaires	18 Page





Current status of Cyber-Threats

Current Status of Cyber-Threats

Hacking, Cracking

**호기심, 실력과시 등의 목적으로
바이러스 제작 등 소극적 형태의 공격**

- 자신의 실력을 자랑하기 위하여 바이러스 제작, 공격 등을 수행하는 크래킹, 대상 시스템의 취약점을 알려 주기 위한 목적의 해킹시도 등
- 화이트 해킹

Overview | 

Evolving Cyber-Threat

Cyber Crime & Espionage

**금전 취득 목적으로 사이버 공격을 수행하거나
정보시스템에 침입하여 군사·산업기밀 등 유출**

- 악의적인 목적으로 정보시스템을 공격하거나, 침입하여 원하는 정보를 탈취하는 행위
- Advanced Persistent Threat
- Wiki Leacks (2010), Operation Aurora (2009)

Cyber Terrorism

**메시지 전달 및 사회 혼란을 유발하기 위한
목적의 대규모의 조직적인 사이버공격**

- 테러성의 공격을 통하여 사회의 혼란을 초래하거나, 정치적 메시지 전달을 위하여 해킹을 통하여 주위 환기
- 7.7 DDoS (2009), NH Bank(2011) : Korea
- Hacktivism : Lulzsec, Anonymous


Cyber Warfare

**사이버공간 내/외부에서 수행되는 다양한
수준의 전투로 네트워크전, 전자전을 포괄**

- 국가에 의하여 혹은 비국가주체에 의하여 적국의 군사 정보체계, 국가 전산자원 등을 공격하는 행위
- 심리전, 네트워크 중심전, 전자기전 등을 포괄
- Estonia(2007), Russia-Georgia(2008), Stuxnet(2010)

KOREA UNIVERSITY Department of Cyber Defense
Graduate School of Information Security
4 / 21

Current Status of Cyber-Threats



CyberAttack
Cyber Terrorism

Cyber Terrorism

사회 혼란을 유발하기 위한 목적의 대규모의 조직적인 사이버공격

- 주요기반시설 혹은 사회적으로 중요한 시설, 서비스를 공격하여 사회적 혼란을 유발하는 형태의 사이버 공격
- 사회 전반에 걸쳐 IT에 대한 의존도가 증가함에 따라 사이버테러는 심각한 혼란 및 피해를 초래할 수 있음

사이버테러의 사례



- 7.7 DDoS(2009)
- 미국과 한국의 주요 홈페이지에 대한 DDoS 공격 발생
- 공공기관, 포털, 금융사홈페이지 등에 대한 접속 장애
- NH Bank(2011)
- 한국의 NH은행에 대한 사이버테러로 전산장애 발생
- 서버 삭제 등으로 전산장애 및 일부 거래기록 유실
- FireSale on DieHard 4.0(2007)
- 교통망, 금융망, 상하수도 시설 등을 해킹을 통하여 장악하여 사회적 혼란 유발

Hacktivism

정치적 견해 등 특정 목적을 가지고 시위의 일종으로 해킹 공격을 수행하는 행위

- 해킹(Hacking)과 행동주의(Activism)의 합성어로, 정치적 목적과 같은 특정 목적을 가지고 시위의 일종으로 정부 및 민간기업을 대상으로 해킹 공격 행위
- 반전, 반세계화 운동, 지적재산권 관련 변화 또는 국가간 영토분쟁 등 정치적·사회적 역학관계 속에서 변조, 정보유출, DDoS 등 해킹공격을 통하여 의견 표출

주요 해커그룹과 해킹티즘 사례

<p>Annoymous </p> <ul style="list-style-type: none"> · IMF 전산시스템 · 마스터카드, 비자카드 · NYSE · 샌프란시스코 대중교통시스템 · 미 법무부 홈페이지 	<p>LulzSec </p> <ul style="list-style-type: none"> · 소니 DB, 웹사이트 · 미 공영방송 PBS · FBI애틀랜타 지부 · 미 상원 웹사이트 · CIA 웹사이트
--	--

KOREA UNIVERSITY Department of Cyber Defense Graduate School of Information Security
5 / 21

Current Status of Cyber-Threats



Beginning of Cyber Weapon
Stuxnet(2010)

Outline of the Stuxnet

이란 부세르 원자력 발전소 가동을 저지하기 위하여 정교하게 제작된 악성코드

- 2010년 6월, 최초로 발견된 SCADA 시스템 대상 악성코드
- 2010년 9월, 이란은 부세르 원자력발전소가 Stuxnet에 감염되었으며, 이로 인하여 가동이 중단되었다고 발표
- 5개의 제로데이 취약점을 이용하여 USB를 통하여 감염되며, SIMENS사의 WinCC와 Step7의 운영시스템에 침투하여 감염된 제어시스템의 PLC 제어권을 획득



Source : The Globe and Mail, "How the Stuxnet virus works"

Stuxnet as a Cyber-Weapon

Stuxnet이 최초의 사이버무기라는 주장

- 스텝넷은 이란의 핵무기 개발을 저지하기 위하여 미국, 이스라엘 등이 협력·개발한 사이버무기로 인식
- 2012년 6월, 뉴욕타임즈는 Stuxnet은 부시 대통령 시절 부터 미국이 주도하여 추진되었으며, 'Operation Olympic Game' 이라 명명된 작전이라 보도

The New York Times

Middle East

Israeli Test on Worm Called Crucial in Iran Nuclear Delay

The New York Times

Middle East

Obama Order Sped Up Wave of Cyberattacks Against Iran

By DAVID E. SANGER
Published: June 1, 2012 | 363 Comments

WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyber-weapons, according to participants in the program.

FACEBOOK
TWITTER
GOOGLE+
EMAIL

KOREA UNIVERSITY Department of Cyber Defense Graduate School of Information Security
6 / 21

Current Status of Cyber-Threats

Cyber Conflicts between Nations Cyber Warfare

Recognize Possibilities of Cyber Warfare


사이버전 관련 사례 발생

- 1차·2차 이라크전, 쿠소보전에서 해킹 및 전자전 장비 등을 통하여 적국의 방어시스템을 무력화한 사례
- 러시아-에스토니아 사이버전쟁(2007), 러시아-조지아전(2008)에서의 사이버 공격 사례
- Stuxnet을 통하여 사이버무기의 활용 가능성과 이를 통한 사이버전의 가능성 확인

사이버전 가능성 인식과 대응

- 여러 사례를 통하여 사이버 상에서 국가간 분쟁의 가능성이 확인됨에 따라 사이버전에 대한 개념 논의 시작
- 현재 사이버전은 초창기 핵무기와 비슷한 상황으로, 핵의 경우 공포로 억제력이 작용하였지만, 사이버전은 이러한 억제력이 없어 대응이 필요함 (Joseph Nye, 2011)
- 각 국의 사이버시령부 창설, 미국의 사이버 공격 시 이를 전쟁행위로 간주하여 물리적 공격 대응 발표 등 사이버전에 대한 대응태세를 갖추고 있는 상황

Recognize the Possibilities of Cyber Warfare




The image shows a stack of news articles from various sources including BBC NEWS, The New York Times, and The Wall Street Journal. The articles discuss cyber warfare, Georgia's conflict with Russia, and the concept of cyberspace wars.


KOREA UNIVERSITY Department of Cyber Defense
Graduate School of Information Security

7 / 21

II Characteristics of Cyber Spaces & Warfare




Ministry of National Defense
Republic of Korea



KOREA UNIVERSITY

Characteristics of Cyber Spaces & Warfare




Distinct Characteristics
Cyber Spaces

Real World	Cyber Spaces
Based on Physical spaces	Based on Information Technologies
Territory	Network
Fixity	Motion/Flux
Embedded	Disembedded
Material	Immaterial
Visible	Invisible
Tangible	Intangible
Actual	Virtual/Abstract
Euclidean/Social Spaces	Logical Spaces

KOREA UNIVERSITY Department of Cyber Defense
Graduate School of Information Security
9 / 21

Characteristics of Cyber Spaces & Warfare



Distinct Characteristics
Cyber Warfare

- 1

비대칭 전력으로서의 사이버전

 - 물리적인 충돌 없이 승리할 수 있는 최신 비대칭전의 한 영역
 - 적은 비용으로 최대의 효과를 줄 수 있으며, 공격자의 익명성이 보장되고, 공격자가 노출되어도 보복이 어려운 등 공격자에게만 유리한 전쟁
- 2

비국가행위자(Non-State Actors)가 수행할 위험성


 - 국제법은 국가 사이의 무력사용만을 규제하는 반면 사이버전은 비 국가행위자에 의해 수행 가능
 - 사이버공격은 누구나 S/W 개발 능력만 있으며 제작, 구매, 대여하여 수행 가능
- 3

전통무기와는 다른 피해양상

 - 사이버전의 무기는 대부분 물리적 피해와는 관련이 없어 전통적인 무기 개념에 포함이 어려움
 - 따라서, 사이버전 역시 UN헌장 제 2(4)조에 금지하는 무력사용이라 보기 어려움

KOREA UNIVERSITY Department of Cyber Defense
Graduate School of Information Security
10 / 21


Characteristics of Cyber Spaces & Warfare



Distinct Characteristics Cyber Warfare


4 피해대상 구분의 어려움

- 사이버전은 목표를 지정하여 공격이 어려우며, 대상이 되는 컴퓨터 등의 민/군 구분도 쉽지 않음
- 공격을 원치 않은 대상이라도 같은 취약점이 존재한다면 영향을 미칠 수 있어 윤리성 논란이 존재




5 공격자 식별 및 사실관계 확인의 어려움

- 사이버공격은 좀비PC의 이용, 타국 서버 경우 등을 통해 이루어져 공격자 식별 및 확인이 어려움
- 방어자에게 과도한 부담을 지우는 비대칭성
- 공격자 역주적 및 식별의 어려움으로 정당한 보복과 처벌을 통한 전쟁 억제력을 힘들게 하는 문제



6 공격자에게도 피해 전파 가능성


- 전세계 모든 국가가 인터넷으로 연결됨에 따라 사이버 공격이 공격자에게도 전파될 가능성 존재
- 미국은 이라크 공격 시 이라크 금융시스템을 공격하려 했으나, 여파가 자국에도 미침에 따라 포기



KOREA UNIVERSITY Department of Cyber Defense
Graduate School of Information Security

11 / 21

Characteristics of Cyber Spaces & Warfare



Example Case of Korea NH Bank Hacking (2011.04)

Outline of the NH Bank Hacking

**한국의 주요 금융기관인 NH은행이
사이버공격으로 인하여 전산 장애 발생**

- 2011년 4월 12일, NH은행의 전산 서버에서 장애가 발생하여 거래 중단 및 일부 서비스 중단
- NH은행 전산을 관리하는 협력업체 직원의 노트북에 의하여 서버 삭제명령 rm.dd 가 전송되었으며, 중계 서버 및 백업서버 275개의 데이터가 손상
- 이로 인하여 시스템이 완전 정상화되기까지 2주 이상 소요되었으며, 일부 거래 기록 유실

사이버테러 행위에 대한 수사 결과

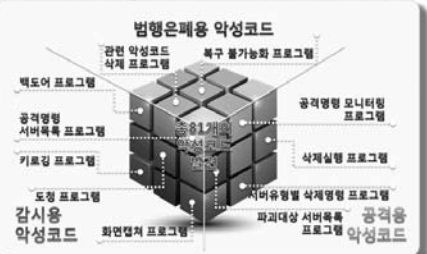
- 수사 결과 해당 직원은 수시로 서버 관리 노트북을 반출하였으며, 해당 노트북에서 81개의 악성코드 발견
- 악성코드 분석 결과, 공격용 악성코드, 감시용 악성코드, 범행은폐용 악성코드로 구성된 정교한 악성코드

Limitation of Response

사이버테러 행위 대응에서 나타난 한계

- 해당 노트북에 접속한 IP 역주적 결과, 여러 국가 IP를 경유하였으며, 이에 따라 공격자 식별에 어려움 겪음
- 경제안보를 위협하는 심각한 사이버테러 행위였음에도, 공격자를 검거 혹은 처벌할 수 있는 방법이 부재하여 향후 공격을 억제하기 위한 방안 부재

범행은폐용 악성코드



KOREA UNIVERSITY Department of Cyber Defense
Graduate School of Information Security

12 / 21



III Ways to Respond Cyber Threats




Ways to Respond Cyber Threats



Cyber Warfare
Cyber Warfare Readiness



사이버
전력 강화

사이버전
억제

Cyber Warfare
Readiness

Doctrine	사이버전 국제협약, 관련 국내법 사이버전교전규칙, 사이버전 전략전술
Organization	사이버사령부를 포함한 군 사이버전 명령체계 민간영역을 포함한 사이버안보 거버넌스
Training	사이버전 대응훈련 각종 전략적 군사훈련에 필수 포함
Material	H/W, S/W 사이버무기연구개발
Leadership /Education	사이버국방인력양성 전문화 대학교육 강화
Personnel	사이버국방인력 확보 효과적인 리크루팅과 경력관리
Facilities	안정적인 사이버무기 생산 시설 사이버전 훈련 설비 확립

KOREA UNIVERSITY Department of Cyber Defense
Graduate School of Information Security

14 / 21

Ways to Respond Cyber Threats



Cyber Warfare
Domestic Approach

Cyber Security Governance

**사이버안보와 관련된
각 조직의 역할과 책임 명확화**

- 각 정부 기관의 사이버보안, 사이버테러, 사이버전 관련 역할과 책임을 명확히 규정
- 위기 상황 발생 시, 공격 유형에 따라 대응 주관 기관을 지정하며, 분산된 사이버보안 관련 역량을 집중시키기 위한 위기대응체계 마련

Military-Public-Private Partnership

**사이버전 대응을 위해서는
민-관-군의 협력체계가 필요**

- 전력망 등 민간이 관리하는 제어시스템과 인터넷 통신망 등 주요기반시설에 대한 공격 대응을 위해서는 공공-민간 협력이 필수적
- 효과적인 대응을 위해서는 민간기업과 학계 전문가 등 다양한 민간의 사이버보안 역할과의 협력 필요

Research & Development

**사이버전 대응을 위한 각종 기술과
공격, 방어 무기 연구·개발**

- 사이버전에서 활용 가능한 논리적 공격, 전자기적 공격, 심리적 공격 등에 대하여 연구 필요
- 역추적 기술, 국방 암호기술, 말리타리 포렌식 기술 등 사이버전에서 요구되는 기술들에 대하여 연구·개발

Human Resource

**사이버전 대응을 위하여
전문인력 양성·확보·훈련 계획 마련**

- 사이버보안에서 가장 핵심적인 요소는 인력으로, 사이버전에서도 보안기술과 군사환경 모두를 숙지하고 있는 전문 인력 양성이 핵심적인 과제
- 기존 군 인력에 대해서도 정보전, 심리전, 전자기전 등에 대한 교육을 통하여 작전수행 능력 향상

KOREA UNIVERSITY Department of Cyber Defense Graduate School of Information Security 15 / 21

Ways to Respond Cyber Threats



Cyber Warfare
International Approach

사이버전 관련 국제협약

- 기존 전쟁 관련 규약의 사이버전 적용가능 여부 및 확장 방안 논의
- 사이버전의 속성을 고려한 새로운 사이버전 관련 협약의 필요성 논의
- 사이버전에서 활용될 수 있는 무기 통제를 위한 국제협약 필요성 논의

사이버전 관련 국제 공조체계

- 초국가적 안보위협에 대응하기 위하여 국제 공조체계 마련의 필요성
- 사이버전 관련 비국가주체에 대한 사법 공조방안 논의
- UN, 인터폴 등 기존 국제기구와 공조방안 논의

사이버안보 협의체계 운영

- 사이버전 관련 규범 마련, 국제 공조체계를 논의하기 위한 협의 체계
- 사이버 위협 대응을 위한 협의체계, 국가 사이버위협 정보 공유
- 공공부문 뿐만 아니라 민간 역시 사이버안보 관련 공동연구와 기술 및 정보의 공유가 이루어질 수 있도록 정부와 민간의 이중 협의 채널 구성

KOREA UNIVERSITY Department of Cyber Defense Graduate School of Information Security 16 / 21

Ways to Respond Cyber Threats



Warfare and Cyber Security International Effort



국제 전쟁 협약

전쟁, 전쟁윤리, 대량살상무기 통제 등을 위하여 국제 협약 마련

- 전쟁을 일정한 법적 형식이나 법규칙에 따라서 수행하기 위한 조약 마련의 필요성 인식으로, 헤이그 평화 회의에서부터 국제 전쟁 협약 마련을 위한 노력
- 전쟁 선포, 양복 수락, 포로 대우, 군사적 필요, 분별 및 비례, 사용 가능한 무기 제약 등으로 구성

사이버안보 관련 국제 협약 및 논의

사이버범죄, 사이버보안 국제 공조를 위한 협약 및 노력

- 사이버범죄 대응 및 사이버보안 강화를 위하여 국제 공조의 필요성 인식
- 부다페스트 사이버범죄 국제회의에서 범죄행위의 범위를 규정하며, 국제공조체계 구축하는 성과
- 런던사이버공간 회의를 시작으로 국제적 논의가 발전되고 있으며, 사이버전 관련 규범도 논의

협약	생무 제목	년도
제네바 협약	지상전에서의 군대 부상자의 처우 개선을 위한	1864
헤이그 회의 II	지상전 법규	1869
헤이그 회의 IV	지상전 법규	1907
제네바 의정서	전쟁에서 독성가스와 채광무기 사용 금지	1928
제네바 협약 I	지상전에 있어서의 군대의 부상자 및 병자의 처우개선에 관한	1864, rev. 1949
제네바 협약 II	해상에서의 군대의 부상자, 병자 및 조난자의 처우개선에 관한	1949
제네바 협약 III	전쟁포로의 대우에 관한	1929
제네바 협약 IV	전시 민간인의 보호에 관한	rev. 1949
제네바 협약	새군기 및 특수무기의 개발, 생산, 비축의 금지에 배기	1975
의정서 I	국제적 무력충돌의 희생자 보호에 관한 의정서	1977
의정서 II	비국제적 무력충돌의 희생자 보호에 관한 의정서	1977
의정서 III	추가되는 식별 가능한 표식의 적용에 관한 의정서	2005



- 사이버공간의 위험성과 해결의 열망에 대한 국제적 공감대 형성
- 사이버공간 문제 해결을 위한 국가 간 협력과 국제행동의 가능성 확인



- 사이버범죄 척결과 사이버 안전 강화를 위한 노력
- 국제협력과 공동대응방안 논의


2013 Seoul Conference

- 국제 사이버전 관련 협약 논의 및 체결을 위한 노력
- 국제 사이버전 관련 기구 유지 등

IV

Conclusion & Questionnaires

Conclusion & Questionnaires



Current Status of Cyber Threat Some New Approaches Needed

사이버전의 현실화

- 사이버 공격은 더욱 정교하며 조직적으로 발전하고 있으며, 테러·전쟁 수준으로 확대
- 전사회적인 정보화로 사이버전 발생 시 국가적 피해가 예상됨

사이버전에 대한 대응 미비

- 사이버전은 기존 전쟁과는 다른 양상을 보여, 기존 전쟁 관련 국제규범으로는 대응이 어려움
- 사이버공격은 여러 국가를 경유하거나, 비국가 주체에 의해 수행될 수 있어 국제공조가 필요

사이버전 준비체계 확립을 위해서는 새로운 접근방식 필요

각 국가의 사이버전 준비체계 확립


- 사이버 위협을 인식하고, 국가 안보를 지키기 위한 대응체계 마련
- 사이버보안 거버넌스, 민-관-군 공조체계, 연구개발, 인력양성 등

국제협약, 공조체계 등 국제적 대응방안 확립

- 기존 전쟁 및 무기 관련 협약의 확대방안 혹은 새로운 협약 마련 논의
- 국제 공동 대응, 협의채널 마련 및 사이버전억제를 위한 공조 방안

KOREA UNIVERSITY Department of Cyber Defense
Graduate School of Information Security
19 / 21

Conclusion & Questionnaires



Questionnaires to each Countries

- Q 1.

Each country's cases of cyber threat and cyber threat level?
- Q 2.

Significance and direction of cyber threats within the framework of international efforts on counter-terrorism?
- Q 3.

Current position, laws enactment, and direction related to cyber threat?
- Q 4.

Cases of inter-agency collaboration for cyber threat response?
- Q 5.

Cooperation and coordination options to counter cyber threat among countries (technology transfer and education etc)?
- Q 6.

Civil capabilities for cyber threat and limitations?

KOREA UNIVERSITY Department of Cyber Defense
Graduate School of Information Security
20 / 21

Thank you.

jilim@korea.ac.kr



일본의 사이버 보안과 정보활동 : 동아시아의 새로운 위협에 대한 대응¹

Motohiro Tsuchiya || 日 게이오 대학교 언론 및 통치대학원 교수

목 차

- I. 서 론
- II. 사이버 안보 및 정보
- III. 일본 정보기관 및 동아시아 정세 변화
- IV. 동아시아의 사이버 위협 확산
- V. 일본 정부의 대응
- VI. 동아시아의 변화
- VII. 결 론

I 서 론

오늘날 많은 국가에서 사이버 보안은 기존에는 없던 새로운 비전통적인 안보 관심사이며 동아시아도 예외는 아니다. 많은 정부 기관과 자산, 사기업, 개인들이 줄줄이

1) 본 논문의 수정본은 Motohiro Tsuchiya, "Cybersecurity in East Asia: Japan and the 2009 Attacks on South Korea and the United States," in Kim Andreasson, ed., Cybersecurity: Public Sector Threats and Responses, Boca Raton, FL: CRC Press, 2012, pp.55~76에 발간되었다.

공격받고 있다. 2009년 7월, 미국 독립기념일 직후, 미국과 한국의 인터넷 서비스가 대규모 디도스 공격을 받았다. 아직도 이 공격을 시도한 범인이 누구지 모르지만 일본을 포함한 많은 국가들은 인터넷 구름 속에 숨은 익명의 전사들 혹은 테러리스트들로부터 국가를 지키는 것이 얼마나 중요한지 깨닫게 되었다.

본 논문은 일본 정부가 2009년 미국과 한국이 받은 공격에 어떻게 대응했는지를 분석한다. 특히 정보기관과 사법당국 간의 협력과 경쟁에 초점을 맞췄다. 기존에 일본 내에서 정보관련 사항에 대해 이 두 기관의 역할은 잘 나뉘져 있지 않았다. 그러나 새로운 사이버 위협들은 정부시스템의 변화를 요구하고 있다. 현존하는 시스템으로는 효과적으로 대응할 수 없을 만큼 그들은 너무 복잡하고 교묘하기 때문이다.

2005년도에 설립된 국가정보보안센터(National Information Security Center : NISC)는 이러한 새로운 환경에 대응하기 위한 핵심기관이다. 이 센터는 총리실 내각산하에 설치되어 있다. 이 센터는 과거에 사이버 안보 관련 기술적인 문제들에 초점이 맞춰져 있었으나, 2009년 7월 사이버 공격 이후 국가안보 차원의 기관으로 빠르게 변하고 있다. 사법당국과 정보기관 간의 협동 시스템인 NISC는 미래 사이버 위협과 기타 위협에 대응하기 위한 일본 정보 시스템 재조직의 첫걸음이 될 것이다. 본 논문은 공공 문서 및 기록을 분석하고 관련 당국과의 인터뷰를 통해 사이버 안보의 더 나은 방향과 제도에 기여할 것이다.

II 사이버 안보 및 정보

사이버 공간의 안보는 탈냉전기 변화의 좋은 예이다. 전쟁은 물리적 테러리스트로부터 네트워크로 이전하고 있다. 군사력으로 전투를 치렀던 지상, 해양, 공중, 및 우주주는 자연적 공간이다. 그러나 사이버 공간은 컴퓨터, 광섬유 및 기타 장치들이 구성하는 인조적 공간이다. 오늘날 군사력의 지휘통제는 정보 및 커뮤니케이션 네트워크에 의존한다. 현대의 디지털화된 군사력은 정보 및 커뮤니케이션 네트워크 없이 싸울 수 없다.

의도적으로 전쟁공간을 발명할 필요는 없다. 그것은 컴퓨터 게임으로도 충분하다. 그러나 세계가 정보 및 커뮤니케이션 네트워크에 점점 의존하고 정보사회가 부상하고 있는 만큼, 우리의 인식 또한 실제 공간 및 영토보다는 사이버 공간으로 치우치고 있다. 우리가 컴퓨터 및 네트워크의 케이블을 잘라버리지 않는 한, 새로운 위협이 있을 수 있고, 우리는 그것을 보호하기 위한 보안이 필요하다.

사이버 공간에는 다양한 종류의 범죄행위가 존재하며, 범죄자 또한 다양하다. 비슷하고 다양한 개념에 차이를 두기 위해서는 2선의 수직선 및 수평선으로 구분된 2차원적 4개의 사각형을 상상해 보자(그림 1 참조). 수평선은 사용자의 의도를 나타내며 “선함”에서 “악함”까지 범위를 둔다. 수직선은 사용자 숫자를 나타내며 “개인”에서 “단체”까지 범위를 둔다. 이 방식에 나타난 4개의 카테고리는 4개의 서로 다른 특성을 보여준다.

첫 번째 카테고리는 좋은 의도를 지닌 개인 사용자이다. 이 사용자들은 “해커”라고 불린다. “해커”라는 용어는 원래 컴퓨터에 상당한 지식을 지닌 개인을 뜻하며 악한 의도를 의미하지 않았다. 현대 용어로는 “깁(Geeks)”라고도 불린다. ‘깁’은 “지나칠 정도로 똑똑하여 특이하거나 독특한 사람”을 뜻한다. ‘깁’에 의해 발전된 네트워킹 문화는 정부문화와 상이하다. 유명한 ‘깁’인, 미국의 메사추세츠 공대(MIT)의 Dave Clark 교수는 다음과 같이 말했다. “우리는 왕, 대통령, 및 투표를 거부한다. 우리는 개략적 합의(rough consensus)와 연속적 코드(running code)를 믿는다.” 개략적 합의

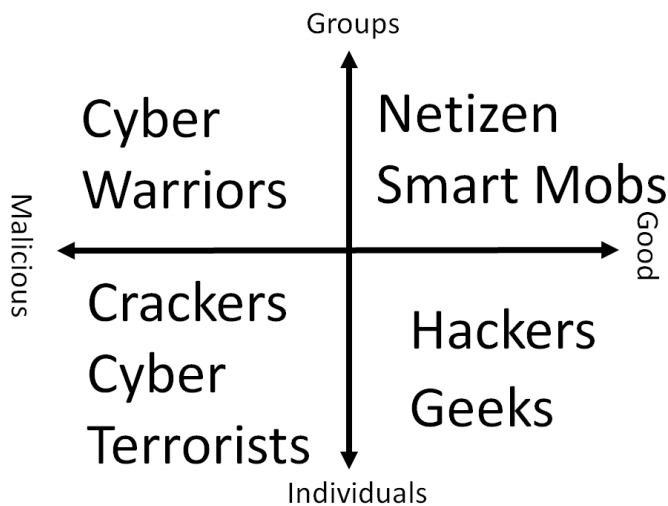


그림 1 : 사이버 안보에 관한 개념

(rough consensus)는 몇년이 걸리더라도 거의 모든 인원이 동의할 때까지 어떠한 사항에 대해서 논의를 한다는 것을 의미하고, 연속적 코드(running code)는 그들이 가능한 실질적인 결과를 도출할 수 있도록 계속해서 시도한다는 것을 암시한다. 그들은 추상적인 관념론이나 실행 불가능한 규칙 따위를 받아들이지 않는다. 많은 정부기관은 이러한 ‘긱’ 들과 함께 일하는 것이 어려울 수도 있다. 하지만, 이런 ‘긱’ 들은 점점 우리의 사회체계를 통제하고 있다.

두 번째 카테고리는 좋은 의도를 지닌 그룹이다. 이들은 “네트워크(net)와 “시민(citizen)”이라는 단어의 조합인 네티즌이라고 알려져 있고, “스마트 몹(Smart mobs)”이라고도 알려져 있다.² 이들은 단체의 목표를 이루기 위해서 네트워크에 기반한 기술과 지식을 사용한다.

문제는 악의를 지닌 사용자이다. 악의를 지닌 사용자 집단은 “사이버 워리어(Cyber warriors)라는 별칭을 지닐 수 있다. 그들은 정부기관이나 비정부기관의 후원을 받을 수도 있다. 어찌되었건, 그들은 조직의 목표를 이루기 위해 네트워크 기술을 남용하는 사용자들이다.

마지막으로, 악의를 지닌 개인사용자들도 있다. 이들은 한때 “해커” 보다도 “크래커(Crackers)”라고 알려져 있었다.³ 하지만, 단순히 개인의 즐거움보다 정치적인 의도로 파괴적 행위를 하는 사용자들은 “사이버 테러리스트”라고 호칭될 수 있다. 일반적으로, “사이버 테러리스트”는 “사이버 워리어(Cyber warriors)” 또한 포함한다고 추정할 수 있다.

악의를 지닌 사용자들의 행위는 그 행동의 내용에 따라 두 가지 카테고리로 나눌 수 있다 미국 RAND 연구소의 연구원 John Arquilla와 David Ronfeldt는 “네트워크 전쟁(net war)”과 “사이버 전쟁(cyber war)”에 차이를 둔다.⁴

네트워크 전쟁은 사회적 수준의 관념적 분쟁으로 이루어져 있으며, 국가 및 사회 간에 일어난다. 그들의 목표는 사회 또는 고위층, 또는 이 두 가지 모두를 표적 삼아, 대

2) Howard Rheingold, *Smart Mobs: The Next Social Revolution*, Cambridge, MA: Perseus Publishing, 2002.

3) Steven Levy, *Hackers: Heroes of the Computer Revolution*, New York: Dell, 1984.

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

상 인구의 “지식”을 분열, 손상, 바꾸는 데에 있다. 간단히 말하자면, 네트워크 전쟁의 목적은 사람들의 머리를 혼란에 빠지게 하는 것이다.

반대로, 사이버 전쟁은 정보관련 원칙에 의거한 군사작전의 수행이다. 이러한 작전은 코소보, 에스토니아 등 기타 지역에서도 수행되었다. 사실상, 이것은 정보 및 커뮤니케이션 체계의 물리적 붕괴를 의미한다.

네트워크 전쟁과 사이버 전쟁의 의미에 차이를 명확히 하기 위해서는, 우선 네트워크 전쟁을 “두뇌전쟁(head war)”이라 간주할 수 있다. 왜냐면 네트워크 전쟁은 머릿속의 무언가를 수정하거나 바꾸는 것을 시도하는 행위이기 때문이다. 반대로, 사이버 전쟁은 “육탄전(body war)”이 될 수도 있다. 사이버 전쟁은 물리적 피해를 의미하기 때문이다.

결론적으로, 사이버 테러리즘의 개념은 주관이 단체인지 개인인지, 그리고 대상이 정신적인지 육체적인지에 따라 다수의 카테고리로 나누어질 수 있다.

우리의 사회체계가 컴퓨터에 의존하면 할수록, 사회는 사이버 테러리스트 공격에 취약해진다. 문제는 컴퓨터와 네트워크는 우리에게 “블랙박스(Black boxes)”를 남긴다는 점이며, 점진적으로 내부의 원리를 이해하는 것이 어려워지고 있다.

그 결과, 우리는 이미 공격을 당하고 있을지도 모른다는 위협에 노출되어 있다. 네트워크를 통한 리모컨 조작으로 댐을 폭파하는 공격은 누구나 알고 있을 것이다. 반면에, 컴퓨터 기록을 수정하려는 목적으로 비밀리에 컴퓨터 데이터 베이스가 노출되었다면, 공격 가해자와 공격 시간은 알려지지 않았을 가능성이 크다. 이것은 왜 사이버 테러리즘이 불안함을 조성하는 어려운 개념인지를 보여준다.

인터넷 관련 기술은 다방면으로 공유되고 있으며, 이를 원하는 사람은 누구나 이용할 수 있는 특성을 지니고 있다. 이것은 숙련되지 않은 인원에게는 해독하기 어려운 블랙박스 같을지도 모르지만, 숙련된 인원에게는 사실상 쉬울 것이다. 인터넷은 거대한 복사 기계와도 같아서 이러한 기술은 순식간에 퍼진다.

美 하버드대학교 교수 Joseph S. Nye, Jr.는 다음과 같이 말했다. 최근 정보통신 기술의 발달에는 힘의 분산이라는 특징이 있다. 사이버 공간은 행위자들의 능력을 평준화 할 뿐만 아니라 뒤섞는다. 또한 “사이버 파워”라는 새로운 힘이 부상하고 있다. 이것은 “사이버 영역에서 전자적으로 연계된 정보자원을 통해 원하는 결과를 얻는 능력”이다. 세력범위 측면에서, 사이버 파워는 해양력(海洋力), 항공력(航空力), 우주력

(宇宙力)에 이은 네 번째 힘이다. 사이버 공간에서는 다양한 네트워크 조직이 부상하고 소규모 행위자들이 더 많은 힘을 얻음으로 인하여 힘이 분산된다.⁵

힘의 확산은 일정한 속도로 이루어지지 않는다. 정보통신 기술의 충분한 기반시설이 구축되어 있지 않은 국가는 사이버 파워를 얻을 수가 없을 것이다. 이러한 기반시설로, 작은 국가의 한 개인이 더 큰 국가의 정부 서버를 표적 삼을 수 있으며, 충분한 지식과 기술은 서버를 공격할 수 있는 능력을 부여한다.

표적이 자신도 모르게 공격을 당하는 사례도 있기 때문에, 법률 집행기관뿐만 아니라 정보기관 또한 국가안보를 위협하는 심각한 사이버 공격에 대응하는 방어에 개입해야 한다.

간단히 말해서 정보가 지식은 아니다. 국가 안보 및 외교 측면에서 정보는, “외부 [기관]에 관련된 가용한 정보의 수집, 처리, 통합, 분석, 평가 및 해석의 결과물이며, 이러한 기관은 외국 정부, 테러리스트 집단을 포함한 단체, 또는 기타 분야를 포함할 수도 있다.⁶ 자료 및 첩보가 아직 확실한 것이 아니라면, 정보는 자료와 첩보에 기반한 확실한 결과물이다. 이러한 정보를 생산하는 정부기관이 “정보기관”이라고 불린다.⁷

본 논문에서는, 냉전 이후 동아시아의 정세가 일본 정보기관을 재활성화시켰다는 점과, 2009년 7월 미국과 한국에 대한 인터넷 공격과 같은 사이버 안보의 증가하는 문제점이 정보기관에 새로운 역할을 부여했다는 점에 대해 논의할 것이다.

5) Joseph S. Nye, Jr., “Cyber Power,” Harvard Kennedy School Belfer Center for Science and International Affairs, May 2010.

6) Joint Chiefs of Staff, U.S. Department of Defense Dictionary of Military Terms, New York: Arco, 1988, p.183.

7) Omori, Yoshio, Japanese Intelligence Agencies, Tokyo: Bungei Shunju, 2005 (Japanese). Kitaoka, Hajime, Introduction to Intelligence, 2nd Edition, Tokyo: Keio University Press, 2009 (Japanese). Kotani, Ken, Intelligence Diplomacy in the U.K., Tokyo: PHP, 2004 (Japanese). Fukuda Mitsuru, Terrorism and Intelligence, Tokyo: Keio University Press, 2010 (Japanese).

Ⅲ 일본 정보기관 및 동아시아 정세 변화

1. 일본 정보기관의 발전

중국의 전설적인 철학자 손자는 2,500년 전에 전쟁 및 스파이에 관한 그의 철학을 기술했다. 약 750년경 그의 사상이 일본으로 건너왔다. 따라서 수많은 닌자 및 첩보원이 생겼고, 사무라이들에게까지도 퍼졌다. 닌자를 잘 활용하기로 알려진 유명한 사무라이 Shingen Takeda는 그의 전쟁 특성에 손자의 철학을 반영하였다. 1604년 Tokugawas의 정복 이후, 일본은 무려 260년 이상 “평화로운 기간”을 즐겼다. 이 기간 중 Tokugawa Shogunate는 일본 전 지역의 질서를 유지하기 위해 닌자를 고용하였다.

1868년 메이지 유신(Meiji Restoration) 이후, 일본은 외국과 모든 교류를 중지하였고 서양 기술 및 사상을 긍정적인 방향으로 받아들였다. 그 중 하나는, 정보에 관련된 군 조직이었다. 일본제국의 해군 및 육군은 정보부문을 설립하였다. 또한, 정보수집, 대-정보, 첩보활동을 시작하였다. 그 중 Motojiro Akashi가 가장 성공적인 임무를 수행하였다. 러시아 및 유럽국가에서 그의 정보수집 및 첩보활동은 1904년 러-일 전쟁에서 일본을 승리로 이끌었다.

오늘날 많은 사람들이 일본제국 육군에 의해 설립된 Nakano School을 잘 알고 있다. 이 학교의 졸업생들은 고도로 숙련된 정보참모들이다. 하지만, 세계 제2차대전 때 전쟁을 수행함에 있어 작전참모들이 정보장교들보다 더 유력하였다. 전쟁 지도층에게 정보활동은 덜 중요하다고 여겨졌기 때문이다.

세계 제2차대전 종전 직전에, 정보장교들은 그들이 전쟁에 패할 것을 알았고, 그들이 수집한 문서, 도구, 장치 및 기타 증거를 모두 파괴하였다. 그리고 전쟁 이후 이 정보장교들은 모습을 감추었다. 그러나 1980년대 이후 그들이 사망하기 전, 그들의 기억을 바탕으로 은닉한 정보에 대한 내용을 책으로 기술하였고 그것은 세상에 공개되었다.⁸⁾

8) 예) 참조: Sugita, Ichiji, War Leadership without Intelligence, Tokyo: Hara Shobo,

전쟁이 끝난 지 얼마 안 되어 몇몇 사람들은 정보활동을 재구성하려고 했다. 경찰청 관료 Jun Murai는 1952년도에 처음으로 조사실장으로 임명되었다. 1957년도에 이 조사실은 내각조사실(Cabinet Research Office)로 개명되었고, 1986년도에 내각정보조사실(Cabinet Intelligence Research Office[CIRO])로 재편성되었다. 정확히 규정되어 있는 것은 아니지만, 오늘날 일본의 정보기관은 경찰청, 외무성,公安조사청 및 방위성 등이 있다. 하지만 이 당시 일본 정보활동의 규모 및 범위는 현재보다 더 소규모였고 폭이 좁았다. 냉전 당시 미-일 안보조약에 의해 거의 모든 정보는 미국으로부터 왔으며, 일본은 영상정보(IMINT)능력이 없었고, 인간정보(HUMINT) 및 신호정보(SIGINT)에는 제한적 능력만 보유하고 있었다. 또한 일본은 오늘날까지 반-간첩법 및 비밀정보 사용허가가 없다. 세계 제2차대전 이후 新평화헌법으로 인해 소설 및 영화 외에 일본에서 간첩(스파이)은 더 이상 인기가 없었으며 이러한 정세는 탈냉전기의 변화를 초래하였다.

2. 일본의 정보활동 강화

1998년도에 북한은 대포동 미사일을 발사하였다. 미사일은 일본 영토 동북지역을 통해 태평양에 낙하하였다. 아직도 북한의 의도가 명확하지는 않지만, 미사일 발포로 하여금 북한이 일본의 국가안보에 얼마나 위협적인지 일본인들에게 명확한 인식을 심어주었다.

2001년에는 북한의 스파이 선박이 일본해역에 진입하였다. 일본 해양경비대는 그 선박을 붙잡으려 했지만, 총격전 이후 선박은 침몰하였다. 선박이 가라앉은 지역은 중국의 배타적 경제수역이었지만, 일본정부는 중국정부로부터 이 선박에 대한 구조 승인을 얻었다. 이 사건 이후 북한 공작원에 관한 기사가 다수 언급되었으며, 일본 내에서 북한에 대한 이미지는 더욱 나빠졌다.

사건 이후, 양측 정부는 정상회담을 갖기 위해 협상하였다. 세계 제2차대전 이후까

1987 (Japanese). Tsukamoto, Makoto, Record of a Intelligence Officer, Tokyo: Chuko Bunko, 1988 (Japanese). Hori, Eizo, Intelligence War Record of a Japanese Imperial Headquarter Staff, Tokyo: Bungei Shunju, 1996 (Japanese).

지도, 일본과 북한은 양국 간 외교관계가 수립되지 않았는데, 2002년도에 준이치로 고이즈미(Junichiro Koizumi) 총리와 김정일이 평양에서 만났다. 고이즈미 총리는 북한에 피랍된 일본인들을 송환하기 위해 교착상태였던 협상을 타개하려는 의도였다. 하지만 김정일은 고이즈미에게 그 중 8명이 사망하였고 5명이 살아있다고 전했으며, 이에 대해 고이즈미는 격분하였지만 회담 이후 공동성명에 서명하였고, 생존한 5명을 일본으로 데려갔다.⁹ 생존한 일본인 5명의 귀환은 일본에서 환대를 받았으며, 특히 북한정부가 이들을 납치한 사실을 인정한 것과 피랍인 다수가 사망하였다는 점, 그리고 아직도 더 많은 사람이 감금되어 있다는 사실은 일본인들의 심금을 울리게 하였다.

그 다음 해에 일본은 수년간 예측되어 왔던 정찰위성을 발사하였다. 이 정찰위성은 기상 및 자연재해 등 정보를 수집하기 위한 의도였지만, 사실상 일본정부가 직접 동아시아의 정세를 관찰하기 위한 것이었다. 일본은 오랜 기간 동안 미국정부 또는 상업위성에 의존해왔던 영상정보 능력을 확대하려고 했다. 이 위성은 미국위성에 비해 영상 해상도가 떨어지고 분석능력이 덜 숙련되었지만, 언제든지 원할 때 영상을 채집할 수 있는 능력은 동아시아의 정세 변화에 있어 결정적인 요소였다.

2004년에는 중국과 관련된 두 개의 사건이 있었다. 첫 번째로, 일본 영해에 중국 잠수함이 진입한 사건이었는데, 일본 해양경비대의 추격 이후, 잠수함은 중국 항구로 서둘러 복귀하였다. 이 잠수함의 진입 의도는 명확하지 않았고, 중국정부는 그 사건이 실수였다고 밝혔다. 이에 대해 중국해군이 일본 해안 및 섬 지역 보안에 대한 도전 및 시험을 하기 위한 것이라는 말도 있다.¹⁰

두 번째로, 상하이 주재 일본영사가 자살한 사례가 있다. 이것은 일반적인 미인계 사건으로, 결혼을 하고 아이를 둔 영사가 바(bar)에서 만난 중국여성과 관계를 가졌다. 이후 그는 중국요원에게 협박당했고, 영사관에서 그가 담당하고 있는 외교 비문을 가져올 것을 요구받았다. 그는 심적으로 괴로워하였으며, 결국 부인과 총영사에게 유서를 남기고 자살하였다. 2006년까지 공개되지 않은 이 사례는 동아시아 정세의 흑독

9) Yomiuri Shinbun, Man who Made Diplomacy a Fight, Tokyo: Shinchosha, 2005 (Japanese).

10) Raul Pedrozo, "Beijing's Coastal Real Estate," Foreign Affairs <<http://www.foreignaffairs.com/articles/67007/raul-pedrozo/beijings-coastal-real-estate>> Access on November 15, 2010.

한 면을 보여주며, 이와 같은 사례들은 일본 정보기관을 강화하자는 여론을 불러 일으켰고 이후 다수의 정책제안과 보고서가 발표되었다.

이러한 사례와 더불어, 2006년 9월 29일, 신조 아베(Shinjo Abe) 총리는 제165회 일본국회에서 정책연설을 하였다. 그는 “완강한 정치적 리더십 아래, 국가안보와 외교 전략에서 신속한 결정을 하기 위해서 총리실 본부기능이 재편성 및 강화될 것이며, 정보수집기능이 개선될 것이다.”¹¹라고 말하였다.

그 다음 해인 2007년 1월 26일에는 국민들에게 “완강한 정치적 리더십과 더불어 더 더욱 복잡해지고 있는 외교 및 국가안보 관련 사항에 즉각적인 대응을 가능케 하기 위해서, 본부로서의 총리실 기능강화를 위한 구조구축을 할 것이다. 또한, 내각의 정보능력을 강화시킬 것이다.”¹²라고 하였다.

추가적으로, 2007년 9월 10일, 아베 총리는 제168회 국회에서 “북한의 미사일 발사와 핵실험 성명의 영향을 아직 잊지 않았다. 우리 국가를 둘러싼 국가안보 환경이 아직 심각하다. 총리실의 지휘기능 및 정부의 정보기능 강화뿐만이 아닌, 국가안보 체계의 재편성이 필요하다.”고 연설하였다.

국회에서 총리가 세 번이나 정보활동 강화에 대해 연설한 것은 국민의 기대치를 높였지만, 아베 총리는 2007년 7월 총선에서 참패를 겪은 후 건강상의 이유로 사임하였다. 2009년 자민당에서 민주당으로의 정부 변화 이후, 아베 정부를 이어받은 야스오 후카다(Yasuo Fukuda) 총리, 아소 다로(Aso Taro) 총리 및 유키오 하토야마(Yukio Hatoyama) 총리 모두 정보 분야에 더 이상 관심이 없었고 일본 내에서 정보강화에 대한 기대는 점점 멀어져 갔다.

하지만, 증가하고 있는 사이버 안보 위협은 일본에서 정보개혁을 추진하는 동향이 되었다. 사이버 안보가 굳이 정보기관에서 다루어야 할 문제는 아니지만, 사이버 공격의 규모가 커지고 있고 국가안보에 미치는 영향이 더욱 심각해지는 만큼, 향후에 있을 공격을 방지하기 위해 정보기관을 개입시킬 필요가 점점 더 커지고 있다.

11) http://www.kantei.go.jp/foreign/abespeech/2006/09/29speech_e.html

12) http://www.kantei.go.jp/foreign/abespeech/2007/01/26speech_e.html

IV 동아시아의 사이버 위협 확산

1. 일본의 사이버 안보와 대응기관

2000년대 일본에서의 인터넷 사용 증가는 사이버 안보라는 새로운 위협의 부상과 발달을 초래하였다. 일본에서 사이버 위협에 첫 번째로 대응하는 정부기관은 경찰이다. 어떠한 사이버 공격이라도 범죄로 분류가 된다면, 경찰청은 범죄자를 붙잡고 기소할 것이다.

하지만, 만약 공격이 단순한 범죄를 넘어 국가안보 위협으로 여겨진다면 군사력이 대응할 것이다(일본의 경우 자위군). 일반적인 웹 사이트를 위조/변조하는 것도 범죄지만, 전산망이나 국가 운송체계 같은 주요 기반시설의 물리적 공격은 이와 다르다.

세 번째 대응기관은 정보기관이며 이들은 사이버 공격을 미연에 예측하고 방지한다. 핵 시설, 운송체계 또는 금융체계에 대한 공격은 돌이킬 수 없기 때문에 이러한 공격을 방지하기 위해 도청 등과 같은 정보활동이 필요하다.

일본의 경우, 앞에서 언급한 세 종류의 정부기관 및 조직이 서로 겹치며, 이들은 엄밀히 분류될 수가 없다. 경찰청 보안국은 법률 집행기관 내부의 강력한 정보당국이며, 방위성의 정보본부는 신호정보(SIGINT)의 정보당국이다. 그리고 내각정보조사실(CIRO)의 실장(Director)은 경찰청 출신 인사이며, 부실장(Deputy Director)은 외무성 출신 인사이다.

본 논문에서 중점적으로 논의하고 싶은 문제는 일본 정부기관이 일본 및 기타 국가를 상대로 한 대규모의 사이버 공격에 어떻게 대응하는 것인가이다. 일본정부가 과거에 겪었던 공격은 웹 사이트 위조 및 게시판 체계 등의 디도스(DDOS)와 같은 비교적 낮은 수준의 공격이었다. 하지만 2009년 7월 미국 및 대한민국에 가한 공격의 규모는 일본 정부의 지도자들을 놀라게 했다. 현재 일본 내 많은 정보관련 기관 중, 국가정보보호센터(National Intelligence Security Center : NISC)가 이러한 정세변화에 대응하여 주요한 역할을 수행한다.

2. 일상에서의 사이버 공격

사이버 공격 및 사이버 범죄의 범위는 더 넓다. 이들의 목표는 개인으로부터 세계적인 범위까지 이른다. 대체로, 사이버공격에는 크게 네 가지 종류가 있다: (1)물리적 피해(댐 붕괴 또는 비행기추락 등), (2)금융적 피해(은행계좌 비인가 접근 또는 불법 주식거래 등), (3)심리적 피해(웹 사이트 조작 또는 서비스중단 등) 및 (4)익명 피해(비밀 작전 같은 피해자도 공격 가해자가 누군지 모르는 공격 등)

〈그림 2〉는 일본에서 보고된 비인가 접근 수치의 추세를 보여주고 있다. 경찰청이 수집한 이 자료는 2001년도에 현저히 높은 수치를 보여주고 그 이후 동향은 안정적이었으나, 2005년도에 다시 증가하였다. 〈그림 3〉은 보고된 웹 사이트 조작 수치를 보여주고 있는데, 2009년 4분기에 대폭 증가한 것을 볼 수 있다. 〈그림 4〉는 웹 사이트 조작의 한 예이다.

정보 사회가 발전함에 따라, 사이버 안보문제는 일본뿐만 아니라 다른 국가에서도 이슈가 되고 있다. 〈표 1〉은 마이크로소프트 컴퓨터 안티-악성소프트웨어(anti-malware) 프로그램이 컴퓨터 시스템 청소를 한 상위 15개국의 목록이다.

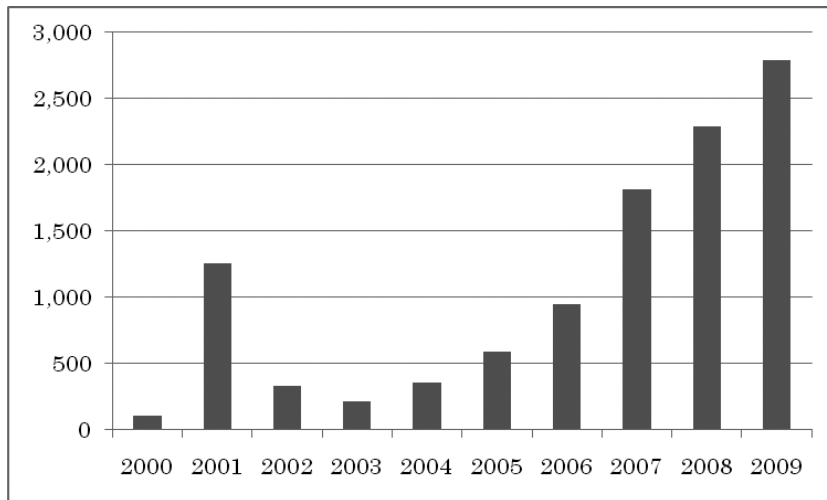


그림 2 : 비인가 접근 보고

출처 : 경찰청

52 일본의 사이버 보안과 정보활동 : 동아시아의 새로운 위협에 대한 대응

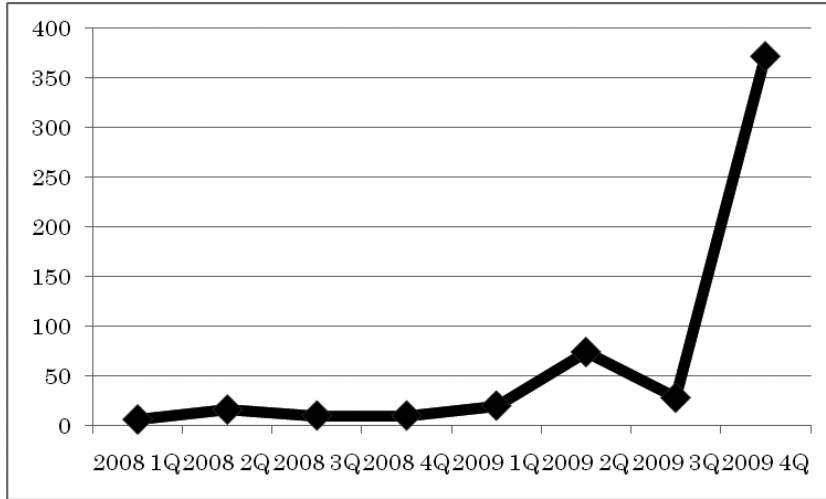


그림 3 : 웹사이트 조작 수치(2008년 1분기~2009년 4분기)

출처 : JPCERT/CC



그림 4 : 웹사이트 조작의 예

출처 : <http://truthjapan.blog118.fc2.com/>

표 1 : 2009년 2분기에 마이크로소프트 안티-악성소프트웨어 프로그램이 청소한 컴퓨터 수치 상위 15개국

순 위	국가/지역	청소된 컴퓨터 (’09년 2분기)	청소된 컴퓨터 (’09년 1분기)	변 화
1	미국	15,383,476	13,971,056	10.1%▲
2	중국	3,333,368	2,799,456	19.1%▲
3	브라질	2,496,674	2,156,259	15.8%▲
4	영국	2,016,132	2,043,431	-1.3%▼
5	스페인	1,650,440	1,853,234	-10.9%▼
6	프랑스	1,538,749	1,703,225	-9.7%▼
7	대한민국	1,367,266	1,619,135	-15.6%▼
8	독일	1,130,632	1,086,473	4.1%▲
9	캐나다	967,381	942,826	2.6%▲
10	이탈리아	954,617	1,192,867	-20.0%▼
11	멕시코	915,786	957,697	-4.4%▼
12	터키	857,463	1,161,133	-26.2%▼
13	러시아	677,601	581,601	16.5%▲
14	대만	628,202	781,214	-19.6%▼
15	일본	609,066	553,417	10.1%▲
	전 세계	41,024,375	39,328,515	4.3%▲

출처 : 마이크로소프트 보안정보 리포트 볼륨 8 [Microsoft Security Intelligence Report Volume 8] (2009년 7~12월) Key Findings Summary

대규모 사이버 공격의 예로서는 2007년 에스토니아, 2008년 리투아니아 및 그루지야가 있다. 이 3개국은 러시아로부터 공격을 받았다고 전해진다(굳이 러시아 정부가 개입되었다는 것을 의미하지는 않는다.). 2007년도에는 이스라엘이 시리아의 대공방어 네트워크를 침략, 무력화시킨 것으로 알려져 있는데, 이 당시 시리아 군은 레이더상에서 이스라엘의 전투기를 찾을 수가 없었다고 한다.¹³

13) Richard A. Clarke, and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, New York: ECCO, 2010, pp.1~11.

한편 캐나다 토론토대학의 연구원 Ronald Deibert 및 SecDev Group의 Rafal Rohozinski는 인터넷 IP패킷의 이상한 송신을 발견하였는데, 일반적인 바이러스는 감염 및 자체복사를 하지만, 그들이 발견한 악성 소프트웨어는 이러한 현상을 보이지 않았다. 이 악성 소프트웨어는 대상컴퓨터에 몰래 침입하여 리모컨에 의해 조작되며 컴퓨터 소유자도 모르는 사이 다른 곳으로 파일을 전송한다.

두 연구원들은 이 악성 소프트웨어의 왕래를 분석하였는데 103개국의 1,295개의 컴퓨터가 감염된 것을 발견하였고, 그 중 30%는 고가치 표적이었다. 또한 왕래를 분석한 결과 이것이 중국으로 향하고 있는 것을 발견하였다. 두 분석가는 이 악성 소프트웨어를 “유령 네트워크(Ghost Net)”라고 불렀다. 그들의 분석은 이 악성 소프트웨어가 자금절도, 갈취, 사생활 침해 같은 일반적 사이버 범죄가 아니라는 것을 보여준다. 하지만, 그들은 도중에 연구를 중단해야 했는데, 추가적인 연구 및 분석을 합법적으로 진행할 수 없었기 때문이다. 유령 네트워크는 국경선을 넘어섰으며, 이것은 법적 관할권에 대한 문제를 제기하였다. 캐나다에서는 합법일지 몰라도, 중국에서는 그렇지 아닐 수도 있다. 이후 그들은 유령 네트워크에 대한 리포트를 작성하여 2009년 3월에 인터넷에 공개하였고,¹⁴ 그들의 경고는 사이버 공간에서 널리 퍼졌다.

그들이 이 악성 소프트웨어를 “유령 네트워크(Ghost Net)”라고 부른 이유는 누가 악성 소프트웨어 네트워크를 운용하는지 확실하지 않기 때문이었다. 사이버 보안이 중요하다고 말하는 것은 쉽지만, 실제로 이 중요성을 느끼기는 어렵다. 하지만 실제로 방대한 규모의 공격이 태평양 동-서 지역에서 이루어졌다.

3. 2009년 7월 미국 및 대한민국을 겨냥한 사이버공격

2009년 7월, 미국 독립기념일 직후, 정체를 알 수 없는 누군가가 미국의 정부 및 상업용 인터넷 사이트에 디도스(Distributed Denial of Service : DDOS) 공격을 감행하였다. 백악관, 국무부, 법무부, 국방부, 야후, 아마존을 포함한 20개 이상의 인터넷 사이트가 표적대상이 되었다.

14) Information Warfare Monitor, Tracking GhostNet : Investigating a Cyber Espionage Network, March 29, 2009 <<http://www.infowar-monitor.net/research/>>.

또한 7월 7일부터 9일까지, 대한민국 국방부, 국회, 국가정보원, 유명 경매 사이트, 금융 분야의 인터넷 사이트가 같은 공격을 받았다. 주요 공격은 7일 18시, 8일 18시, 9일 저녁에 줄줄이 이어졌으며, 감염된 컴퓨터는 한반도 및 기타 18개국에까지 퍼졌다. 한국의 총리실장은 T/F회의에서, “이것은 우리 국가체계에 대한 공격이며, 국가 안보를 겨냥한 행위 또는 도발이다.”라고 말했다. 추후 분석에 따르면 두 나라에 대한 공격은 동일한 프로그램에 의해 이루어진 것이라고 한다.

최초에, 한국 국가정보원은 국회의원들에게 북한의 개입가능성을 언급하였지만 확실한 증거가 없었다. 이후 한국 정부는 북한 정부가 한국 커뮤니케이션 체계를 분열시키기 위해 컴퓨터 프로그램을 발전시키라는 명령을 내렸다는 정보를 입수했다. 2주 후에는 한국정보보호진흥원(Korea Information Security Agency : KISA) 및 부산 소재 한 대학교를 겨냥한 시뮬레이션 테스트 조짐을 입수하였다. 이러한 정보 하나 하나는 북한의 개입을 의심케 하는 생각으로 이루어졌다. 하지만, 대다수의 인터넷 사용자는 공격 도중 심각한 문제를 찾지 못했고 단지 연결 상태가 느릴 뿐이라고 느꼈다. 감염된 컴퓨터는 기능을 잃었지만, 심각한 피해는 보고되지 않았다.

두 국가를 겨냥한 디도스 공격 이후, 한국정부는 일본정부에 일본에 위치한 컴퓨터 서버 8개에 대한 조사를 의뢰했다. 이 서버들은 사이버 공격의 발판(stepping stone)으로 여겨졌다.¹⁵ 발판은 실제 공격 가해자의 흔적을 감추는 수단이다. 그러나 이 8개의 서버는 개인소유였고 서버의 소유자조차 어떻게 본인들의 서버가 공격에 사용되었는지 알 수 없었다.

8개 서버 중 3개는 고정 IP주소가 있었기 때문에 확인이 되었고, 특정 프로그램 및 공격의 루트가 발견되었다. 그러나 다른 5개 서버는 상업 인터넷 서비스 제공자들에 의해 사용되었고 다양한 IP주소가 할당되어 있었다. 이것들을 확인하는 것이 커뮤니케이션 보안성에 반대되기 때문에, 5개 서버는 아직 알려지지 않았다.

3개 서버에서 발견된 프로그램은 동일하였다. 하지만, 감염된 루트를 찾아내는 것은 불가능하였다. 프로그램에서 표적을 겨냥하는 암호가 발견되었고, 리스트에 있는 표적만 공격을 당했다. 하지만 프로그램이 완전히 분석될 수는 없었다. 누가 실제 공격의 가해자이고 어디에 위치해 있는 것에 대한 정보는 없었다. 또한 북한의 개입도

15) 2010년 7월 2일 경찰청 인터뷰.

증명되지 않았다. 북한은 그들의 고유 IP주소가 없었고 중국에서 IP주소를 빌려왔다. 공격에 사용된 IP주소는 중국 소유라는 말도 있다.

일본의 동맹국인 미국과 우방국인 한국이 공격을 당했다는 사실은 일본 지도층을 놀라게 하였다. 아래에서는 그들이 이에 대해 어떻게 대응하였는지 살펴보고, 경찰청, 방위성 및 국가정보보안센터(NISC)의 역할을 살펴보겠다.

V 일본 정부의 대응

1. 경찰청

2009년 7월에 행해진 공격은 경찰청의 긴장을 고조시켰다. 우방국에 행해진 공격은 일본 정부에 사이버 공격이 실질적이고 직접적인 위협이라는 것을 인식시켰다. 경찰청은 미래에 있을 공격에 대비하기 위한 계획을 수립하기 시작했고, 2009년 7월 공격은 참조하

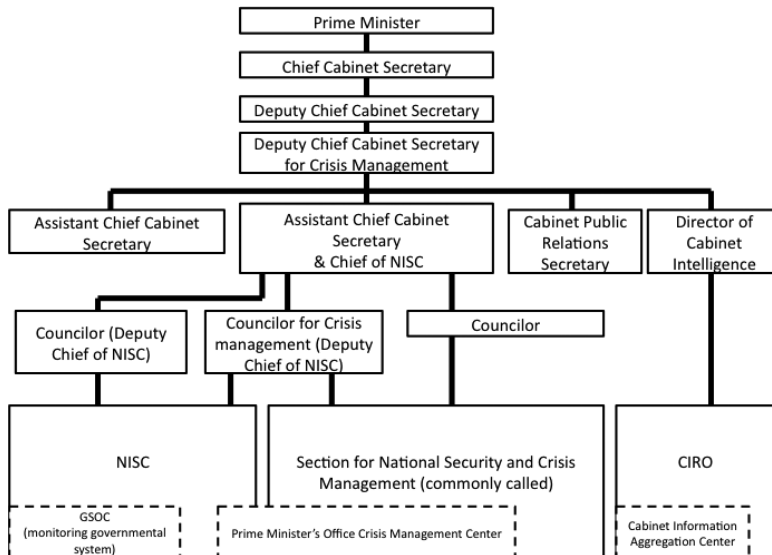


그림 5 : 사이버보안 위기관리구조

출처 : 경찰청

기 좋은 사례가 되었다. 2010년 3월 9일, 일본 정부는 사이버 문제를 다루기 위해 새로운 구조를 편성하였다(그림 5). 이 구조에서 사이버 공격은 지진이나 화산폭발 등 자연재해와 같은 수준의 위기로 간주되며, 공격이 시작되면 위기관리 메커니즘이 작동할 것이다.

추가적으로, 경찰청은 전국 150곳에 인터넷 통신 24시간 감시체제를 유지하고 있다. 또한 경찰청은 주요기반시설 운용기관 600여 곳과 접촉하고 있으며, 의심스러운 행동이 발견되면, 그들은 경찰청에 연락한다. 운용기관은 보안정책을 수립하고, 야간 대응체제를 갖추고 있다.

이러한 구조변화는 당시 관방장관이었던 Mr. Hirofumi Hirano가 이끌었다. 2009년 7월 사이버 공격 이후, Mr. Hirano는 그의 참모들에게 만일 일본이 이러한 공격을 당하면 어떻게 대응할 것인지 물으면서, 미래에 있을 공격에 대비할 것을 지시하였다. 사실 2008년 봄부터 사이버 공격에 대비하자는 논의가 있었지만, 실질적인 준비는 그의 지시 직후 시작되었다.

경찰청은 2009년 7월 공격을 공식적으로 평가하지는 않았다. 담당관들은 공격이 피해를 입히는 것보다는 시위 목적이라고 간주했지만, 공격이 시위적 목적이라고 보기에는 너무 길었다. 디도스 공격은 공격당한 서버에서 어떠한 자료도 가져가지 않고 공격 가해자의 실제 의도를 파악하기가 어렵다.

2. 방위성

일본 방위성은 2009년 7월 사이버 공격에 대한 일본 내 영향은 적었다고 생각했는데, 자위군(Self Defense Force)을 포함하는 방위성의 체계는 인터넷으로부터 독립적이었기 때문이다.¹⁶ 2010년 5월 “국가 보호를 위한 정보보안전략(Information Security Strategy for Protecting the Nation)”이 공표되기 전까지 방위성은 사이버 안보를 단순한 컴퓨터시스템 수준이라고 인식하고 있었으며¹⁷ 이후, 방위성은 사이버 안보를 국가안보 수준으로 고려해야 한다는 생각을 하기 시작했다.

16) 2010년 10월 4일 방위성 인터뷰.

17) NISC, Information Security Strategy for Protecting the Nation, May 2010, available at <http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf>.

이는 일본의 자위대는 법적 제한으로 인해 해외파병을 하지 않기 때문에 일본 방위성의 주요 목표가 일본 영토 내 지휘통제 체계를 보호하는 데 있기 때문이기도 하다.

한편 2009년 당시 미국 국방부 부장관이었던 William J. Lynn은 외교논설에서, 일본 방위성은 외부 위협으로부터 충분한 준비를 하고 있지만, 내부 위협의 대응에 있어서는 아직 많은 문제가 있다고 하였다.¹⁸ 단적인 예를 들면 방위성 내 컴퓨터 시스템 사용은 엄격하게 제한되지만, USB 메모리와 같은 장치는 쉽고 별다른 제한 없이 이용된다. 따라서 이러한 약의에 찬 계획을 완벽히 차단하는 것은 어렵고 비밀정보가 이러한 장비를 통해 유출될 수 있으며, 바이러스나 악성 프로그램이 시스템 내부에 침입할 수도 있다.

긴급 상황 발생 시, 경찰청 및 방위성은 상황에 대응하기 위해 서로 협력하는 구조로 이루어져 있다(그림 6). 또한 국가정보보안센터(NISC)를 관리하고 일부 업무를 수행하기 위해 방위성에서 자위군 관료를 NISC에 지원하기도 한다.

방위성은 경찰청과 같은 감시체계가 없기 때문에 방위성은 방위성을 겨냥한 공격만 탐지할 수 있고, 일본 정부를 겨냥하는 공격의 큰 그림을 얻을 수가 없다. 그러므로 방위성은 NISC를 통해서 정보를 얻어야 한다. 또한, 방위성은 사이버 공격을 분석하지 않고 총무성 및 경제산업성이 운영하는 사이버클린센터(Cyber Clean Center : CCC)가 이를 담당한다.

달리 설명할 필요 없이, 몇몇 사이버 공격은 안티바이러스 소프트웨어로 다룰 수 없으며, 매일 다양한 스팸 메시지 및 포트스캔 접속(port-scanning access)이 존재한다. 2010년 가을 센카쿠 분쟁(Senkaku Islands dispute)이후, 일본 정부의 웹사이트 접근 수치가 미묘한 증가가 있었지만 심각한 영향은 없었다.

그러나 방위성 입장에서는 누가 공격하는지는 주요 관심대상이 아니다. 자국 방위 측면에서, 자위군은 어떠한 적으로부터도 국가를 보호해야 하며, 공격 가해자를 파악하고 잡는 것은 방위성의 역할 범위에서 벗어난다. 그들의 최우선 사항은 국가를 “보호”하는 것이다.

한편 방위성은 미국 오바마 정부가 수립한 USCYBERCOM(미국사이버사령부)에

18) William J. Lynn, III, “Defending a New Domain: The Pentagon's Cyberstrategy,” *Foreign Affairs*, vol. 89, no. 5, September/October 2010, pp.97~108.

관심을 보이고 있으며, 자위군 산하에 이와 비슷한 조직을 보유하려는 움직임을 보일 수도 있다. 국가를 보호하기 위해서 방위성과 자위군은 그들의 커뮤니케이션 체계를 첫 번째로 보호해야 하기 때문이다. 이를 위해 방위성은 지난 2010년, 2011년 3월까지 “사이버 공간 방위대”를 설립할 것이라고 밝히기도 했다.¹⁹

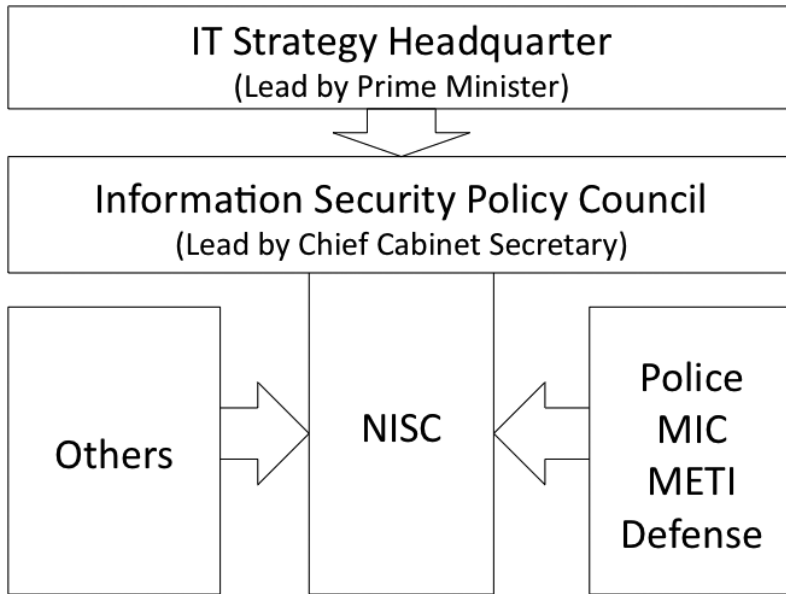


그림 6 : 일본 국가정보안보 조직

출처 : 내각부

3. 국가정보보안센터(NISC)

인터넷의 인기가 2000년대 들어 증가하면서, 사이버 보안방법이 주요 정책이슈가 되었다. 이에 따라 2000년 2월, 내각부 산하 정보안보부문(Information Security Section)이 창설되었으며 이는 2005년 4월에 국가정보보안센터(NISC)로 발전하였다. 동년 5월에는, 국가정보보안의회(National Information Security Council)가 설립되기도 했다. 이러한 동향의 배경에는, “선진 정보안보국가”의 인식, 즉 정보 및

19) 방위성, “Japan's Defense and its Budget”, 방위성, 2010, p.8.

커뮤니케이션 기술의 안전한 환경에 대한 인식이 일본 경제 및 일본 국가의 고복지 발전에 필수적인 것으로 여겨졌기 때문이다. NISC는 국가정보보안회의의 사무국 역할을 하며, 다양한 전략, 계획 및 목표를 발전시키고 있다. 또한 공-사 공통정보(또는 사이버) 보안정책을 협조하도록 되어 있다.

국가정보보안회의는 2005년 3월 30일 IT전략본부장, 즉 일본 총리에 의해 창설되었다. 관방장관이 의회에서 의장역할을 하고 부의장은 과학기술 정책장관이 담당한다. 의회 의원들은 국가공안위원장, 총무성장관, 산업경제성장관, 방위성장관을 포함한다. 또한 민간부문에서 6명의 전문가가 의회에 가입되어 있다.²⁰

의회는 2006년 2월 2일, “정보보안에 대한 첫 번째 국가전략 : 신뢰할 수 있는 사회창출을 향하여(First National Strategy on Information Security : Toward the Creation of a Trustworthy Society)”를 내놓았다.²¹ 이는 향후 3년간을 대상으로 하며, 매년 새로운 계획을 발표하도록 되어 있다. 그리고 2009년 2월 3일에는, “정보보안에 대한 두 번째 국가전략 : IT시대의 강력한 ‘개인’ 및 ‘사회’를 향하여(Second National Strategy on Information Security : Aiming for Strong ‘Individual’ and ‘Society’ in IT Age)”를 발간하였다.

2009년 7월 두 번째 국가전략의 발표 이후, 미국 및 한국을 겨냥한 대규모 사이버 공격이 이루어졌다. 한편 2009년 8월, 장기간 집권했던 자민당(Liberal Democratic Party : LDP)이 대선에서 패했으며, 일본민주당(Democratic Party of Japan : DPJ)이 연합정권을 만들었다. 그리고 의회와 국가정보보안센터(NISC)는 사전 정책을 개정하기 시작하였고, 2010년 5월 11일 “국가보호를 위한 정보보안전략”을 내놓았다. 본 전략은 2010년부터 2013년까지를 대상기간으로 하며, 2009년 발표한 두 번째 국가전략을 포함한다. 또한 매년 계획을 만들 것을 명하였는데, 본 전략의 첫 번째 페이지는 다음과 같다.

정보보안에 관한 두 번째 국가전략이 결의된 이후, 2009년 7월 미국과 한국에 대규모 사이버 공격이 이루어졌다. 또한, 대규모 개인정보 유출 사례가 잇따라 발생했다.

미국과 한국에 대한 대규모 사이버 공격은 특히 경제활동 및 사회생활에

20) 저자는 의회 전문의원임.

21) http://www.nisc.go.jp/active/kihon/pdf/bpc01_ts.pdf

서 정보 및 커뮤니케이션 기술에 점점 의존하고 있는 일본에 경각심을 일으켰다. 정보보안의 위협이 곧 국가안보의 위협이 될 수 있다는 것과 이에 대한 효과적인 위기관리가 요구된다는 것을 말이다.²²

이것은 미국과 한국에 대한 사이버 공격이 일본의 사이버 안보정책 개정에 중요한 역할을 하였다는 것을 의미한다.

앞서 언급한 일본의 국가 전략에는 3가지 기본 원칙이 있다. 첫째 정책 강화 및 대책 개선, 둘째 새롭게 변화하는 환경에 적합한 정보보안 정책 구축, 그리고 셋째는 수동적 정보보안 방책에서 능동적 정보보안 방책으로의 변화이다. 첫 번째 및 두 번째로 발표한 국가전략에서 사이버 공격이 등한시되거나 덜 심각하게 여겨졌다고 말하는 것은 긍정하지 못하지만 국가전략에서 사이버 공격이 대두되었다는 점은 주목할 만하다.

그러나 일본 민주당 정책의제에서 사이버 안보는 높은 비중을 차지하지는 않았다. 2009년 8월 민주당이 정권을 잡은 후 9개월 동안 국가정보보안의회가 열리지 않았다. 그리고 얼마 지나지 않아, 민주당은 자민당 정권 때 창설된 장관급 회의는 검토거나 통합, 또는 폐지되어야 한다고 발표하였으며, 정부 업무를 검토하는 과정에서 다양한 종류의 예산이 삭감되거나 절감되었다. NISC의 활동 또한 영향을 받을 것이라 생각했다.²³ 하지만 새 정부가 재고하려 했던 의회 및 NISC의 존재가, 넘쳐나는 다른 정책의제에 묻힌 것 또한 사실이다. 총리, 관방장관 및 기타 장관들은 다른 문제에 집중하기에 너무 바빴다.

국가전략 발표 후 약 한달 뒤, 유키오 하토야마(Yukio Hatoyama)총리가 사임하였고, 민주당 대표 나오토 간(Naoto Kan)이 정부를 이어 받았다. 그리고 새 내각 출범 후 처음으로, 2010년 7월 22일 국가정보보안의회 회의가 열렸다. 또한 “정보안보 2010”이라는 연례 계획이 허가되었다. 이 계획의 첫 번째 항목은 “대규모 사이버 공격사태 대책 개선”이었고, 총 19개의 정책항목이 기재되었다.

22) NISC, Information Security Strategy for Protecting the Nation, May 2010, available at <http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf>.

23) 실제로 2009년 11월까지 장관급 회의 18개가 폐지됨.

http://www.kantei.go.jp/jp/tyoukanpress/rireki/2009/11/17am_siryoun.pdf

VI 동아시아의 변화

1. 중 국

동아시아는 사이버 공격을 포함한 사이버 활동 측면에서 볼 때, 세계에서 가장 활동이 활발한 지역이다. 인터넷 사용자는 세계에서 인구수가 가장 많은 중국과 인도로 인해 급격하게 늘어나고 있다. 그리고 이 지역 내 사이버 안보에 가장 열기를 띠는 곳은 중국과 한국이다. 역사적 분쟁으로 인하여 일본은 종종 중국과 한국의 사이버 공격대상이 된다. 그리고 오늘날 정책체계와 양국을 둘러싼 국제정세는 동아시아 사이버안보에 영향을 끼치고 있다.

사이버 공간에서 중국의 존재는 점점 더 커지고 있다. 2010년 3월을 기준으로 전세계 인터넷 인구가 약 16억 명으로 추정되고, 그 중 중국이 4억 명 이상으로 4분의 1을 차지한다. 하지만 인터넷의 중국 인구 내 시장 침투율은 아직 30%이다. 만일 이 수치가 선진국 수준까지 올라간다면, 중국의 존재는 매우 압도적일 것이다.

하지만 중국은 온라인상에서 다른 국가를 공격하는 것으로 악명 높다. 2007년 타임즈는 중국이 2050년까지 세계적 경쟁 국가들(특히 미국, 영국, 러시아, 한국)을 상대로 “전자적 지배”를 시도하려고 한다는 글을 실었다. 본 글에 의하면, 2005년도에 미국 국방부에 대해 79,000건의 사이버 침입 시도 사례가 있었다고 한다. 그 중, 미국 육군 101 및 82 공수부대, 제4보병사단에 연결된 컴퓨터 침입사례를 포함한 1,300건이 대표적인 공격사례로 평가된다.²⁴

2010년 1월에는 대규모 검색엔진인 구글이 중국 정부와 논쟁을 시작하였다. 구글은 중국이 요구하는 검열제도를 더 이상 따르지 못하겠다고 하였고, 무료 이메일 서비스인 G-mail이 중국으로부터 공격을 받고 있다고 주장하였다. 미국 정부의 도움

24) Tim Reid, “China’s Cyber Army is Preparing to March on America, says Pentagon,” Times Online, September 8, 2007 <http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2409865.ece> (access on May 9, 2010).

으로 구글은 중국 정부의 정책을 바꾸려 시도하였지만, 결국 구글은 중국시장에서 철수하였고 홍콩 구글 사이트로 그들의 검색엔진을 변경하기 위한 서비스 라이선스를 얻었다.

이러한 중국의 사이버 공격에 관한 뉴스는 미디어를 통해 널리 퍼졌다. 하지만 중국은 중국 정부, 중국 공산당 및 인민해방군은 어떠한 사이버 공격에도 개입되어 있지 않다고 주장하였고, 오히려 중국이 외부세력에 의해 지속적으로 공격을 받고 있다고 하였다. 2009년 Norton Online Living Report는 중국 인터넷 사용자 중 53%가 그들의 컴퓨터에 사이버 침해를 경험한 적이 있다고 밝혔는데 이것은 조사된 국가들 중 가장 높은 수치이다.

중국 정부는 그들이 검열시스템 또는 “사이버 만리장성”을 도입한다는 것에 대해 인정한다. 이 시스템은 20세기 재래식 검열방식과는 사뭇 다르다. 인터넷의 모든 왕도를 감시하는 것은 당연히 불가능하며, 데이터 규모는 폭발하고 있다. 컴퓨터 프로그램이 검열절차를 대부분 만들어놓고 인간은 정책적 결정만 할 뿐이다. 여기에는 아주 복잡한 “벽 쌓는(walling)” 기술이 중국 인터넷 시스템에 도입되었다.

중국에서는 뉴욕타임즈, 워싱턴포스트, CNN 및 기타 뉴스매체를 접하기가 어려웠다. 때때로 이러한 매체들이 중국 정책을 비난하는 글을 올리기 때문이다. 하지만 중국 외부 인권단체가 프록시 서버를 통해 검열을 변경하면서 중국 정부는 규정을 해제하였다. 트위터, 유튜브 및 페이스북 같은 몇몇 온라인 소셜서비스는 아직도 차단되어 있지만, 이러한 서비스는 중국 외부에서 굉장히 인기가 높고 중국에서도 인기가 있을 수도 있다. 다수의 중국 인터넷 사용자들이 다른 방법을 통해 트위터를 사용하고 있다. 사회주의 국가가 사회미디어를 차단한다는 것이 큰 모순이다. 중국 내에서는 구글 뿐만 아니라 기타 검색엔진도 검색 키워드의 블랙리스트를 따르고 있으며, 키워드 검색의 결과는 중국과 다른 나라에서 각기 다르다.

중국정부가 인터넷에 대한 강력한 통제를 유지하는 가운데, 중국에서 많은 사이버 범죄 및 공격이 이루어진다는 것은 이상하다. 중국에서는 인터넷 연결서비스 제공자와 콘텐츠서비스 제공자 모두 등록되어 있어야 하고 제공자는 그들의 고객을 면밀히 감시한다. 그리고 중국 시민들은 인터넷 카페를 사용할 때, 사용자는 그들의 ID를 등록해야만 한다. 모든 국제 관문이 정부의 통제를 받기 때문에, 중국 정부는 국제 인터넷통신을 통제한다. 만약 정부가 정말 엄격하다면, “불법” 또는 의심되는 인터넷 통신

을 차단할 수 있다. 바로 이러한 점이 중국 외부 사람들로 하여금 중국 정부가 외국을 겨냥한 사이버 공격에 개입하고 있다고 믿게 하는 것이다.

2. 한 국

한국은 대량 판매시장에서 세계 최초 광대역망 채택국이었다. 한국은 1998년도에 심각한 아시아 경제/금융위기를 맞았는데, 경제적 불황을 극복하기 위해 당시 김대중 대통령은 1999년도에 “21세기 사이버코리아(Cyber Korea 21)”를 제안하였고, 디지털시대에 맞는 새로운 정책 및 경제적 동향에 걸맞은 국가로 만들기 위해 야심찬 기술 및 정책을 도입하였다. 주요 기술로는 반도체, 인터넷 광대역망 접속을 위한 ADSL(Asymmetric Digital Subscriber Line), CDMA(Code Division Multiple Access) 핸드폰기술 등이 있다. 일본 디지털 업체들이 국내시장에 묶여있는 동안, 한국의 삼성 및 기타 디지털 장비업체들은 세계적으로 퍼져나갔다.

한국이 광대역망 채택에 선진화된 것에는 다양한 이유가 있다. 그 중 하나는 한국 전체인구의 1/5이 서울에 살고 있으며, 그 중 대다수가 아파트에 살고 있다는 점이다. 광범위한 지역에 광대역망 기술을 설치하는 것은 비용이 많이 들지만, 한국의 인구는 서울 및 몇몇 도시에 집중되어 있다. 그리고 한국 국민들은 일자리를 얻고, 자녀 교육, 저렴한 물건 구매 등의 목적으로 더 빠른 속도를 얻기 위해 경쟁하였는데 이것 또한 이유 중의 하나였다.

성공적인 광대역망 보급은 한국인들로 하여금 그들의 새로운 사이버 문화를 자랑스럽게 하였다. 사이버 문화는 삶의 중요한 일부분이었지만, 동시에 ID 도용범죄 같은 사이버 보안의 새로운 위협이 부상했다.

한국의 모든 인터넷 사이트는 사용자들에게 그들의 주민등록번호를 등록할 것을 요구하였다. 이 숫자 시스템은 서비스 제공자들이 고객을 파악하는 데에 이해를 도왔지만, 동시에 ID 도용범죄는 사회의 심각한 문제가 되었다. 금융사기, 위장 도용, 사생활 침해, 기타 범죄 및 공격이 이루어졌으며, 컴퓨터 바이러스 및 스팸 메일은 더욱 악화되었다.

2002년 4월 발표된, 한국정부의 세 번째 정보 및 커뮤니케이션 기술(ICT) 계획 “e-

Korea Vision 2006”에는 공/사 파트너십에 의한 사이버 안보 기반시설 발전이 필요하다는 사이버 안보 관련 내용이 있다. 당시 한국의 정보통신부는 2002년 7월 “Secure e-Korea 2002~2007”을 발간하였다. 하지만, 2003년 1월 25일, 슬래머웜(Slammer worm) 바이러스가 한국 핵심 인터넷 서버에 심각한 피해를 입히기 시작했다. 인터넷 서비스가 강제로 몇 시간 동안 폐쇄되었으며, 이 사건은 “1·25 인터넷 대란(Big Confusion)”이라고 불린다. 이 사건 이후 한국 정부는 2004년 “국가 정보보안 기본지침”을 발행했다.

2008년 이명박 대통령은 정보통신부를 재편성하고 기능을 행정안전부, 문화체육관광부 및 지식경제부로 이전하였다. 또한 현재 방송통신위원회가 정보통신 산업을 관장한다. 하지만, 사이버 안보의 국가안보적 측면은 국가정보원에서 관리되고 있다. 국가정보원 산하, 국가사이버안전센터(National Cyber Security Center : NCSC)가 주요 정책결정 기관이다. 정부 외에 정보통신윤리위원회(Korea Internet Safety Commission : KISC)가 컴퓨터 보안사고 대응팀(Computer Security Incident Response Team : CSIRT)으로 편성되어 있으며, 한국인터넷진흥원(Korean Information Security Agency : KISA)이 정부 및 민간부문의 징검다리 역할을 한다.

2009년 7월 미국과 한국을 겨냥한 대규모 사이버 공격은 한국에 매우 큰 충격이었다. 한국은 북한이 어떤 종류든지 위협의 원천이 될 수 있고 북한이 사이버 공격을 감행할 것이라는 것을 쉽게 예측할 수 있었기 때문에 이러한 공격에 준비가 되어 있었지만 큰 피해를 입었다. 한국의 한 기사는 “한국은 인터넷 선진국으로서의 위상이 있었고 IT관련 기술 수출로 경제를 뒷받침한다. 그러나 이번 공격의 가장 큰 피해는 한국의 이와 같은 이미지에 손해를 입었다는 것이다.”라고 하였다.

아직도 우리는 누가 이 공격을 감행했는지 모르지만, 한국 정부는 북한 및 기타 세력의 공격으로부터 사이버 공간을 방어하는 데에 더욱 진지하게 대처했다. 예를 들어, 2010년 2월, 한국정부는 유엔(United Nations)산하 국제 사이버 안보 조직을 창설하여 서울에 위치하는 것을 제안하였다. 아직 합의가 이루어지지 않았지만, 한국 정부는 왜 사이버 기반시설을 보호해야만 하는지 잘 인지하고 있다.

VII 결론

냉전 이후 동아시아 정세변화에 대응하기 위해서, 국가 안보의 위협요소를 제거하기 위한 정보 활동범위 확대는 일본의 중요한 정책 의제이다. 최근 몇 년간 일본에 대한 사이버 공격 가능성의 증가는 정보기관에 새로운 역할을 위임하였다. 여태까지, 일본을 상대로 한 성공적인 대규모 사이버 공격사례는 없었다. 그러나 두말 할 필요 없이, 미래에 공격이 없을 것이라는 보장은 없다.

정보의 목적은 이러한 위협의 실마리 및 조짐을 사전에 파악하는 것에 있고, 이때 우리는 정보가 실용적이라고 평가할 수 있다. 그리고 정보의 실패는 우리에게 큰 손실 및 피해를 불러온다. 따라서 이와 같은 공격을 멈추게 하는 것뿐만 아니라 더 나은 방법으로 대응하기 위한 고려가 필요하다.

2009년 7월의 사이버 공격은 일본의 사이버 안보대책을 한 걸음 진전시킨 계기가 되었다. 비록 정권교체가 큰 요소지만, 제2차 정보보안 기본계획(the Second Information Security Basic Plan)이 2009년 7월 사이버 공격 이후에도 현재까지 여전히 유효하며, 중복해서 언급되었다는 점은 주목할 만하다.

국가정보보안센터(NISC)는 일본 정보사회 내에 위치해 있지는 않지만, 공동체 및 일본 지도층의 더 나은 접근을 위해 도움을 제공해야 한다. NISC의 역할은 사이버 안보 준비태세에 핵심적이다. 따라서 우리는 국가안보 환경에 대한 NISC의 역할을 조금 더 명확히 규정지를 필요가 있다.

일본 사회 내 정보범위 확대는 사생활 및 기본인권에 관한 우려사항을 제고시킬 수 있다. 예를 들어 현재 일본에서는 불법이지만, 사이버 테러리즘을 방지하기 위해 커뮤니케이션을 도청하는 집행권이 필요할 수도 있다. 국가정보보안의회 및 NISC는 지속적으로 전략을 내고 있지만, 이것을 실현시키기 위한 구체적 정책이 필요하다. 그리고 무엇보다 의회, NISC, 기타 관련 기관 및 민간부문이 국가를 보호하고 더 나은 준비태세를 갖추기 위해 총리 및 내각의 정치적 의지가 필요하다.

Cybersecurity and Intelligence Activities in Japan: Responses to Rising Threats in East Asia¹

Motohiro TSUCHIYA || Professor Keio University

목 차

- I . Introduction
- II . Cybersecurity and Intelligence
- III . Japanese Intelligence Agencies and Changes in
the Situation in East Asia
- IV . Widening Cyber Threats in East Asia
- V . Responses by Japanese Government
- VI . Changes in East Asia
- VII . Conclusion

1) Modified version of this paper is published in the edited book: Motohiro Tsuchiya, “Cyber security in East Asia: Japan and the 2009 Attacks on South Korea and the United States,” in Kim Andreasson, ed., *Cybersecurity: Public Sector Threats and Responses*, Boca Raton, FL: CRC Press, 2012, pp.55~76.

I Introduction

Cybersecurity is a new and non-traditional security concern in many countries today. It is not an exception in East Asia too. Many facilities and assets of governments, private companies and individuals are being attacked in a wave-like fashion. In July 2009, soon after the U.S. Independence Day holidays, large-scale DDOS (Distributed Denial of Service) attacks targeted American and South Korean Internet services. We cannot still confirm who were the real attackers behind overtaken computers, but these attacks made the governments to realize the importance to defend their countries from anonymous warriors or terrorists who were hiding themselves in Internet clouds.

This paper aims to analyze how the Japanese government responded to the July 2009 attacks in the U.S. and South Korea. Our interests are especially in the cooperation and competition between intelligence and law enforcement agencies. These two types of agencies are not well divided inside the Japanese intelligence community. Although the revival of intelligence agencies such as Cabinet Intelligence Research Office (CIRO) after the Japanese defeat in the World War II was relatively quick, the National Police Agency has been more powerful both in intelligence and law enforcement activities than any other security-related agencies. That is, there has been no clear wall between law enforcement and intelligence activities in terms of organizational functions. However, new cyber threats are forcing changes in the governmental system, because they are too complicated and elusive to respond under the existing organizations.

National Information Security Center (NISC), established in 2005, is a key

player in this new environment. It is an inside agency under the Cabinet Office of Prime Minister. It used to focus on technical measures for cyber security, but it is quickly acquiring national security perspectives after the July 2009 attacks. If NISC were to be a cross point of intelligence and law enforcement, this cooperation system between law enforcement and intelligence agencies could be a first step to reorganize Japanese intelligence system to prepare for future cyber and other types of threats. In this paper we analyze public documents and records and do interviews with concerned parties to shed light on better directions and arrangements for cyber security.

II Cybersecurity and Intelligence

Security in cyberspace is a good example of changes in the Post-Cold War era. Warfare is moving from physical territories to networks. Land, sea, air and outer space, where military forces have fought battles, are natural space. However, cyberspace is an artificial space, which computers, optic fibers, and other devices are constructing. Nowadays command controls of military forces are dependent on information and communication networks. A modern digitalized military force cannot fight anymore without them.

There is no need to invent a battle space intentionally. Computer games are enough. However, as the world is getting dependent on information and communication networks, and as information society emerges, our consciousness is going into cyberspace more than real world space and territories. Unless we cut convenient cables of computers and networks, there can be new threats and we need security to protect them.

There are various kinds of criminal activities in cyberspace, and perpetrators are various too. In order to differentiate between various similar concepts, try imagining a two dimensional plane separated into four quadrants by two axes, one vertical and one horizontal [Figure 1]. The horizontal axis signifies the intent of the user, ranging from “good” to “malicious”. The vertical axis signifies the number of users in question, which ranges from “individual” to “group.” The four categories created in this method show four different entities.

Entities in the first category are individual users that possess good intentions. The users of this sector are called “hackers.” The term “hacker” originally meant an individual with considerable computer knowledge, and did not signify malicious intent. In modern language, they may also be called “geeks.” A geek is defined as “a peculiar or otherwise odd person, especially one who is perceived to be overly intellectual.” Net culture, which is developed by geeks, is quite different from government culture. One of famous geeks, Prof. Dave Clark of MIT (Massachusetts, Institute of Technology) in the U.S., once said, “We reject kings, presidents, and voting. We believe in rough consensus and running code.” Rough consensus means

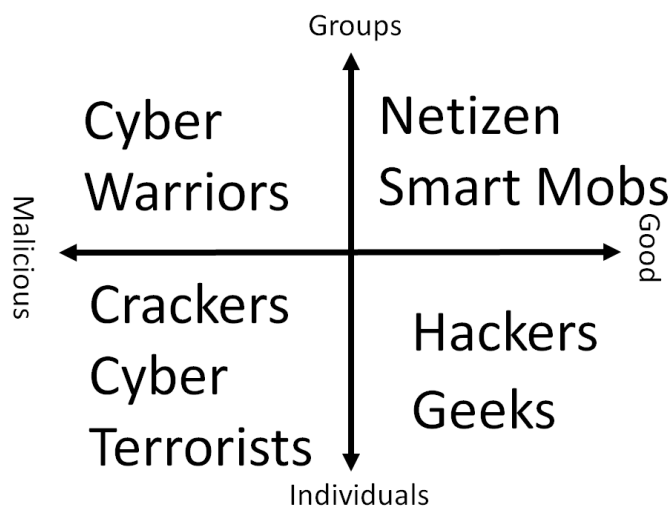


Figure 1: Concepts around Cyber Security

that they keep on discussing issues until almost all of the members agree, even if it takes several years. And running codes imply that they try to be as practical as possible. They don't accept abstract idealism and unworkable codes. It might be difficult for government agencies to work with geeks. These geeks, however, are increasingly controlling our social systems.

The second category entities are groups with good intentions. They are known as netizens, which is a combination of the words "net" and "citizen", or alternatively as "smart mobs."² These users utilize technology and knowledge shared over a network to achieve group objectives.

The problem consists of users with malicious intent. Groups of users that possess malicious intentions can be dubbed "cyber warriors." They may be sponsored by governments or non-government entities. Either way, they are users who abuse network technology in order to achieve organizational goals.

Lastly, there are individual users with malicious intentions. These users were once known as "crackers" rather than "hackers."³ However, users who conduct destructive activities with political motivations rather than mere personal enjoyment can be labeled "cyber terrorists." It should be assumed that in general usage, the term "cyber terrorist" includes "cyber warriors" as well.

Activities conducted by users with malicious intent can be divided into two categories depending on their content. Researchers John Arquilla and David Ronfeldt of the US based RAND Corporation differentiate between the terms "netwar" and "cyberwar."⁴ Netwars consist of societal-level

2) Howard Rheingold, *Smart Mobs: The Next Social Revolution*, Cambridge, MA: Perseus Publishing, 2002.

3) Steven Levy, *Hackers: Heroes of the Computer Revolution*, New York: Dell, 1984.

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

ideational conflicts, and take place between both countries and societies. Their aim is to disrupt, damage, or modify what a target population “knows,” by the targeting of public or elite opinion, or both. Simply stated, the objective of netwar is to mess with people’s heads.

In contrast, cyberwar is the conducting of military operations according to information-related principles. Such operations were conducted in Kosovo, Estonia, and other places. Put frankly, it consists of the physical disruption of information and communications systems.

In order to clarify the difference of meanings between netwar and cyberwar, I would like to call the former “head war,” because netwar is the act of trying to modify or change something in your head. In contrast, the latter could be called “body war,” as cyber war means physical damage.

To sum up what has been said so far, the concept of cyber terrorism can be broken down into multiple categories based on the subject being a group or an individual, and the target being mental or physical.

The more our social system becomes dependent on computers, the more vulnerable our society becomes to attack by cyber terrorists. The problem is, computers and networks remain “black boxes” to many of us. It is becoming increasingly more difficult to understand the inner workings.

As a result, the danger exists that we may not even know that an attack is taking place. Attacks such as the demolition of a dam via remote control over a network are obvious to anyone. On the other hand, if a computer database is covertly accessed with the objective of modifying its records, it is quite likely that the time and perpetrator of the attack may go unknown. This is the reason that cyber terrorism has become a difficult concept that evokes unease.

Technology regarding the Internet is widely shared, and possesses the characteristic of being exploitable by anyone if so desired. Though it remains a black box to the uninitiated, it may in fact appear easy to the

trained eye. The Internet is also a gigantic copying machine, and such technology spreads rapidly.

Harvard professor Joseph S. Nye, Jr., pointed that “diffusion of power is characteristic in recent development of ICTs. Cyberspace does not simply level power of actors, but complex it. And a new power called “cyber power” is emerging. It is “the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain.” In terms of domain, cyber power is the fourth power after sea power, air power and space power. In cyberspace many types of network organizations rise and power is diffused as small actors gain more power.⁵

Power diffusion does not proceed in a constant pace. Countries, which do not have enough infrastructures of ICTs, won't be able to gain cyber power. With some kind of infrastructure, an individual in a small country can target a government server in a larger country. Enough knowledge and skills make it for him to give damages to the servers.

Because it sometimes happens that targets cannot recognize of being attacked. Therefore, not only law enforcement agencies but also intelligence agencies should be involved in defense against cyber attacks, especially serious attacks concerning national security.

Here intelligence is not knowledge in a simple sense. In national security and diplomacy, it means “product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign [entities]” and those entities “may include foreign governments, groups (including terrorist organizations), or areas.”⁶ Although data or information is not refined yet, intelligence is refined product made

5) Joseph S. Nye, Jr., “Cyber Power,” Harvard Kennedy School Belfer Center for Science and International Affairs, May 2010.

6) Joint Chiefs of Staff, *U.S. Department of Defense Dictionary of Military Terms*, New York: Arco, 1988, p.183.

of data and information. Governmental organizations, which produce such intelligence, are called “intelligence agencies.”⁷

In this paper, we argue that the situations in East Asia after the end of the Cold War revitalized Japanese intelligence agencies and that growing concerns on cyber security, especially the attacks to American and South Korean Internet sites in July 2009, added a new role to intelligence agencies.

III

Japanese Intelligence Agencies and Changes in the Situation in East Asia

1. Development of Japanese Intelligence Agencies

Sun Tsu, a legendary Chinese philosopher, wrote his ideas on war and spy activity 2,500 years ago. And his idea was imported to Japan in around 750. It produced a lot of ninjas, or secret agents, employed by Samurais. One of the most famous samurais, who used ninjas well, is Shingen Takeda. His war colors printed Sun Tsu's words. After the conquest by the Tokugawas in 1604, Japan enjoyed a “peaceful time” for more than 260 years. The Tokugawa Shogunate employed ninjas to maintain orders all over the country.

After the Meiji Restoration in 1868, Japan broke off all intercourse with foreign countries and imported western technologies and ideas in a positive

7) Omori, Yoshio, *Japanese Intelligence Agencies*, Tokyo: Bungei Shunju, 2005 (Japanese). Kitaoka, Hajime, *Introduction to Intelligence*, 2nd Edition, Tokyo: Keio University Press, 2009 (Japanese). Kotani, Ken, *Intelligence Diplomacy in the U.K.*, Tokyo: PHP, 2004 (Japanese). Fukuda Mitsuru, *Terrorism and Intelligence*, Tokyo: Keio University Press, 2010 (Japanese).

way. One of them is military organization regarding intelligence. Both of the navy and army of the Japanese Empire established intelligence sections. And they started collection of information, counter-intelligence, and covert actions. One of the most successful activities was done by Motojiro Akashi. His intelligence gathering and covert actions in Russia and European countries lead to the Japanese victory in the Japan-Russo War in 1904.

Today more people know the Nakano School established by the Imperial Army. Graduates of the school were highly skilled intelligence staffs. However, during the World War II, operational staffs became more powerful than intelligence officers to conduct the war. Intelligence activities were regarded less important by the war leaders.

Right before the end of the World War II, intelligence officers knew that they would lose the war and destroyed their documents, tools, devices and other evidences by themselves. After the war, the officers hid themselves from anybody's eyes. In 1980s and after, sometime before they close their lives, they started writing their memoirs and they were published.⁸

Soon after the war ended, some people tried to reorganize intelligence activities. Jun Murai, bureaucrat of the National Police Agency, was appointed as the first chief of the Research Office in 1952. It was renamed as Cabinet Research Office in 1957 and was reorganized as Cabinet Intelligence Research Office (CIRO) in 1986. Today's Japanese intelligence community, even though it was not clearly defined, includes National Police Agency, Ministry of Foreign Affairs, Public Security Intelligence Agency, and Ministry of Defense. But the scale and scope of intelligence activities

8) For example, see: Sugita, Ichiji, *War Leadership without Intelligence*, Tokyo: Hara Shobo, 1987 (Japanese). Tsukamoto, Makoto, *Record of a Intelligence Officer*, Tokyo: Chuko Bunko, 1988 (Japanese). Hori, Eizo, *Intelligence War Record of a Japanese Imperial Headquarter Staff*, Tokyo: Bungei Shunju, 1996 (Japanese).

in Japan used to be smaller and narrower. During the Cold War most of intelligence came from the United States under the Japan-U.S. Security Treaty. Japan didn't have IMINT (Imagery Intelligence) capabilities and had limited HUMINT (Human Intelligence) and SIGINT (Signal Intelligence) capabilities. There has been no anti-spy act and security clearance until today. Under the new peace constitution after the end of the World War II, spy can never be popular in Japan except in novels and movies. However, these situations started changing in the Post-Cold War era.

2. Reinforcement of Japanese Intelligence Activities

In 1998 North Korea launched a Taepodong missile. It flew over the north east part of the Japanese main island and fell in the Pacific Ocean. Although the intention of North Korea is not still clear yet, the missile impressed the Japanese citizen how dangerous North Korea was against Japanese national security.

In 2001 a North Korean spy ship came to the Japanese coast. The Japanese Coast Guard tried to catch the ship, but it sank itself after exchange of fires. Although the place where the ship sank was in Chinese exclusive economic zone, the Japanese government got permission from the Chinese government to salvage the ship. There were a lot of articles linked to North Korean agents. This incident worsened the image of North Korea among Japanese citizens.

Behind the incident both of the governments were negotiating for a summit talk. Japan and North Korea still don't have a diplomatic relationship after the end of the World War II. In 2002 Prime Minister Junichiro Koizumi and Kim Jong Il met in Pyongyang. Prime Minister Koizumi intended to break the deadlocked negotiation to bring back the

kidnapped Japanese from North Korea. However, Kim told Koizumi that eight of them were dead and only five were alive. Koizumi railed, but he signed a joint statement at the end of the talk and took the five to Japan.⁹ The return of the five was hailed in Japan, but the fact that North Korea admitted the kidnapping by government's hands and many of them were dead and the doubt that many more were still confined hardened Japanese people's minds.

Next year Japan launched information-gathering satellites, which had been anticipated for many years. These satellites were intended to gather various kinds of information such as weather and natural disaster, but the real purpose of the Japanese government is to watch East Asian situations with their own eyes. The Japanese government tried to expand its IMINT capabilities, which were dependent on U.S. governmental or commercial satellites for a long time. The resolution of images taken by the satellites was lower than American satellites and analysis skills were less adept, but the capabilities to take images anytime wanted were critical in the changing situation in East Asia.

In 2004 there were two incidents related to China. First, a Chinese submarine entered the Japanese territorial waters. After being chased by the Japanese Coast Guard, it rushed to return to a Chinese port. Its intention was not clear, and the Chinese government said it was a mistake. It is said that the Chinese navy is challenging and testing Japanese security power along coastlines and in island areas.¹⁰

Second, a Japanese consul in Shanghai committed a suicide. This is a

9) Yomiuri Shinbun, *Man who Made Diplomacy a Fight*, Tokyo: Shinchosha, 2005 (Japanese).

10) Raul Pedrozo, "Beijing's Coastal Real Estate," *Foreign Affairs* <<http://www.foreignaffairs.com/articles/67007/raul-pedrozo/beijings-coastal-real-estate>> Access on November 15, 2010.

typical honey trap. The consul, who were married and had a child, had an affair with a Chinese lady whom he met in a bar. He was blackmailed by a Chinese agent and asked to bring diplomatic codes of which he was in charge at the consulate. He was in anguish and committed a suicide after making farewell notes to his wife and the consulate general. This case, which was not revealed until 2006, again projected an image of brutal sides of the East Asian situation. This series of the events raised voices for reinforcement of Japanese intelligence agencies and a lot of policy proposals and reports were published.

Along these events, Prime Minister Shinzo Abe made a policy speech at the 165th National Diet on September 29, 2006. He said, "In order to enable swift decisions under strong political leadership on national security and diplomatic strategies, the headquarters function of the Prime Minister's Office will be reorganized and strengthened, and intelligence gathering functions will also be enhanced."¹¹ On January 26 next year he told the nation again, "In order to enable prompt response, with strong political leadership, to diplomatic and national security issues that are becoming all the more complex, we will work to establish structures to strengthen the functions of the Prime Minister's Office as headquarters. We will also work to enhance the intelligence capability of the Cabinet."¹²

Furthermore, on September 10, 2007, Prime Minister Abe said at the 168th National Diet, "No one has forgotten about North Korean missile launch and the impact of the statement of nuclear weapon test. The national security environment around our country is still serious. We need not only to strengthen commanding function at the Prime Minister's office and intelligence function of the government, but also to restructure our national

11) http://www.kantei.go.jp/foreign/abespeech/2006/09/29_speech_e.html

12) http://www.kantei.go.jp/foreign/abespeech/2007/01/26speech_e.html

security system.”

It heightens national expectation that the prime minister mentioned strengthening of intelligence activities in his speeches at the national diet three times. However, Prime Minister Abe resigned for a health reason after a big defeat in the national election in July 2007. Neither Prime Ministers Yasuo Fukuda and Aso Taro, who succeeded Abe's administration, nor Prime Minister Yukio Hatoyama, after the change of administration from the Liberal Democratic Party to the Democratic Party of Japan in 2009, were not interested in intelligence anymore. Expectation to strengthen intelligence in Japan faded away.

However, the rise of cyber security threats became another trend to push intelligence reforms in Japan. Cyber security is not necessarily an issue to be dealt with by an intelligence agency, but as cyber attacks become larger in scale and impact to national security becomes more serious, it becomes more necessary to involve intelligence agencies to prevent an attack on ahead.

IV Widening Cyber Threats in East Asia

1. Cyber Security and Corresponding Agencies in Japan

Expansions of Internet use in Japan around 2000 lead to emergence and development of a new threat, cyber security. The first corresponding government agency to cyber threats is police. If any of cyber attacks can be categorized as a crime, a police agency will catch and prosecute a perpetrator. However, if the attack goes beyond a simple crime and is

perceived as a national security threat, a military force (Self Defense Force in Japanese case) will respond to it. Falsification of web sites is just a crime, but physical attacks to critical infrastructures such as power grids or national transportation systems will be different.

The third corresponding agency is intelligence. It tries to forecast and prevent attacks beforehand. Attacks against nuclear facilities, transportation systems or financial systems are redeemable. In order to prevent those attacks, intelligence activities such as wiretapping are needed.

In Japanese case, these three types of government agencies and organizations are overlapping and going beyond each territory. They cannot be separated in a rigorous manner. The Security Bureau of the National Police Agency is a powerful intelligence section inside a law enforcement agency. The Intelligence Headquarter of the Ministry of Defense is also an intelligence section for signal intelligence (SIGINT). The top directors of the Cabinet Intelligence Research Office (CIRO) are always from the National Police Agency, and the deputy directors are always from the Ministry of Foreign Affairs.

The central problem which I want to discuss in this paper is how the Japanese governmental agencies respond to large-scale cyber attacks against Japan and other East Asian countries. Attacks, which the Japanese government suffered in the past, were at the relatively lower level such as falsification of web pages and DDOS against bulletin board systems. However, the scale of attacks against the U.S. and South Korea in July 2009 impressed Japanese government leaders. Among many related agencies, the National Information Security Center (NISC) is playing a central role in these situational changes.

2. Cyber Attacks in Everyday Life

Scope of cyber attacks and cyber crimes is wider. Their goals spread from individual to international. Broadly speaking, there are four main types of cyber attacks: (1) physical damage (such as demolition of a dam or clash of airplanes), (2) financial damage (such as unauthorized access to bank account or illegal stock exchange), (3) psychological damage (such as web falsification or service disruption) and (4) virtual damage (which are not recognized by victims such as covert operation).

Figure 2 shows the increase of reported unauthorized access in Japan. As the National Police Agency collected information in a proactive manner in 2001, its number is unusually high. The trend is stable after that, but it turned upward in 2005. Figure 3 shows the number of reported web falsification. It rose in the fourth quarter of 2009. Figure 4 is an example of web falsification.

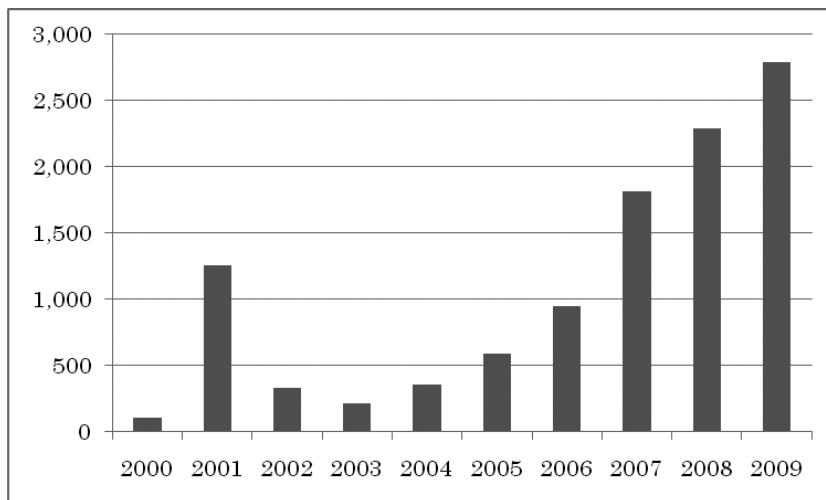


Figure 2: Reported Unauthorized Access

Source: National Police Agency

Cyber security is a problem not only in Japan, but also in other countries as they move to information society. Table 1 is a list of the top 15 countries where Microsoft's desktop anti-malware products cleaned.

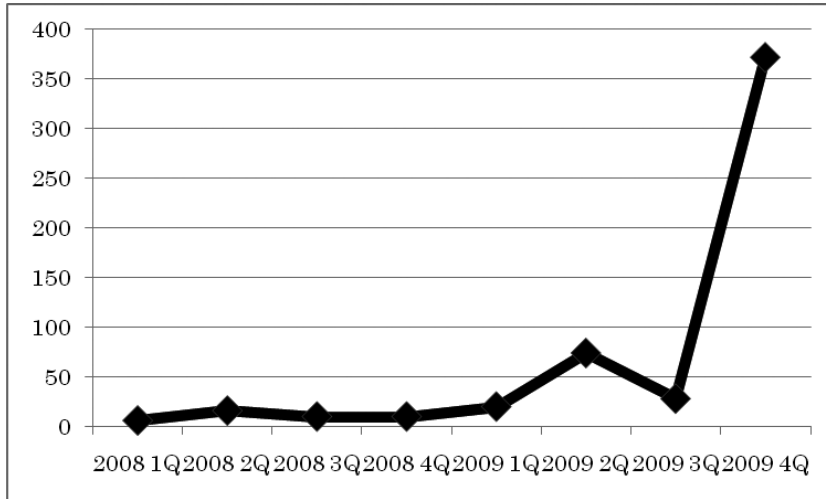


Figure 3: Number of Web Falsification (First Quarter of 2008 to Fourth Quarter of 2009)

Source: JPCERT/CC



Figure 4: Example of Web Falsification

Source: <http://truthjapan.blog118.fc2.com/>

Table 1: The Top 15 Locations with the Most Computers Cleaned by Microsoft Desktop Anti-malware Products in 2H09

	Country/Region	Computers Cleaned (2H09)	Computers Cleaned (1H09)	Change
1	United States	15,383,476	13,971,056	10.1%▲
2	China	3,333,368	2,799,456	19.1%▲
3	Brazil	2,496,674	2,156,259	15.8%▲
4	United Kingdom	2,016,132	2,043,431	-1.3%▼
5	Spain	1,650,440	1,853,234	-10.9%▼
6	France	1,538,749	1,703,225	-9.7%▼
7	Korea	1,367,266	1,619,135	-15.6%▼
8	Germany	1,130,632	1,086,473	4.1%▲
9	Canada	967,381	942,826	2.6%▲
10	Italy	954,617	1,192,867	-20.0%▼
11	Mexico	915,786	957,697	-4.4%▼
12	Turkey	857,463	1,161,133	-26.2%▼
13	Russia	677,601	581,601	16.5%▲
14	Taiwan	628,202	781,214	-19.6%▼
15	Japan	609,066	553,417	10.1%▲
	Worldwide	41,024,375	39,328,515	4.3%▲

Source: Microsoft Security Intelligence Report Volume 8 (July through December 2009)
Key Findings Summary

Examples of large-scale cyber attacks are Estonia in 2007, Lithuania and Georgia in 2008. These three countries were allegedly attacked from Russia (it does not necessarily mean that the Russian government was involved). In 2007 Israel was said to invade into and disable Syrian air defense network.

The Syrian army couldn't find any Israeli jet fighters in its radar system.¹³

Two Canadian researchers, Ronald Deibert of University of Toronto and Rafal Rohozinski of SecDev Group, found strange transmission of IP packets on the Internet. Usual virus creates infection and duplication of itself, but the malware they found didn't do such things. It invades secretly into a target computer and is controlled by remote to send files to somewhere without owner's knowledge.

The two researchers analyzed the traffic of the malware and found that 1295 computers in 103 countries were infected with the malware and 30 % of the infected computers were high value targets. And the traffics implied that they were going to China. The two analysts called the malware "GhostNet." Their analysis showed that it was not for usual cyber crimes such as financial theft, blackmail or privacy invasion. However, they had to give up their research on the way. Further research and analysis could not be done legally. The GhostNet traffics went beyond national borders. It raised a problem of legal jurisdiction. Even if it is legal in Canada, it might not be so in China. Then, they wrote a report and made it public online in March 2009.¹⁴ Their warnings widely echoed in cyberspace.

The reason why they called it "GhostNet" is that it was not clear who were operating the malware network. It is easy to say cyber security is important, but it is hard to feel its importance for real. However, clear and present massive scale of attacks broke out on the east and west sides of the Pacific Ocean.

13) Richard A. Clarke, and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, New York: ECCO, 2010, pp.1~11.

14) Information Warfare Monitor, *Tracking GhostNet : Investigating a Cyber Espionage Network*, March 29, 2009 <<http://www.infowar-monitor.net/research/>>.

3. Cyber Attacks against the United States and South Korea in July 2009

In July 2009, right after the U.S. Independence Day holidays, someone started DDOS (Distributed Denial of Service) attacks against governmental and commercial Internet sites in the U.S. More than 20 Internet sites including the White House, Department of State, Department of Justice, Department of Defense, Yahoo! and amazon were targeted.

On July 7 through 9, South Korean Internet sites such as Ministry of Defense, National Congress, National Intelligence Service (NIS), popular auction sites, financial sectors were attacked. Infected computers were spreading over South Korea and 18 other countries. Major attacks occurred in a wave fashion at 18:00 on 7th, at 18:00 on 8th and at night on 9th. The Chief of the Korean Prime Minister's Office said in a task force meeting, "This is an attack against our country's system and an act or provocation to our national security." Later analysis indicated that the attacks against two countries were done by the same program.

At first, Korean National Intelligence Service told some members of the National Congress about possibilities of North Korean involvement. But no clear evidences were presented. The South Korean government received information saying that the North Korean government had issued an order to develop computer programs to crack South Korean communications systems. Two weeks later, the government gained signs of simulation tests targeting KISA (Korean Information Security Agency) and a university in Pusan. These pieces of information lead to suspicious notion of North Korean involvement. However, most of Internet users didn't find serious problems during the attacks. They just felt that connections were slower. Infected computers became disabled, but no serious damages were reported.

After the attacks against the two countries, the South Korean government sent an inquiry to the Japanese government on eight computer servers in Japan. These servers seemed to be used as stepping stones for the attacks.¹⁵ Stepping stone is a way of hiding traces of a real attacker. The eight servers were owned by private sector and owners of the servers had no idea of how their servers were used for the attacks.

As three of the eights had a fixed IP address, they were identified and specific programs of stepping stone were found. The other five were used in commercial internet service providers and dynamic IP addresses were allocated to them. As it is against secrecy of communications to identify them, the five were still unknown.

The programs, which were found in the three servers, were the same. However, it was not possible to locate the route of which they were infected. In the program, a code to direct targets was found. Only the targets listed were attacked. But the program itself could not be fully revealed. Information, which leads to who was a real attacker and where he/she was located, was not available. And North Korean involvement was not proved. North Korea didn't have their own IP addresses and it was borrowing them from China. IP addresses which were used in the attacks were said to be owned by China.

The fact that Japanese ally (the U.S.) and its neighbor (South Korea) were attacked impressed the Japanese leaders. We will see below how they responded to this. We want to focus on National Police Agency, Ministry of Defense, and National Information Security Center (NISC).

15) Interview at the National Police Agency on July 2, 2010.

V Responses by Japanese Government

1. National Police Agency

The attacks in July 2009 heightened sense of tension in National Police Agency. Attacks to the neighboring country made the Japanese government recognize cyber attacks as real and direct threats. The Agency started making schemes to prepare for future attacks, and the July 2009 attacks became a good example to refer. On March 19, 2010, the government set up a new structure to deal with cyber issues (Figure 5). Under this structure cyber attack is recognized as one of crises including natural disaster such as earthquake or eruption. Crisis management mechanisms

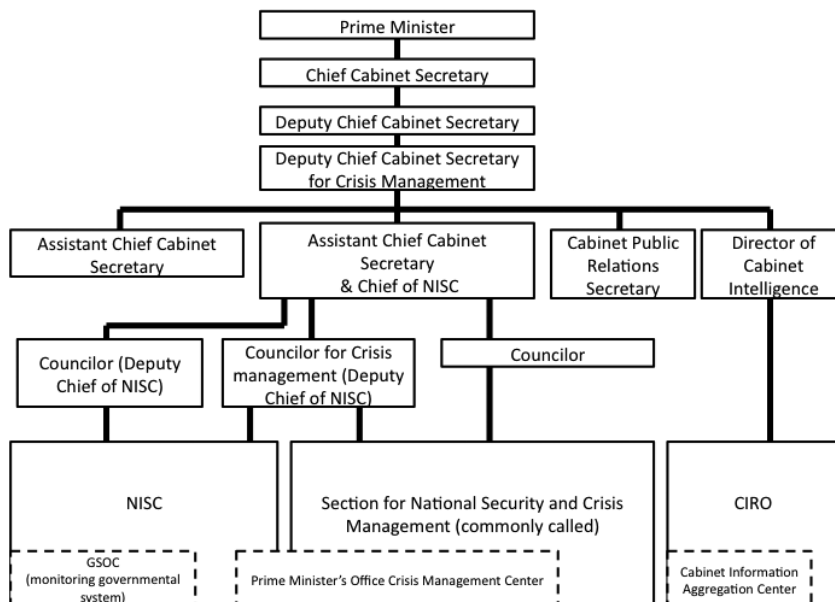


Figure 5: Crisis Management Structure for Cyber Security

Source: National Police Agency

will start working when an attack breaks out.

In addition, the National Police Agency has a fixed 24-hour monitoring system of Internet traffics in 150 points nationwide. And the Agency has contacts with 600 critical infrastructure operators. If they find a suspicious activity, they will report to the Agency. The operators are advised to make security policy and to set up a nighttime response window.

These kinds of structural changes were lead by Mr. Hirofumi Hirano, then Chief Cabinet Secretary. After looking at the July 2009 attacks, Mr. Hirano asked his staffs what would happen if Japan were attacked in this manner, and ordered them to prepare for future attacks. Although there had been discussions to prepare for cyber attacks since spring of 2008, serious preparations started right after his direction.

The National Police Agency has not officially evaluated the July 2009 attacks. Officers in charge felt that the attacks were more demonstrating than harming, but they were too long for a demonstrating purpose. DDOS attacks don't take any data from attacked servers. It is difficult to know the real intention of the attacker.

2. Ministry of Defense

The Ministry of Defense of Japan thought that the influence by the July 2009 attacks were minimum, because its systems including the Self Defense Force (SDF) were quite independent from the Internet.¹⁶ Note, however, that the Ministry was thinking of cyber security as computer system level until the release of “Information Security Strategy for Protecting the Nation” in May 2010.¹⁷

16) Interview at the Ministry of Defense on October 4, 2010.

17) NISC, Information Security Strategy for Protecting the Nation, May 2010, available at <http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf>.

The Ministry started thinking that it should be considered as national security level.

It was less important for the Ministry of Defense that Japanese ally (the U.S.) and neighbor (South Korea) were attacked. The Ministry was thinking that such attacks could come to Japan anytime. The U.S. Military has a long tail of logistics in order to deploy troops overseas, for example in Iraq or Afghanistan. On the contrary, the SDF is not expected to deploy overseas due to the constitutional limit. Then, the main goal of the Ministry is to protect its command and control systems inside Japanese territories.

The Ministry is preparing enough to threats from outside Japan, but there is still a problem of internal threats as William J. Lynn, Deputy Secretary of Defense, wrote in his Foreign Affairs article.¹⁸ Although users of the systems are strictly limited, devices such as USB memory stick are easy and convenient. It is difficult to stop such ill-planned actions completely. Confidential information can be flown out through such devices and virus or malware can be brought into systems.

In case of emergency, the National Police Agency and the Ministry of Defense are mandated to cooperate to respond to the situation (Figure 6). In order to make it happen under the NISC, the Ministry missions 7 self-defense officials to NISC.

As the Ministry has no monitoring system such as National Police Agency, the Ministry can detect attacks against it only, and cannot grasp the whole picture of attacks against the Japanese government. It needs to get information through the NISC. And the Ministry does not analyze attacks by itself. Cyber Clean Center (CCC) which is operated by the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade

18) William J. Lynn, III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, vol. 89, no. 5, September/October 2020, pp.97~108.

and Industry will do such analysis. Needless to say, some attacks cannot be dealt with by anti-virus software. And there are numerous spam messages and port-scanning accesses every day. After the Senkaku Islands dispute in autumn of 2010, there was a slight increase of access to web sites of the Japanese government, but there was no serious influence. Those increases of access could be dealt with at the system management level. For the Ministry, it doesn't matter much who is attacking. In terms of defense, the SDF must protect the nation from any enemies. Identifying or catching them is out of scope of the Ministry of Defense. The highest priority is to “protect” the nation.

The Ministry is interested in USCYBERCOM, which the Obama administration set up. It is possible that the Ministry would have a similar organization under the SDF. In order to protect the nation, the Ministry and the SDF must protect their own communications system first. And they are going to set up “cyber space defenseunit” (tentative title) by March 2011.¹⁹

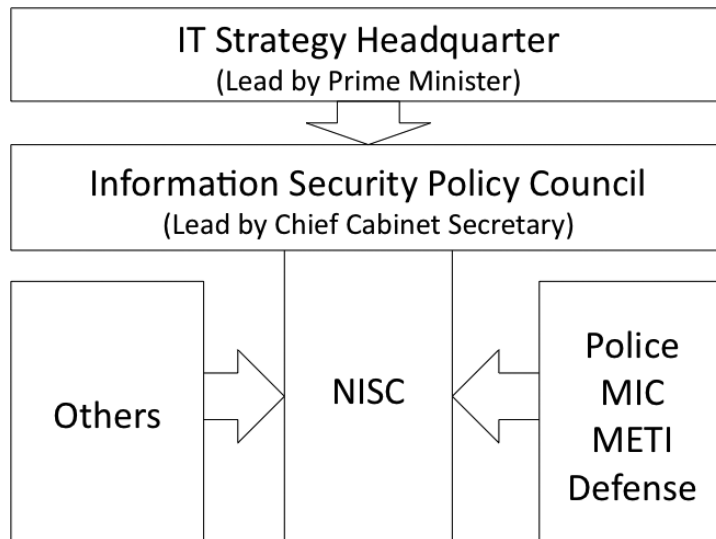


Figure 6: Organization for National Information Security in Japan

Source: Cabinet Office

19) Ministry of Defense, “Japan’s Defense and its Budget,” Ministry of Defense, 2010, p.8.

3. NISC

As Internet population in Japan started growing in 1999 or 2000, cyber security measures became a policy issue. There were several web falsification incidents allegedly from foreign sources. In February 2000 the Information Security Section was created under the Cabinet Office. And it became the National Information Security Center (NISC) in April 2005. Next month of that, the National Information Security Council was established. In the background of these movements, realization of safe environment for ICTs, that is, realization of “advanced information security country,” was regarded vital to sustainable development of the Japanese economy and higher welfares for the Japanese nation. NISC is serving as secretariat bureau of the National Information Security Council and is developing various kinds of strategies, initiatives and goals. It is also mandated to coordinate public-private common information (or cyber) security policies.

The Council was established by the Chief of the IT Strategy Headquarter, that is, Prime Minister of Japan, on May 30, 2005. The Chief Cabinet Secretary is chairing the council and deputy chair is Minister of State for Science and Technology Policy. Members of the Councils include the Commissioner of the National Public Safety Commission, Minister of Internal Affairs and Communications, Minister of Economy, Trade and Industry, Minister of Defense. And six expert members from the private sector join the Council.²⁰

The Council released its “First National Strategy on Information Security: Toward the Creation of a Trustworthy Society” on February 2, 2006.²¹ It

20) The author is one of the expert members of the Council.

21) http://www.nisc.go.jp/active/kihon/pdf/bpc01_ts.pdf

covered fiscal year 2006 to 2008 and mandated to publish a plan for each year. The “Second National Strategy on Information Security: Aiming for Strong ‘Individual’ and ‘Society’ in IT Age” was released on February 3, 2009 covering FY 2009 to 2011.

However, after the Second National Strategy, in July 2009, the massive scale of cyber attacks against the United States and South Korea broke out. In August 2009 the Liberal Democratic Party (LDP), which had been in a ruling position for a long time, was lost in a national election, and the Democratic Party of Japan (DPJ) made a coalition government. Then, the Council and the NISC started revising previous policies and released “the Information Security Strategy to Protect the Nation” on May 11, 2010. This strategy covers FY 2010 to 2013 including the Second National Strategy and mandated annual plan to be created. The first page of the Strategy says like below.

After the Second National Strategy on Information Security was resolved, a large-scale cyber attack took place in the United States and South Korea in July 2009. Also, numerous incidents of large-scale private information leaks occurred one after another.

The large-scale cyber attack in the United States and South Korea particularly alerted Japan—where many aspects of economic activities and social life are increasingly dependent upon Information and Communication Technology (ICT)—to the fact that a threat to information security could be a threat to national security and require effective crisis management.²²

It means that the cyber attacks against the United States and South Korea played a critical role in the revision of Japanese cyber security

22) NISC, Information Security Strategy for Protecting the Nation, May 2010, available at <http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf>.

measures.

The basic principle of the Strategy has three points. First, strengthening of policies and upgrading of counter measures, second, establishing information security policy to be adjusted into new changing environments and third, transformation from reactive information security measures to proactive ones. It is not fair to say that cyber attacks were neglected or considered less serious in the First National Strategy and the Second National Strategy. However, it is noteworthy that cyber attack concerns hatched to the fore in the Strategy.

In the last week of September 2010, U.S. Department of Homeland Security had the world's largest simulation called "cyber storm" in cooperation between the government and the private sectors. Japan joined it for the first time: NISC, National Police Agency, Ministry of Economy, Trade and Industry, and non-profit JPCERT/CC. More than 3000 people in 13 countries participated in the simulation. It was the third cyber storm after February 2006 and March 2008.²³

Cyber security was not so high in DPJ's policy agendas. The Council's meeting was not held for 9 months after DPJ took the administration in August 2009. Soon after taking the office, DPJ announced that minister-level meetings, which were created under LDP administrations, should be reviewed, merged, or abolished. In the review process of government works, various kinds of budget were cut or reduced. It was said that NISC's activities were also to be influenced.²⁴ But it is also true that existence of the Council and NISC was buried in flooding policy agendas that the new administration tried to rethink. Prime Minister, Chief Cabinet Secretary

23) Erika Toh, "13 Countries Cooperate to Combat against Cyber Attacks," *Asahi Shinbun*, October 4, 2010.

24) Actually 18 ministerial meetings were abolished by November 2009. http://www.kantei.go.jp/jp/tyoukanpress/rireki/2009/11/17am_siryou.pdf

and other ministers were too busy to work on other issues.

About one month after the release of the Strategy, Prime Minister Yukio Hatoyama resigned and Naoto Kan, new leader of DPJ, succeeded the administration. Under the new cabinet, the National Information Security Council's meeting was held on July 22, 2010, and it authorized its annual plan called "Information Security 2010." The first item in it is "upgrading counter measures for large-scale cyber attack situations" and 19 policy items were listed in the plan.

VI Changes in East Asia

1. China

East Asia is one of the hottest regions in the world in terms of cyber activities including cyber attacks. The number of Internet users are growing rapidly mainly due to China and India, largest population countries in the world. Hottest spots for cyber security in the region are China and South Korea. Japan is sometimes a target of cyber attacks from China and South Korea due to historical disputes, but they are not sole reasons. Today's political systems and international situations around both of the countries are influencing cyber security in East Asia.

Chinese presence in cyberspace is becoming greater and greater. The whole Internet population is estimated as around 1.6 billion, and China takes one fourth, more than 400 million as of March 2010. However, the penetration ratio in Chinese population is still around 30%. If the number goes up to the same level as developed countries, Chinese presence will be

overwhelming.

However, China is "notorious" for attacking other countries online. The Times reported in 2007 that China is trying to achieve "electronic dominance" over each of its global rivals by 2050, particularly the US, Britain, Russia and South Korea. According to the same article, the Pentagon logged more than 79,000 attempted intrusions in 2005. About 1,300 were successful including the penetration of computers linked to the U.S. Army's 101st and 82nd Airborne Divisions and the 4th Infantry Division.²⁵

In January 2010, a search engine giant, Google, started disputes with the Chinese government. It claimed that it could not follow censorship anymore, which was mandated by the Chinese government, and that their systems, especially free e-mail service Gmail, were being attacked from China. With U.S. government's support, Google tried to change Chinese government's policy in vain. Google withdrew from the Chinese market in the end and got a service license to reroute their search engine to its Hong Kong site.

These kinds of news on Chinese cyber attacks are flooding over media, but the Chinese government is claiming that none of the Chinese government, the Chinese Communist Party and its People's Liberation Army are involved in any cyber attacks, and that China is being continuously attacked by foreign powers. Norton Online Living Report 2009 reported that 53% of Chinese Internet users had experienced cyber intrusion into their computers, the highest among surveyed countries.

The Chinese government admits that they are introducing censorship system, or "cyber great wall." This system is somehow different from

25) Tim Reid, "China's Cyber Army is Preparing to March on America, says Pentagon," Times Online, September 8, 2007 <http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2409865.ece> (access on May 9, 2010).

conventional censorship in the 20th century. It is definitely impossible to check all the traffics in the Internet. The scale of data is exploding. Computer programs do most of the censorship procedures and humans make only political decisions. Very sophisticated “walling” technologies are introduced into Chinese Internet systems.

It used to be difficult to access New York Times, Washington Post, CNN and other news media from China, because they sometimes post articles to criticize Chinese politics. However, the Chinese government lifted its regulation, as human rights groups outside China made proxy servers to reroute censorship. Some of online social services such as Twitter, YouTube, and Facebook are still being blocked. These services are very popular outside China and could be popular in China too. Many Chinese users are using Twitter with some alternative methods. It is a big irony that a socialist country is blocking social media. Not only Google but also other search engines are following a black list of search key words. Results of keyword searches are different inside China.

It is quite strange that there are a lot of cyber crimes and attacks in China while the government is maintaining stronger control over the Internet. Both of Internet connection service providers and content service providers must be registered and providers watch their customers in detail. Even when a Chinese citizen uses an Internet café, he/she must register an ID. The government is also regulating international traffics, because all of international gateways are under control of the government. If the government is really serious, it can stop “illegal” or suspicious traffics. This point makes people outside China to believe in government’s involvement in cyber attacks against foreign countries.

2. South Korea

South Korea was the earliest broadband adopter for mass market in the world. The country saw serious economic downturn in the Asian economic/financial crisis in 1998. In order to recover from the depression, President Kim Tae-jung proposed “Cyber Korea 21” in 1999 and introduced ambitious technologies and policies to make the country fit into a new political and economic modes in the digital age. Key technologies include semiconductor chips, ADSL (Asymmetric Digital Subscriber Line) for Internet broadband access, and CDMA (Code Division Multiple Access) for mobile phone. Samsung and other digital vendors went global, while Japanese vendors stuck to its domestic market.

There are many reasons why South Korea got advanced in broadband adoption. One of them is more than 1/5 of the total population is living in Seoul and most of them are living in apartment complexes. It is costly to lay broadband access technologies in vast areas, but the population in South Korea is concentrating in Seoul and several cities. People competed to gain faster speeds to get jobs, educate children, buy cheap, and other purposes.

The success in broadband penetration made the South Korean to feel proud of their new cyber cultures. They are important part of life there. However, new threats of cyber security arose at the same time, especially ID theft. A big boom of online economy in South Korea was made possible by its resident registration number, which is assigned to every citizen in South Korea in order to burn out North Korean agents hidden in South Korean society. All of Internet service sites requested users to register their own numbers. The number system helped service providers to understand customers better. However, theft of ID numbers became a serious social problem. Financial fraud, impersonation, privacy invasion and other crimes

and attacks were seen. In addition, computer viruses and spam mails were getting worse.

South Korean government's third ICT promotion plan, "e-Korea Vision 2006," published in April 2002 included a chapter for cyber security saying that advancement of cyber security infrastructure by public-private partnership was needed. The Ministry of Information and Communication published "Secure e-Korea 2002-2007" in July 2002. However, on January 25, 2003 Slammer worm started bringing serious damages to core Internet servers in South Korea. The services were forced to shut down for several hours. This incident is called "1.25 Big Confusion." In order to protect the nation, the South Korean government issued "National Information Security Basic Directive" in 2004.

In 2008 President Lee Myung-bak reorganized the Ministry of Information and Communication, and its functions were transferred to Ministry of Public Administration and Security (MOPAS), Ministry of Culture, Sports and Tourism, and Ministry of Knowledge Economy (MKE). And Korea Communications Commission (KCC) is regulating the industry now. However, national security perspective of cyber security is administrated by the National Intelligence Service (NIS). Under NIS, National Cyber Security Center (NCSC) is the core of policy making. Outside the government, KISC is a CSIRT (Computer Security Incident Response Team) and KISA (Korean Information Security Agency) is playing a role to bridge between the government and the private sector.

The large-scale cyber attacks against the U.S. and South Korea in July 2009 was a big shock to South Korea. They had been ready for those kinds of attacks because their neighbor North Korea could be a major source of any threats and it was easy to expect North Korea would start a cyber attack. But they got big damages. One of Korean journalists wrote, "South Korea was proud to be an Internet advanced nation and its economy is

supported by exports of IT-related technologies. The biggest loss in this attack was that its image was hurt.”

We still don't know who did the attacks, but the South Korean government is more serious now to defend its cyber domain from any attacks by North Korea and others. For example, in February 2010, the South Korean government proposed to set up an organization for international cyber security under the United Nations and to locate it in Seoul. It was not agreed, but the government understands well why it must protect its cyber infrastructures.

VII Conclusion

In order to respond to changing situations in East Asia after the end of the Cold War, widening scope of intelligence activities to get rid of national security threats is an important policy agenda in Japan. Rising possibilities of cyber attacks in recent years added a new role to intelligence agencies. So far, there has been no successful large-scale cyber attack against Japan. Needless to say, it does not guarantee an attack would never come in the future. As a goal of intelligence is to find clues and signs of such threats beforehand, we might be able to say that intelligence is working. Even if so, a failure of intelligence brings huge loss and damage. Not only to stop an attack, but also to respond to it in a better way are necessary to be considered.

The attacks in July 2009 build a momentum to move forward Japanese cyber security measures. The change of administrations is a big factor, but it is noteworthy that the Second Information Security Basic Plan was

overwritten while it was still active after the attacks.

NISC is not within the Japanese intelligence community, but it must help the community and political leaders for better approaches. Its role is critical in cyber security preparedness. We need to define NISC's role more clearly in national security environments.

Widening scope of intelligence in society might raise anxieties over privacy and other basic human rights. For example, we might need executive power to wiretap communications to prevent cyber terrorism, which Japanese law doesn't allow (but wiretapping for law enforcement purposes is allowed). The Council and NISC are publishing a series of strategies, but we need concrete policy measures to fulfill them. Among other things, Prime Minister's and his cabinet's political will are needed to move forward the Council, NISC and other related agencies and private sectors towards better preparation to protect thenation.

러시아 군의 현대화 : 21세기 전략을 찾아서

Dmitri Trenin || 카네기 모스크바 센터장

목 차

- I. 서 론
- II. 러시아 군 개혁 : 성과와 과제
- III. 미-러의 전략적 관계와 유럽 미사일 방어체제
- IV. 러시아 안보의 주요 과제
- V. 결 론

I 서 론

2008년, 러시아 지도부는 지난 20여 년간 방치되어 있었던 군 개혁 작업에 착수하였다. 이와 같은 결정은 이로부터 1년 전인 2007년 2월 과거 군사 조직에서의 경험이 전무한 아나톨리 세르듀코프를 국방장관으로 임명하는 파격적인 인사와 함께 시작되었으며, 2008년 8월에 벌어진 남오세티아 5일 전쟁 이후 대중들에게 발표되었다. 남오세티아 전쟁에서 러시아는 그루지야 군을 제압하며 승리를 거두었지만 한편으로는 러시아 군의 심각한 약점을 드러낸 바 있다.

한편 2011년, 러시아 정부는 방위산업 현대화를 위한 대규모 사업에 착수하기로 결

정하였다. 해당 계획은 향후 10년 동안 20조 루블(약 7,000억 달러)을 투입하여 러시아 군이 사용하는 무기체계와 장비를 업그레이드하는 것을 골자로 한다. 이와 같은 노력은 소련의 해체 이후 처음으로 러시아 정부 정책의 우선순위에 중대한 변화가 있었음을 보여주며, 러시아 정부가 더 이상 군사현안을 뒤로 미루지 않고 최우선순위에 두어 해결하고자 한다는 사실을 반증하고 있다. 그러나 이를 위해서는 필연적으로 막대한 재정 자원을 투입해야만 한다.

II 러시아 군 개혁 : 성과와 과제

세르듀코프 국방장관이 주도해온 군 개혁 노력은 블라디미르 푸틴 대통령의 전폭적인 지지 하에 이후 지난 4년 동안 다음과 같은 주요한 성과를 내었다.

- 비대한 장교 조직을 100,000명 이상 감축하고 민간 분야와 비교하여 경쟁력을 확보하기 위해 나머지 장교들의 봉급을 2~3배 인상하였다.
- 제2차 세계대전 방식의 동원 병력인 간부 조직(할당 병력의 10~20%) 및 정원 미달 부대(할당 인원의 50%)를 다수 해체하고 군 기지, 저장시설, 부지 등을 대폭 축소하였다.
- 러시아 군의 지휘구조를 3단계로 새롭게 나누었다: 군 총참모부 - 지역사령부 - 여단(지상군 및 타 군도 동일하게 적용)
- 전략적 수준의 대규모 군사 연습을 재개하였다.
- 최초로 아웃소싱제를 도입, 군 인원을 비군사 인원으로 대체하였다.
- 최초로 민간 출신 국방장관을 임명하고 총참모부장직을 그 예하로 두어 군에 대한 정치적 통제를 강화하였다.

러시아 군의 개혁은 러시아 정부가 뒤늦게 자국의 전략적 상황에 대한 기본 재평가를 실시함에 따라 탄력을 받게 되었다. 냉전이 종식되고 20년이 흐른 후, 과거 군 임

무의 주요 초점이었던 몇몇 주요 적국들을 상대로 한 대규모 분쟁 문제는 그 가능성이 매우 낮아짐에 따라 우선순위가 낮게 조정되었다. 그 대신, 1990년대의 체첸 전쟁, 2008년 그루지야 전쟁과 같은 러시아 국경 부근에서의 국지전 문제를 가능성이 높은 무력 충돌의 형태로 규정하고 우선순위를 격상시켰다. 이로 인해 러시아 군은 지난 130여 년 동안 조직의 뼈대가 되었던 기존의 동원체제로부터 탈피할 수 있게 되었다.

군 개혁은 비대한 군사 조직을 최적화하고 정치 지도부의 군사수단 활용 능력을 증진시키는 것에 중점을 두었다. 2006년, 푸틴 대통령은 체첸 전쟁 당시 1,400,000명의 군 병력 중 오직 65,000명만을 활용하여 북코카서스 지역에서 대테러 작전을 수행하도록 할 수도 있었다는 점을 지적하였고, 그 후 2008년, 육군부대의 13%만이 상시 대비태세를 유지하게 되었다. 현재 추구하고 있는 러시아 군의 비전은 더욱 이동성이 높고 교전에 대해 상시 대비태세가 잘 갖추어져 있는 상설군을 조직하는 것이다. 또한 전투 대비태세의 개념을 기존 24시간(통보로부터 교전지역에 도착하기까지의 시간)에서 1시간으로 단축하여 개정하였다.

군 개혁의 또 다른 주축을 이루는 것은 지휘통제 구조의 개선이다. 새로운 구조는 더 이상 동원 관리에만 얽매이지 않고 작전수행 위주로 구성되었다. 따라서 기존 사령부를 구성하던 5단계 중에서 2개(사단 및 연대)를 없애고, 사단 조직을 여단으로 재편성하고 그 예하에 대대를 두었다. 군관구의 수는 기존 6개에서 4개로 축소하였으며 이름은 그대로 유지하되 실제로는 각 해당 지역의 모든 군 병력에 대한 책임을 갖는 합동전략사령부로서의 역할을 담당하도록 하였다. 이로 인해 육군 부대의 91%와 공군·해군 부대의 약 50%가 감축되었으며 더불어 새로 창설되는 부대들은 서로 유사한 표준 무기체계와 장비를 사용할 수 있도록 하였다.

또한 개혁의 핵심은 인원요소에 있다. 필요 이상의 고위급 장교를 감축시켰으며 임관 장교의 수를 2008년의 335,000명에서 220,000명으로 감축시켰다. 반면 계약직인 부사관과 자원입대 인원수를 2012년 180,000명에서 2017년까지 425,000명으로 늘릴 계획이며, 또한 기존에 러시아 군의 주축을 이뤄온 징집 인원수를 2017년까지 270,000명으로 줄일 계획이다. 이와 함께 군인의 봉급 및 혜택과 제대군인의 연금을 2배 이상 인상하여 군 입대 자원의 질을 향상시키고 계약 군인의 재입대를 보장하도록 하였다.

마지막으로, 군의 무기, 탄약 및 장비를 현저히 업그레이드 하였다. 물론 현대식 무기를 어떻게 정의하느냐에 따라 달라지겠지만 현재 현대식 무기가 러시아 군 전체에

서 차지하는 비율은 약 30% 정도로 추산되며 2020년까지 70%로 늘어날 것으로 보인다. 국방예산 중 물자획득이 차지하는 규모는 2000년의 20%에서 2010년 38%, 2013년에는 59%까지 확대될 예정이며 러시아 총 국방지출은 2011년 GDP 대비 2.9%에서 2014년에는 3.9%로 증가할 것으로 예상된다. 러시아 국방예산을 달러로 계산하면 미국의 총 국방예산의 7% 정도밖에 못 미치는 수치이지만 향후 현저히 증가할 것으로 예상된다. 평소 러시아의 공식 수치에 1.5% 정도 더하여 추산하는 스톡홀름 국제평화연구소(SIPRI)의 보고서에 따르면 러시아는 2014년에 GDP 대비 4.8%인 현재 미국의 수치를 추월할 것으로 전망된다. 이는 유럽 또는 중국보다 훨씬 높은 수치이다.

러시아 총 노동력의 1.5%인 150만 명 정도가 종사하는 방위산업 또한 러시아 정부의 새로운 요구사항에 발맞춰 유사한 재구조, 통합 및 개혁의 움직임이 보이고 있다. 2011년, 국방부와 마찬가지로 러시아 정부는 강력한 새 인물인 야심찬 정치가이자 과거 나토 주재 러시아 대사를 역임한 바 있는 드미트리 로고진을 임명하여 러시아 방위산업 조직의 현대화 전환과정을 총괄하도록 하였다. 2012년 재선에 성공한 블라디미르 푸틴 대통령은 공약으로 방위산업을 “재산업화” 정책의 원동력으로 만들겠다고 선언하였다. 비록 현재까지의 성과는 미미하지만 이는 기존의 방위산업이 갖고 있는 문제점을 뚜렷이 드러내었다.

러시아 방위산업이 겪고 있는 주요 문제점들은 다음과 같다 : 노동력, 생산 및 공장의 노후화, 낮은 특대형 구조(2010년 기준 업체 수 1,700개 이상, 이 중 가장 큰 규모의 업체도 국제 기준과 비교하면 작은 수준), 전반적인 경쟁력 및 투명성 부족, 만연한 부정부패, 불투명하고 비현실적인 가격책정 제도, 수출위주 기업의 호황과 국내시장 위주 기업의 불황 간의 확연한 차이, 비효율적인 연구·개발 업무, 대외협력 부족 심화, 지난 20년 동안 방위산업에 대한 자금공급 부족 고질화 등.

한편 러시아 정부는 방산 업체에 대한 국방부의 역할을 강화하고 2020년까지의 군사 기술 우선순위를 다음과 같이 제시하였다 : 핵 역지력을 제공하는 전략체계, 방공체계, 통신, 자동화 지휘·통제·정보 장비, 전자 대항책, 무인기, 무인타격체계, 수송기, 해군체계(특히 북극해 및 태평양 지역), 정밀유도 무기체계, 장병 개인보호 수단 등.

러시아 정부는 원유 값 침체 및 하락으로 인한 경제 저성장(중기적으로 연간 3~4%)과 예산 긴축에도 불구하고 군 현대화를 위해 이미 책정한 예산을 모두 투입할 의지를 보이고 있다. 그러나 방위산업을 향후 몇 년 사이에 군과 같은 수준으로 최적화하고

재구성할 수 있을지는 미지수이다. 확실한 점은 이러한 최적화와 재구성 없이는 국방 비로 책정된 중요한 예산이 낭용되고 러시아 군 능력의 증대와 관련이 없는 곳에 쓰일 가능성이 높다는 것이다.

한 가지 우려사항이 더 있다면 러시아가 개혁을 수행하는 과정에 있어서 새로운 안보 및 국방 “소프트웨어”를 구상하는 노력이 확연히 부재하다는 사실이다. 그러나 2012년 5월 7일자로 공포된 대통령령은 “향후 30~50년에 대해 분석하고 전략계획을 세우기 위한 질적으로 새로운 체계”를 수립하고 국가 무기체계 사업에 대한 지침을 제공하도록 규정하고 있다. 이는 경제, 국내, 해외 및 안보 정책, 과학·기술, 인구통계와 더불어 기타 주요 분야에서의 세계적·국가적 흐름을 예측하고 분석하도록 하는 훌륭한 첫걸음이다. 더불어 이와 같은 분석을 토대로 냉전시대의 고정관념에서 벗어나 21세기 세계관을 새로 수립할 필요가 있다.

Ⅲ 미-러의 전략적 관계와 유럽 미사일 방어체제

2010년, 러시아 군은 새로운 교리를 공식적으로 채택하였다. 이는 지난 수십 년간 러시아 군 사고방식에서 지배적이었던 대규모 전쟁 개념을 지양하고 있다. 이는 큰 발전이며 군 개혁과 현대화를 향한 길을 열어주는 것이라 할 수 있다. 해당 교리는 대규모 전쟁 대신 미국과 같은 주요 강대국에 대한 핵 억지력과 국지적·지역적 우발사태에 중점을 두고 있다. 억지력이 세계에서, 특히 핵 강대국들 사이에서 전략적 안정 유지를 위해 중요한 역할을 하고 있다는 것은 자명한 사실이다. 하지만 냉전 종식 이후에 억지력은 이제 매우 달라진 역할을 담당한다. 21세기에 미국과 러시아 간 핵 교류가 이루어질 가능성은 매우 낮다. 하지만 핵 관련 분야에서 예측성 및 안전성 개선을 위해 추가적으로 노력할 여지는 남아있다. 미-러 간의 전략적 관계는 유럽 미사일 방어체제 등의 전략적 협력을 통한 상호 신뢰구축 방안을 통해 안정될 수 있다.

향후 중기적으로 볼 때, 유럽 미사일방어 문제는 난관이자 기회로 작용할 수 있다. 동 사안에 대하여 합의가 이루어지지 않을 경우 미-러 관계는 시간이 지남에 따라 더

욱 악화될 수 있고, 세계 전략 균형에 불안정을 초래할 수 있다는 측면에서 보면 이는 난관으로 작용할 것이다. 동시에 미사일 방어체제 협력에 있어서 이란의 잠재적 미사일 위협으로부터 미국의 자산 및 동맹국을 보호하고자 하는 미국의 국익에 반하지 않는 동시에 러시아의 핵 억지력을 확보할 수 있는 방안을 도출해내는 기회가 될 수 있다. 이러한 협력방안은 과거의 적대감이 아직 남아있고 서로를 경계하는 상태로 존재하는 현재의 전략적 미-러 관계를 보다 협력적이고 비적대적인 관계로 발전시킬 수 있는 주요 변수로 작용할 것이며 또한 미국과 러시아가 지금의 변화하는 세계에서 긍정적인 역할을 담당할 수 있도록 유도할 것이다.

미국과 나토 동맹국들은 최근 유럽에 미사일 방어체제를 도입하기로 결정하였으며 러시아 또한 본 사업에 참여 제안을 받은 바 있다. 그러나 러시아는 나토 사업 중 일부 단계에서 요격미사일(SM3 Block IIB)을 배치하는 것에 대해 우려를 표명하였으며, 러시아 측 주장에 따르면 해당 요격미사일은 러시아가 보유한 대륙간탄도미사일(ICBM)을 요격할 수 있는 능력을 갖추고 있다. 이에 대한 대응책으로 러시아는 유럽 미사일 방어체제 공동 운영을 제안했으며, 이것이 불가능할 경우에는 유럽 미사일 방어체제가 러시아의 전략 무기에 대응하는 능력을 포함하지 않도록 법적 구속력을 갖는 합의를 미국과 체결하는 방안을 제안했다. 그러나 미국이 이와 같은 러시아의 제안을 받아들일 수는 없을 것이다.

그러나 여전히 문제를 해결해야 할 필요성과 방안은 존재한다. 본 사안에 대한 해결책을 찾고자 하는 이유는 미-러 간의 합의가 없을 경우에 양국 모두 실질적인 손해를 감수해야 하며, 또한 역으로 생각해보면 양국 간의 협력은 양국의 국가 안보를 증진시킬 수 있기 때문이다. 즉, 본 사안은 미-러 관계를 좌우하는 전략적 변수로 작용할 수 있는 것이다. 양국은 서로에 대한 핵 억지력 확보, 핵 무력화 능력 및 제3자로부터의 미사일 위협에 대한 미-러 양국의 전략적 안정성 확보를 위해 협력해야 한다. 따라서 미국은 러시아 지도부가 지속적으로 억지력을 확보하려 할 것인지, 또한 러시아가 이란의 핵·미사일 개발사업 진척 수준에 대하여 우려하고 있는지에 대해 관심을 가져야 할 것이다.

미국-나토-러시아는 다음 원칙을 바탕으로 유럽 미사일방어체제에 대한 협력을 진행할 수 있을 것이다 : (1)1987년 미국과 소련이 체결한 중거리 핵전력 협정(INF)에 의거 금지된 중거리 탄도미사일을 보유하는 등 제3국으로부터 발생하는 위협 문제에 대응 (2)상호 협력노력을 통해 해당 위협에 대한 각 국가 대응의 효율성 증진 (3)미사

일방어 분야 내 협력을 활용, 미-러 관계를 서서히 비적대적이고 협력적·전략적인 관계로 발전시켜 유럽-대서양 지역 내에 안보 공동체 창설. 위 원칙들은 카네기재단에서 추진한 유럽-대서양 국제안보 위원회(EASI)에서 수립하였다.

이를 기반으로 한 협력방안에는 다음 주요 요소들을 포함시킬 수 있다: (1)국가 및 동맹국의 미사일 방어체계 간 교류: 현 시점에서 공동 미사일 방어체계는 실현 가능성이 희박하고 여전히 각 국가들이 각자의 안보 및 방어에 대한 총책임을 가진다. (2)관련국들의 정보 자산을 통합, 제3국의 미사일 활동에 대한 실시간 정보 교환 (3)타국을 목표로 발사되어 자국 영토를 거쳐 날아가는 미사일을 당사국이 격추하도록 하는 작전 절차 가동 (4)미-러 미사일 방어체계를 상호 호환시킬 수 있도록 적절한 기술 교환 (5)행정 협정의 형식으로 위 요소들의 체계화 등.

위에 제안된 방안을 당장 실행에 옮길 수는 없다. 대신, 미국과 러시아는 위성 및 레이다 정보를 실시간으로 수집, 공유하는 협력 본부를 구성하여 미사일 공격에 대한 공동 통지를 제공하는 일부터 시작해야 할 것이다. 이 본부는 나토 회원국(예, 폴란드 또는 벨기에) 한 곳과 러시아에 설치되는 것이 바람직하며, 각 본부에는 나토 및 러시아 인원을 함께 배치하여 미사일 활동에 대한 공통된 상황도를 구상할 수 있도록 해야 한다. 또한 이러한 본부를 설치함으로써 이미 미-러 간 2000년에 체결한 바 있는 조기경보 정보교환 합의서를 이행할 수 있고, 좀 더 높은 수준의 교류와 통합을 진행할 수 있을 것이다. 러시아에 설치되는 본부에서는 자료를 통합하고 전체적인 상황도를 구상하는 일에 초점을 두는 한편, 나토 국가에 설치되는 본부에서는 실제 미사일 위협에 대한 대응을 협조하는 일을 수행하도록 할 수 있겠다. 이를 위해서는 2012년 3월에 재개된 미-러 탄도미사일방어 연합지휘참모 연습을 확대하여 중-장거리 미사일에 대한 방어를 포함하도록 하는 것이 필요하다.

유럽 미사일방어 협력에서 가장 민감한 부분이자 중요한 사항은 미국과 러시아 모두 각자의 요격미사일을 배치하도록 하는 것이다. 이러한 배치는 양국의 핵무기 비축과 관련하여 존재하는 전략적 균형을 깨뜨리는 것이 아니다. 이것의 의도는 말하자면 러시아를 자극하여 러시아가 미사일방어 자체를 위협으로 간주, 미국에 대한 억지능력을 증강하는 상황을 방지함과 동시에 이란 미사일에 대한 효과적인 방어능력을 구축하자는 것이다. 이러한 목표는 EASI 위원회 미사일방어 실무단에서 논의한 결과 충분히 달성할 수 있다고 평가되었다. 따라서 미국은 미사일 방어체계를 장착한 이지스

함을 지중해와 북해 인근에 배치하여 해당 지역에서 표적들을 요격할 수 있겠고, 러시아는 S-400 및 S-500 체계를 탑재한 함선을 흑해, 발트해, 바렌츠해, 그리고 백해 등에 배치할 수 있겠다.

시간이 지남에 따라 미-러 간의 미사일방어 협력은 양국의 전략적 관계를 근본적으로 변화시킬 것이다. 간단히 말해서 양국이 각자의 핵무기 비축량을 장기간 동안 유지하면서 제3국으로부터의 미사일 위협에 대응하기 위해 긴밀히 협력한다는 것은 불가능하다. 서로가 양국의 국가안보 전략과 군사 교리에 대해 “속속들이” 이해할 수 있게 된다면 냉전시대 전략과 교리의 잔재를 완전히 씻어 낼 수 있을 것이다. 1990년대 당시 발칸반도 평화유지 활동을 중요도가 낮고 수직적인 성격이라는 이유(또한 러시아인들의 악감정으로 인해)로 러시아가 참여를 거부했던 것과는 달리 미사일방어 협력은 전략적이고 동등한 것이다.

미-러 간의 유럽 미사일방어 협력방안은 러시아와 서방세력 간의 관계를 비무장화하고 많은 분야에서 발전의 길을 열어줄 것이다. 현재의 개선된 상황 속에서는 비전략적 핵무기 및 전략적 비핵화에 관한 생산적인 협상 또한 가능할 것이다. 이는 미-러 간 향후 전략 핵무기 감축을 위한 새로운 합의서를 체결하도록 하는 길까지 열어줄 수 있을 것이다.

IV 러시아 안보의 주요 과제

또 다른 우발사태인 국지적·지역적 전쟁 문제를 자세히 들여다 보면 러시아의 안보 상황이 과거에 비해 더욱 안정적이기도 하고 불안정적이기도 하다는 것을 알 수 있다. 긍정적인 측면에서 보면, 유럽과 아시아에서 지역전이 발생하여 러시아를 연계시킬 수 있는 가능성은 미-러 간 핵 교류를 진행하는 것만큼 가능성이 낮다고 할 수 있다. 영국, 프랑스, 독일 등 대부분의 주요 나토 국가들은 이미 러시아와 안정적이고 전반적으로 비무장화된 관계를 유지하고 있다. 과거 러시아를 상대로 전쟁을 치른 경험이 있는 국가들 중, 핀란드는 사실상 비무장화하였고, 터키 또한 같은 방향으로 가는

과정 중에 있다. 러시아-폴란드 간의 화해 절차 또한 어렵지만 진행되고 있다. 이제 남은 국가는 발트해 국가들과 그루지야이다. 하지만 발트해 국가들은 나토와 유럽연합의 회원국이고 이들과 러시아가 군사적으로 충돌할 가능성은 매우 낮다. 미국의 우방인 그루지야의 경우는 여전히 2008년 전쟁의 영향이 남아 있지만 그루지야 국내의 변화하는 상황으로 인해 러시아와의 재차 충돌로 이어지기는 어려운 상황이다. 또한 중요하게도, 우크라이나는 비동맹원칙을 채택하고 있어 적어도 현재로서는 러시아 측의 우려를 덜어주고 있다. 나토의 동유럽국가에 대한 미사일방어 추진 확대와 함께, 미국, 유럽, 러시아는 유럽-대서양 지역에서 안보 공동체를 형성하는 방향으로 나갈 준비를 해야 한다. 그리고 이는 러시아뿐만 아니라, 미국 및 유럽 국가들의 안보정책이 추구하는 주요 목표가 되어야 한다.

아시아에서는 1960~80년대의 충돌로 손상된 중국과의 관계가 정상화되었다. 양국은 곤란한 국경 문제를 해결하고 국제적·지역적 수준에서의 전략 파트너십을 체결하였다. 중국이 지속적으로 군사력을 확충할 가능성이 있지만 러시아와 중국 정부에게는 서로 선린 관계를 유지하고 파트너십을 발전하는 것 외에는 더 나은 대안이 없다. 러시아에게 있어 최악의 상황은 중국이 적대적으로 변모하는 것이고 마찬가지로 중국에게도 “북쪽의 위협”이 재발하는 것은 중국의 전략적 입지를 매우 약화시키는 것이다. 일본과의 관계는 남쿠릴열도를 둘러싼 분쟁에도 불구하고 이를 해결할 적절한 타협점만 찾을 수 있다면 유럽 국가들과 마찬가지로 비무장화될 수 있을 것이다. 그에 반하여 한국과의 관계는 문제가 없다고 할 수 있다. 더욱이 러시아 정부는 한국을 매우 소중한 경제 파트너라고 인식하고 있다. 향후 한국 주도의 한반도 통일이 이루어진다면 러시아 정부 입장에서는 지정학적으로 안정성을 확보하고 경제적으로는 좋은 전망을 갖는다고 인식할 것이다. 태평양 지역의 경우 러시아는 미국을 지역 안정을 위한 주요 요소라고 인식한다.

부정적인 측면에서 보면, 러시아는 남쪽으로 눈을 돌려 북코카서스 국경지대에서의 끊임없는 분쟁과 아프가니스탄과 중동아시아까지 이르는 남쪽 측면지역의 혼란을 주목해야 한다. 이 지역은 1970년 후반부터 러시아 군이 많은 분쟁을 치러 왔던 곳이며 평화와 안정과는 거리가 먼 곳이다. 러시아는 집단안보조약기구(CSTO)를 활성화하고 해당 지역에서 동맹국들과의 교류를 증진하는 등의 안보 노력을 주도해야 하며, 카자흐스탄과 같은 명목상의 동맹국들과의 협력, 중국, 인도, 상하이협력기구 소속 국가

및 해당 지역 내 기타 국가와의 교류, 미국과의 절차 발전 등에 대한 방안을 강구해야 한다. 이와 같은 노력들은 모두 군사·안보 범주에 속하는 것이며 아직 제대로 된 기틀이 마련되지 않은 부분이 많다.

V 결론

이와 같은 상황을 종합적으로 고려하면 현재 러시아 군은 방향설정도 없이 마치 머리는 없고 몸만 있는 군 개혁과 국방 현대화를 진행하고 있는 것으로 보인다. 이제는 이미 진행 중인 관리, 재정, 산업 부문에 더하여 전략적 측면을 제시하는 진지한 국가적 토론이 필요한 시점이다. 러시아 전략가들은 막중한 임무를 떠맡고 있으며 이는 러시아의 사고방식이 얼마만큼 성숙하고 현대적으로 변모하였는지 평가하는 시험이 될 것이다.

RUSSIA'S MILITARY MODERNIZATION : IN SEARCH OF A 21ST CENTURY STRATEGY

Dmitri Trenin || Director, Carnegie Moscow Center

In 2008, after nearly two decades of neglect, the Russian leadership finally embarked on a military reform. The decision must have been taken the year before, with the very unusual appointment of Anatoly Serdyukov, a man without any previous experience with the defense establishment, and it was made public in the wake of the five-day war in South Ossetia, which, although resulting in Russia's resounding victory over Georgian forces, exposed a number of glaring weaknesses of the Russian military.

In 2011 the Kremlin decided on a large-scale effort to modernize the Russian defense industry. It allocated 20 trillion rubles, or about 700 billion dollars, over a decade to upgrade the weapons and equipment which the Russian military is using. This effort amounts to a significant change in the Russian government's priorities since the break-up of the Soviet Union. This is material proof that military issues are no longer on Moscow's backburner: they are very much front and center. Inevitably, they also require a major commitment of financial resources.

In the four years, the military reform effort, led by Defense Minister Serdyukov with full support from Vladimir Putin, has brought some significant results.

- The oversize officer corps was trimmed by over 100,000, and the remaining officers' pay was doubled or tripled, to make it competitive with the civilian sector;
- the many cadre units (10~20% of assigned strength), and the under strength units (50% of their assigned personnel), which only made sense for a WWII-style mobilization effort, were dismantled, alongside many military bases, storage facilities, and compounds;
- a new command structure of the Russian Armed Forces came into being, based on three levels: the General Staff of the Armed Forces – Regional Commands – brigades, as applied to the Land Forces, and equivalent in the other services;
- large-scale military exercises were resumed, all the way up to the strategic level;
- outsourcing is being practiced for the first time, with military personnel being relieved of non-military chores;
- political control over the military was strengthened, with the appointment of the first fully civilian Minister of Defense and with the Chief of the General Staff being made fully subordinate to him.

The impetus for the reform has been a long-overdue basic reassessment by the Kremlin of Russia's strategic situation. Two decades after the end of the Cold War, a large-scale conflict against several major adversaries, formerly the principal mission of the armed forces, has been deprioritized as far less probable than ever before. Instead, local wars along the perimeter of Russia's borders – like the Chechen campaigns of the 1990s and the early 2000s or the 2008 war against Georgia – were elevated to being the principal likely form of military engagement. This made it possible to do away with the traditional mobilization system, which had been the backbone of the Russian defense establishment for the last 130 years.

The central idea of the reform has been to optimize the bloated military establishment and to increase the availability of military tools to the political leadership. In 2006, President Putin complained that during the Chechen war only 65,000 servicemen – out of the Armed forces’ nominal strength of 1,400,000 – could be used against the terrorist threat in the North Caucasus. In 2008, only 13% of the Army units were in a permanent state of readiness. The ambition – now being implemented – is to build a standing military force which would be more mobile and permanently ready for engagement. The notion of combat readiness has also been revised: from 24 hours from the moment of notification to embarkation onto the area of engagement to just one hour.

Another major axis of the reform has been improving the command and control structure. No longer fixated on managing mobilization, the new structure has to focus on operations. Thus, two out of five levels of command – division and regiment – were dismantled, with divisions reformed into brigades, consisting of battalions. The military districts – whose number shrank from six to four – kept the title, but were actually transformed into joint strategic commands, responsible for all the military forces within their geographical area. This resulted in scrapping 91% of Army units and just under 50% of all units in the Air Force and the Navy. New units, moreover, are to use similar standardized types of weapons and equipment.

Key to the reform is the personnel factor. The surplus of senior officers has been reduced, from 335,000 commissioned officers in 2008 to 220,000. The number of contracted men (NCOs and volunteer soldiers) is to go up from 180,000 in 2012 to 425,000 in 2017, and the number of conscripts, historically the mainstay of the Russian military, is to decrease to 270,000

by 2017. The pay and benefits of the military personnel and the pensions of retired military officers have been more than doubled, in order to attract better quality people to the Armed Forces and to ensure reenlistment of the contracted servicemen.

Finally, the arms, ammunition and equipment of the Armed Forces are to be radically upgraded. The share of modern weapons, estimated at 30% now, should grow to 70% by 2020 – even if the definition of what constitutes “modern” is not clear. The share of materiel acquisition in the defense budget, which stood at 20% in 2000, is set to grow from 38% in 2010 to 59% in 2013. Russia’s defense expenditure is expected to rise from 2.9% of GDP in 2011 to 3.9% in 2014. Even though, in dollar terms, the Russian defense budget is a puny 7% of that of the United States’, Russia’s defense burden will rise considerably: in 2014, according to SIPRI, which usually adds 1.5% to official Russian figures, Russia will surpass the current U.S. level of 4.8% of GDP. This is much higher than in Europe or in China.

The Russian defense industry, which employs about 1.5 million people, or 1.5% of the workforce, faces a similar prospect of restructuring, consolidation and reform, in order to be able to rise to the Kremlin’s new demands. As with the Ministry of Defense, a new energetic person, Dmitry Rogozin, an ambitious politician and a former ambassador to NATO, was selected by the Kremlin in 2011 to oversee the transition to a more modern defense industrial complex. Vladimir Putin, re-elected President in 2012, vowed to make the defense industry the locomotive of his policy of “re-industrialization”. So far, little progress has been made, but the problems of the industry have been thrown into sharper relief.

The main issues include ageing workforce, production and plant the

archaic outsize structure (over 1,700 companies in 2010, with even the largest among them rather small by international standards) a general lack of competitiveness and transparency; widespread and pervasive corruption; opaque and unrealistic pricing mechanisms; a stark divide between the export-oriented enterprises, which are thriving, and those which produce for the domestic market, which are depressed; ineffective research and development practices; too little foreign cooperation; and chronic underfunding of the industry in the past two decades.

The Kremlin has strengthened the role of the MOD vis-à-vis the defense companies, and laid down its military-technological priorities to 2020. These include: strategic systems providing nuclear deterrence; airspace defense systems communications, automated command, control, intelligence equipment; electronic counter-measures; drones; unmanned strike systems; transport aircraft; naval systems, especially for the Arctic and the Pacific; precision-guided weapons systems and munitions; individual soldier's protection means.

The Kremlin's will to spend the promised funds on military modernization is there, despite the slower economic growth in the country (between 3-4% p.a. in the medium term) and tight budget constraints caused by stagnating or falling oil prices. It is not clear, however, whether the defense industry can be optimized and restructured in the next few years, even to the same degree as the Armed Forces. What is absolutely clear though is that without such optimization and restructuring the significant funds allocated for national defense will likely be misappropriated or spent on the things which will not increase Russia's military capabilities.

There is another cause for concern. What is conspicuously missing in the

Russian reform efforts is an attempt to come up with a new security and defense “software”. True, the Presidential decree of May 7, 2012, mandates the establishment of a “qualitatively new system of analysis and strategic planning for national defense for the next 30–50 years” which should provide guidance to the national weapons program. This is a commendable step, which foresees integrating analysis and forecasting of global and national trends in economics, domestic, foreign and security policy, science and technology, demographics and other key areas. Underlying such analysis, moreover, there needs to be a 21st century worldview, free from the stereotypes of the Cold War era.

Russia’s new military doctrine was formally adopted in 2010. It all but eschews the notion of a large-scale war which for many decades formed the centerpiece of Russian military thinking. This is a huge step forward, unblocking the path toward reform and military modernization. Instead of major wars, the focus in the doctrine is on nuclear deterrence of the principal powers – primarily the United States – and on local and regional contingencies. Deterrence, one has to admit, continues to be the centerpiece of strategic stability in the world, particularly among the leading nuclear powers. Deterrence, however, plays a very different role now, two decades after the Cold War. A U.S.–Russian nuclear exchange in the 21st century is a remotest possibility. There is room, however, for further efforts to enhance predictability and security in the nuclear area. Strategic relations between Russia and the United States need to be stabilized by means of trust building through strategic cooperation, e.g. on missile defenses in Europe.

The issue of missile defense in Europe represents both a challenge and an opportunity for the medium-term future. The challenge is that, in case there is no agreement on the issue, U.S.–Russian relations can seriously

deteriorate over time, making the global strategic balance less stable. The opportunity lies in developing a formula for cooperation on missile defenses which would not affect either the U.S. interest of protecting its assets and allies against a possible Iranian missile strike, or the security of Russia's nuclear deterrent. Such cooperation would be a true game-changer, capable of transforming U.S.-Russian strategic relations from their present post-adversarial and wary state toward a more collaborative and non-adversarial formula for the future. This, too, would affect the global standing of both Russia and the United States in a changing world, and in a positive way.

The United States and its NATO allies have made a decision recently to begin deploying missile defenses in Europe. The Russian Federation has been invited to participate in this NATO program. For its part, Moscow has expressed concern over the advanced stages of the NATO program which provide for deployment of interceptors (SM3 Block IIB) which, the Russians claim, can shoot down some of Russia's own intercontinental ballistic missiles (ICBMs). To guard against that, Moscow has proposed a joint dual-key missile defense system in Europe or, failing that, concluding a legally binding agreement with the United States making sure that its missile defenses in Europe shall not have the capacity against the Russian strategic arsenal. This Russian proposal, however, is unacceptable to the United States.

Yet, there is both a need and a way to try to square the circle. The principal reason for seeking a solution to the issue should be the realization that the absence of an agreement would leave the United States and Russia materially worse off and, conversely, that their cooperation would add to each party's national security. Thus, the issue is either a strategic game-changer or a game-breaker between Washington and Moscow. The basis

for cooperation lies in both sides' sincere concern about strategic stability in the world, which is founded on secure nuclear deterrence vis-à-vis each other and on the ability to neutralize nuclear and missile threats coming from third parties. What logically follows is that the United States should be interested in the Russian leadership' s continued confidence in the integrity of its deterrence, and that the Russian Federation should be concerned about the evolution of the Iranian nuclear and missile programs.

Possible U.S./NATO-Russian cooperation on missile defense in Europe can be based on the following principles: (1)addressing the evolving third-country threat from medium-range and intermediate-range ballistic missiles banned under the 1987 U.S.-Soviet INF Treaty; (2)enhancing the effectiveness of each country' s response to this threat through mutual cooperative efforts; (3)using cooperation in the missile defense area to gradually develop an essentially non-adversarial, collaborative strategic relationship between the United States and Russia, and thus creating a security community in the Euro-Atlantic region. These principles have been developed by the international Commission on Euro-Atlantic Security (EASI Commission) initiated by the Carnegie Endowment.

A cooperative arrangement built on such a foundation would include the following key elements: (1)interaction between national/alliance missile defense systems: a joint missile defense system is unrealistic at this point, and each sovereign partner remains fully responsible for its own security and defense; (2)integration of the parties' information assets, providing for real-time exchange of data on third-country missile activity; (3)functioning operational protocols allowing parties to intercept missiles flying over their territory but aimed at the territory of another party; (4)appropriate technology transfers to make U.S. and Russian missile defense systems

compatible; (5)codification of the above arrangements in the form of an executive agreement.

The elements of the proposed arrangement cannot be implemented immediately. Rather, the United States and Russia should begin by creating cooperation centers for pooling and sharing information and data from satellites and radars operating in real time to provide a common notification about missile attack. Such centers should be established in a NATO country (e.g., Poland or Belgium) and in Russia.

Each should be staffed by NATO and Russian officers working side by side to form a uniform picture of missile activity in the relevant area. In essence, creation of such centers would implement the U.S.–Russian agreement reached already in 2000 on early warning data exchange, this time on a higher level of interaction and integration. While the Moscow center would focus on integrating dataand forming a comprehensive picture, the center in a NATO country would focus on coordinating response to actual missile threats. For this purpose, joint U.S.–Russian command–staff exercises on ballistic missile defense, which were resumed in March 2012, should be expanded in scope to include defense against medium– and intermediate–range missiles.

The essential and most sensitive part of any arrangement on cooperative missile defenses in Europe is making sure that as both the United States and Russia deploy their interceptors, these deployments do not impair the strategic balance existing between the two countries’ nuclear weapons arsenals. The idea is, in a nutshell, to build effective defenses against Iranian missiles without provoking Russia into considering those defenses as a threat to itself, and responding by raising its deterrence capability vis–

à-vis the United States. As discussions within the EASI Commission Working Group on Missile Defense have demonstrated, meeting that objective is thoroughly feasible. Thus, U.S. naval ships carrying Aegis missile defense systems would be capable of engaging their targets from their deployment areas in the Mediterranean and in the North Sea. Russian naval ships with S-400 and S-500 systems would be deployed in the Black, Baltic, Barents and White Seas.

Missile defense cooperation between Russia and the United States would over time lead to a fundamental transformation of the two countries' strategic relations. It is simply impossible, in the long term, to cooperate closely on addressing missile threats from third parties while keeping vast nuclear weapons arsenals pointed at each other. Much better understanding – “from the inside” – of each partner's national security strategy and its military doctrine would result in fully cleansing the legacy of the Cold War from those strategies and doctrines. Cooperation on missile defense would be truly strategic and equal – unlike joint peacekeeping experience in the Balkans in the 1990s, which was dismissed at the time as both peripheral and hierarchical (and naturally resented by the Russians as such).

A cooperative U.S.-Russian missile defense arrangement for Europe would essentially demilitarize Russia's relations with the West and unblock progress in a number of areas. In this improved atmosphere, productive negotiations on non-strategic nuclear weapons and on strategic non-nuclear ones would become possible. This, in turn, would open the way to new U.S.-Russian agreements on further reductions of their strategic nuclear weapons arsenals.

A closer look at the other two contingencies – regional and local wars –

reveals that Russia's security situation is both more and less stable than ever before. On the positive side, regional wars in Europe and Asia threatening to draw Russia in are almost as improbable as a Russian-American nuclear exchange. Most NATO countries, including the leading ones, Britain, France and Germany, maintain stable and generally demilitarized ties with Russia. Of the neighbors, with whom Russia fought wars in the past, relations with Finland are also de facto demilitarized, and those with Turkey are being transformed in the same direction. The Russo-Polish reconciliation process, difficult as it is, is under way. What remains is essentially the Baltic States and Georgia. The former, however, are members of NATO and the European Union, and a military conflict with them looks highly unlikely. As to Georgia, a friend of the United States, the impact of the 2008 war remains a deterrent; moreover, domestic changes in Georgia do not lead toward renewed confrontation with Russia. Very importantly, Ukraine has opted for a non-bloc status, putting to rest Russian fears – at least for now. With NATO's further eastern enlargement a non-issue and the missile defense settlement in the works, America, Europe and Russia would be ready to move toward forming a security community in the Euro-Atlantic, which should be a prime goal of Russia's, as well as America's and European countries' security policy.

In Asia, relations with China, marred by confrontation from the 1960s through the 1980s, have been normalized. The two countries solved their thorny border issue and have engaged in a strategic partnership at global and regional levels. China's military might continues to grow, but for Moscow as well as Beijing, keeping their good-neighborly relations intact and developing partnership has no good alternative. A hostile China is Russia's worst nightmare; by the same token, a revived "threat from the north" makes China's strategic position highly vulnerable. Russia's relations with Japan,

despite the dispute over the South Kuril Islands, can become as demilitarized as those with Europe – if only an appropriate compromise solution to the territorial issue is found. By contrast, relations with the Republic of Korea are essentially non-problematic. Moscow, moreover, views Seoul as a highly valuable economic partner. In future, Seoul-led reunification re-unification of Korea is considered in Moscow to be both geopolitically stabilizing and economically promising. Looking across the Pacific, Russia views the United States as a major element of regional stability.

On the negative side, Russia has to look south, to the restless borderland of the North Caucasus and the turbulent southern flanks all the way to Afghanistan and the Middle East. This is an area where Russian forces have had to engage in a number of conflicts since the late 1970s and where peace and stability are a long way off. Russia needs to lead in some security efforts, such as re-energizing the Collective Security Treaty Organization, and engaging with its allies in the region; it has to find ways to cooperate with its nominal allies in the region, such as Kazakhstan; to engage China, India and other regional powers within and outside the Shanghai Cooperation Organization; and to develop a modus operandi with the United States. All these efforts have a clear military security dimension, and much of the groundwork is yet to be laid.

This creates a situation in which Russian military reform and defense modernization appears an effort to create a body without a brain yet to direct its activities. A serious national debate is in order to add a truly strategic dimension to the managerial, financial and industrial ones already being constructed. The Russian strategic community faces a crucial task, which will be a test of how mature and how modern its thinking has become.

미국의 역내 존속과 유럽의 개입 도모 : 아태 지역의 전략적 영향력 행사를 위한 스마트 국방

Heiko Borchert¹ || Sandfire AG 대표이사, 안보 국방 컨설턴트

목 차

- I. 서 론
- II. 아태 지역의 안보와 방위 과제
- III. 유럽의 안보 및 방위 : 현명한 대안 모색
- IV. 아태 지역과 유럽 · 미국의 스마트 국방 협력
- V. 결 론

I 서 론

방위와 안보 부문에서, 유럽연합 회원국과 아태 지역 간의 격차가 더 커질 가능성은

1) 헤이코 보르체르트 박사(Dr. Heiko Borchert)는 스위스 안보 및 국방 컨설턴트 회사 Sandfire AG의 대표이사를 역임하고 있다. 그는 헤이그 전략연구센터 특임전문가이며, '포괄적 접근(Comprehensive Approach)의 이론 및 시행' 책 시리즈의 공동편집자이자, Zeitschrift für Aussen- und Sicherheitspolitik 잡지 편집위원이다. 스위스 주재 St. Gallen 대학교에서 국제학, 경영학, 법학, 경제학을 공부하였으며, 박사학위를 취득하였다. 그의 주 분야는 안보, 공/사 안보협력, 주요기반시설 보호, 에너지 안보, 해양 안보, 사이버 안보, 국방기획, 및 안보부문 변화 등이다.

희박하다. 지난 몇십 년간 최악의 정치·경제 위기를 겪은 유럽연합 회원국은 내부 안정화를 위해 관심을 유럽연합 내부로 전환하였다. 유럽연합 회원국은 위기의 여파를 수습하기 위해, 특히, 국방 예산을 대폭 삭감하는 노력을 하고 있다. 이에 대해, 곧 임기가 끝나는 군사위원회 의장인 하칸 사이렌(Hakan Syren) 장군은 “소외된 유럽이란, 위기가 아니라 현실이다.”라고 경고했다.² 그 결과, 1990년대 발칸 반도의 국제 위기관리 운영 기간 동안 부각된 유럽 국방력의 부족은 그 이후로 더욱 심화되었고 유럽이 여전히 이를 해결하기 위해 애쓰고 있다는 것은 놀라운 사실이 아니다. 이렇듯 분명한 문제에도 불구하고, 유럽연합 회원국은 다른 지역에 비해 전략지정학적으로 비교적 평온한 국면을 맞고 있다.

반면, 아태 지역은 다른 이유로 세계의 이목을 끌고 있다. 경제 성장은 이 지역을 세계의 새로운 지리 경제적 중심으로 변모시켰다. 호주머니를 꽉 채운 아태 지역의 최대 국방비 지출 국가의 국방비는 2012년 말 유럽 전체의 국방비를 곧 넘어설 전망이다.³ 비록 무역에 있어서의 상호관계 때문에 주요 무역 상대국에 영향을 주는 문제로부터 안전할 수는 없었지만, 아태 지역 국가들은 대체로 미국과 유럽연합의 경제·재정 위기의 영향을 받지 않았다.

아태 지역에는 여전히 국가적 적대감과 지역적 긴장감, 국수주의 정책 등이 만연하며, 게다가 아태 지역의 여러 국가들은 주변국을 억지할 뿐만 아니라 공격적이고 어찌면 선제공격을 목적으로 군사력을 강화하고 있다.⁴ 그 결과, 아태 지역의 안보는 취약해 보이며, 헝클어진 깃털을 정리하기 위해서는 전반적인 안보의 틀을 마련해야 한다.

이와 같은 배경 하에서 얼핏 보면 유럽의 방위 협력 관련 경험이 아태 지역에 그다

2) Hakan Syren, “Facing realities – in search of a more European mindset”, Cyprus EU Presidency High Level Seminar에서 기조연설, 브뤼셀, 2012년 9월 19일, p.3, <http://www.consilium.europa.eu/media/1749978/ceumc_keynote_speech_cyprus_presid_seminar_19_sep2012_2012.pdf>

3) <<http://www.iiss.org/publications/military-balance/the-military-balance-2012/press-statement/>> (accessed 16 October 2012). 현 아시아 국방지출패턴 세부 사항 평가는 다음을 참조: Joachim Hofbauer, Priscilla Hermann, and Sneha Raghavan, Asian Defense Spending, 2000–2011 (Washington, DC: CSIS, 2012).

4) Military Balance 2012 (London: Routledge, 2012), pp.205~208.

지 적용되지 않는 것으로 보이지만 그렇지 않다. 의심할 여지없이, 유럽연합과 나토 국가는 심각한 경제·재정 상황을 감안하여 통합과 공유, 역할 특화에 대해 논의하고 있다. 그러나 아태 지역의 입장에서 볼 때, 나토가 통합과 공유, 역할 특화라고 명명한 스마트 국방이라는 개념에 대한 전략적 근거가 주는 인식은 여러 국가를 공동의 협력 관계로 묶어 놓는 것이다. 유럽은 빈약한 국방·안보 역량을 지원하는 비용을 함께 부담하기 위해 통합과 공유에 대해 논의하고 있다. 그러나 아태 지역 측면에서, 스마트 국방은 외부 국가가 아태 지역에 지속적으로 관여하거나 새로 관여하기 위한 수단으로 인식할 수 있다. 세계 경제 강국으로 떠오르고 있는 아태 지역 국가들이 점차 중요해지고 있는 타 지역의 문제를 해결하기 위해 아태 지역의 안정을 도모하고 공동의 활동을 조직하는 것은 중요하다고 할 수 있다. 유럽연합과 나토 국가는 스마트 국방을 “내부자”끼리 논의하는 반면, 아태 지역 국가는 기회를 놓치지 않고 스마트 국방을 유럽 국가와 태평양 국가와 같은 “외부자”들과의 결속을 다지는 데 활용할 수도 있다. 이와 같은 의미에서 특히 이 두 지역 내에서 미국의 역할이 중요하다. 유럽이 미국의 주요 관심 국가의 파트너로 계속 남고자 한다면, 아시아 내에서 미국의 중심 역할이 유럽에게 궁극적이며 전략적인 자극임을 깨닫고 아태 지역과의 통합과 공유에 참여해야 한다. 아태 지역 국가는 미국을 이 지역의 균형을 궁극적으로 조절해주는 국가로서 유지시키고 통합과 공유를 쓸모 있는 방법으로 여기며, 미국 정부와의 관계를 강화할 수도 있다. 그 결과, 유럽연합과 아태 지역 국가 모두 상호 협력과 미국과의 협력을 증진시키는 방법인 통합과 공유에 관심을 가질 수도 있다.

II 아태 지역의 안보와 방위 과제

유럽은 아태 지역에 최소 3가지 매우 중요한 전략적 이해관계를 갖고 있다. 첫째, 아태 지역은 중요한 무역 상대국이다. 작년, 유럽 연합의 27개국과 아시아-유럽 정상 회의(ASEM) 회원국에 수출한 제품의 총액은 3,300억 유로(유럽 연합 27개국 수출 중 21.6%)에 달하고 수입한 제품의 총액은 5,320억 유로(유럽 연합 27개국 수입 중

31.6%)이다.⁵ 양자 간 무역 관계를 좀 더 자세히 살펴보면, 유럽 연합 27개국이 아시아 품목 중 첨단기술 제품에 상당히 의존하고 있음을 알 수 있다. 예를 들어, 아시아-유럽 정상회의 회원국은 모든 유럽 연합의 27개국의 집적 회로 및 전자 부품 수입 중 80% 이상, 유럽연합의 전자정보처리 및 사무실용 비품 수입 중 78%를 차지한다.⁶ 또한, 중국과 인도, 인도네시아, 일본, 싱가포르, 한국 중에는 유럽 연합의 주요 원자재(예 : 게르마늄, 인듐, 마그네슘, 희토류 원소, 탄탈륨, 바나듐) 수입 총액의 70% 이상을 차지하는 국가도 있는 등 ASEM 회원국은 중요한 원자재 공급 국가이다.⁷

둘째, 아태 지역과의 무역 관계를 볼 때, 유럽은 아태 지역과의 시장 및 운송 통로를 분명히 이용하고자 하는 전략적 이해관계를 갖고 있다. 그러나 21세기에 소위 글로벌 코먼즈(Global Commons, 국제공공재)로 여기는 해상 및 기타 영역(예 : 공해, 우주, 사이버 공간)에 대한 접근에 있어 점차 경쟁이 더욱 심화될 것이라는 우려가 최근 들어 점차 늘고 있다. 결국, 아태 지역이 유럽의 다른 두 가지 이해관계에 상당한 영향을 준다는 측면에서 보면 아태 지역 내 불안정으로 이어지는 위협이 바로 궁극적인 위협 시나리오라고 할 수 있다.

서로 다른 동향은 지역 강국 간의 관계를 심각히 왜곡하고 그 결과 유럽의 이해관계에도 영향을 줄 가능성이 있다. 유럽의 입장에서 볼 때, 다음 5가지 동향이 가장 중요한 것으로 보인다:

1. 변화하는 전략 지정학적 · 지리 경제적 영향권

아태 지역의 전략지정학 · 지리 경제적 영향권의 재설정 은 점점 확대되는 이 지역의

5) 1996도에 설립된, ASEM은 ASEAN국가 중국, 인도, 일본, 몽골, 파키스탄, 한국을 포함하는 비공식 협력절차이다.

6) 유럽연합 무역 집행기관 총국(Directorate General for Trade of the European Commission)에서 제공한 통계, <http://trade.ec.europa.eu/doclib/docs/2006/september/tradoc_113472.pdf> (2012년 10월 17일 접속).

7) EU 주요 원자재. 주요 원자재 정의 관련 Ad-hoc Working Group보고서(Brussels: European Commission, 2010), pp.77~81.

경제적 영향과 함께 진행된다. <표 1>에서 보여주듯이, 중국-미국 간 무역 관계는 이 지역에서 가장 중요하다. 그러나 총계를 보면, 유럽연합 27개 회원국과의 무역 총액이 7억 7,543만 3백유로(2010)에 달하므로 유럽연합 27개 회원국이 아태 지역에서 가장 중요한 무역 상대국이다.⁸ 그러나 이는 현 상황의 단면만을 보여주는 결과일 뿐이다. 미국 시티은행이 발표한 향후 무역 전망에 따르면, 중국과 인도의 성장은 근본적으로 40년 후의 무역거래 형태를 바꿀 것이다.

중국과 인도는 2050년까지 세계 최대 무역국가가 될 것으로 전망된다. 그 뿐만 아니라, 양국 총합 무역 점유율 27.2%는 향후 미국과 독일의 무역 점유율을 합한 것보다 약 3배나 많을 것이며 이는 무역 통로에 영향을 줄 것이다. 2010년 유럽 내 무역은 세계 무역의 19.9%를 차지하는 수준으로 신흥 아시아 국가와 서유럽뿐만 아니라 선진 및 신흥 아시아 국가 간 무역보다도 적었다. 2050년까지 아시아는 전반적인 경제적 비중의 중심을 차지할 것이다. 선진 및 신흥 아시아 국가 간 무역은 세계 무역의 14.9%, 그 뒤를 이어, 신흥 아시아 국가 간 무역은 12.5%, 신흥 아시아 국가와 서유럽 간 무역은 8.3%를 차지한다. 흥미롭게도, 2010년 서유럽과 북미 간 무역은 세계 무역의 5.8%를 차지했고, 2050년에는 세계 10대 무역 국가 명단에도 포함되지 않을 것이다.⁹

적어도 지금까지는, 무역 관계가 안보 관계의 강력한 지표였다. 그렇기 때문에 향후 무역 통로의 새로운 형태가 아태 지역과 그 이외 지역의 안보 관계에 어떤 영향을 줄 것인가는 중대한 문제이다.¹⁰ 시티은행 조사에 따르면, 미국과 유럽이 아태 지역과 관계를 유지하기 위해서는, 지금이 바로 무역 관계를 안보 협력을 개선하기 위한 도구로 사용해야 할 때이다.

8) 미국과의 무역은 6,791억 9천만 유로이었고, 중국과의 무역은 6,097억 3천2백만 유로에 달했다. 참조: <http://trade.ec.europa.eu/doclib/docs/2006/september/tradoc_113472.pdf>

9) Willem Buiter and Ebrahim Rhabari, Trade Transformed. The Emerging New Corridors of Trade Power (New York: Citi, 2011), pp.22~24.

10) 세부사항은 possible future development paths을 참조. 참조 : Avery Goldstein and Edward D. Mansfield, eds., The Nexus of Economics, Security, and International Relations in East Asia (Stanford: Stanford University Press, 2012).

표 1: 일부 아태 지역 국가의 주요 무역 상대국(2011년, 총 수출입의 %)

국가	무역 상대국 순위											
	1		2		3		4					
	수입	수출	수입	수출	수입	수출	수입	수출	수입	수출	수입	수출
IND	PRC 12.3	UAE 12.4	UAE 8.8	USA 10.7	CHE 6.3	PRC 7.9	USA 5.8	HKG 4.3				
IDN	PRC 18.7	PRC 13.3	JPN 14.1	JPN 11.3	SGP 7.5	USA 9.7	USA 7.8	IND 8.2				
JAP	PRC 21.5	PRC 19.7	USA 8.7	USA 15.3	AUS 6.6	ROK 8.0	SAU 5.9	TWA 6.2				
MYS	JPN 12.6	SGP 13.4	PRC 12.6	PRC 12.6	USA 10.7	JPN 10.4	THA 6.2	USA 9.5				
PRC	JPN 11.2	USA 17.1	ROK 9.3	HKG 14.1	TWA 7.2	JPN 7.8	USA 7.0	ROK 4.4				
PHL	JPN 11.0	JPN 18.5	USA 10.9	USA 14.8	SGP 8.1	PRC 12.7	ROK 7.3	SGP 8.9				
SGP	MYS 10.7	MYS 12.2	USA 10.7	HKG 11.0	PRC 10.3	PRC 10.4	JPN 7.2	IDN 10.5				
ROK	PRC 16.5	PRC 24.2	JPN 13.0	USA 10.7	USA 8.5	JPN 7.1	SAU 7.0	HKG 5.6				
THA	JPN 20.8	PRC 11.0	PRC 13.3	JPN 10.5	MYS 5.9	USA 10.4	USA 5.9	HKG 6.7				
TWN	JPN 18.6	PRC 27.2	PRC 12.8	HKG 13.0	USA 9.2	USA 11.8	ROK 6.3	JPN 5.9				
VNM	PRC 23.6	PRC 11.1	ROK 13.2	USA 10.9	JPN 10.4	JPN 10.8	TWN 8.6	ROK 4.7				

국가 코드: AUS 호주, CHE 스위스, HKG 홍콩, IDN 인도네시아, IND 인도, JPN 일본, MYS 말레이시아, PHL 필리핀, PRC 중국, ROK 한국, SAU 사우디아라비아, SGP 싱가포르, THA 태국, TWN 대만, UAE 아랍에미리트, USA 미국, VNM 베트남

출처 : <<http://www.gtai.de/GTAI/Navigation/DE/Trade/Maerkte/wirtschaftsklima.html>>

2. 접근 · 지역거부 문제(A2/AD)

국제 전략지정학 환경이 변화하면서, 글로벌 코먼즈의 자유를 위협에 빠뜨리는 발전은 세계 전역의 전략 공동체의 이목을 집중시켰다. 글로벌 코먼즈는 재화와 사람, 자원, 정보의 자유로운 소통을 위해 무엇보다 중요한 해양과 공해상, 우주, 사이버 공간을 모두 하나로 묶는다. 이러한 소통의 질과 방향에 영향을 줄 수 있는 국가가 영향력을 행사한다. 즉, 접근 · 지역 거부 문제(A2AD)가 방해받지 않는 글로벌 코먼즈의 적용과 관련이 있기 때문에, 접근 · 지역 거부 문제가 전략적으로 중요하다는 것을 알 수 있다.¹¹

11) 비슷한 논의는 다음을 참조: Andrew F. Krepinevich, "Strategy in a Time of Austerity: Why the Pentagon Should Focus on Assuring Access," Foreign Affairs, Vol. 91, No. 6 (November-December 2012): 58-69; Caitlin Lee, "Planning beyond the pivot," Jane's Defence Weekly, 2012년 10월 31일, pp.26~32.

바로 지금, 아태 지역에서는 접근·지역 거부 문제가 대두되고 있다. 예를 들어, 동중국해의 해양 자원을 둘러싼 영유권 분쟁은 세계에서 가장 번화한 해상로 중 하나인 동중국해 해상 안정성을 위협하고 있다. 함정 공격용 미사일과 위성 공격력에 대한 중국의 투자 때문에 해상과 우주에서의 행동의 자유에 관해 우려가 제기되었다.¹² 또한, 환경 기준과 철광석 선적에 관해 중국과 브라질 간 빚어지고 있는 논쟁을 통해, 접근·지역 거부 문제가 단순히 군사적 문제가 아니라 무역 관계에도 영향을 줄 것임을 분명히 알 수 있다.¹³ 결국, 하드웨어와 소프트웨어 제품으로 인한 사이버 취약성은 양자 무역 관계와 주요 기반시설 보호에 대한 악영향 때문에 또 다른 논쟁거리를 제공한다.¹⁴

12) 미국 국방부 (OSD), Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012 (워싱턴DC: 국방부, 2012): 6~10. For a more detailed assessment, see also: Office of the Secretary of Defense, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011 (워싱턴DC: 국방부, 2011), pp.28~32.

13) Leslie Hook and Robert Wright, "China blocks Vale's large iron ore carriers," Financial Times, January 31, 2012, <http://www.ft.com/cms/s/0/b0fa84e6-4bf6-11e1-b1b5-00144feabdc0.html#axzz29ZJ49Xlk>; Fayen Wong and Jeb Blount, "Vale/China iron ore ship dispute deepens," Reuters, February 2, 2012, <http://mineweb.com/mineweb/view/mineweb/en/page504?oid=144539&sn=Detail&pid=504>; Alison Leung and Randy Fabi, "China's ban on Vale's iron ore carriers costs Chinese firms," Reuters, May 10, 2012, <http://www.mineweb.com/mineweb/view/mineweb/en/page504?oid=151218&sn=Detail> (accessed October 17, 2012).

14) Permanent Select Committee on Intelligence, Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunication Companies Huawei and ZTE (Washington, DC: U.S. House of Representatives, 2012); U.S.-China Economic and Security Review Commission, The National Security Implications of Investments and Products from the People's Republic of China in the Telecommunications Sector (Washington, DC: U.S.-China Economic and Security Review Commission, 2011).

3. 해상 불안정성과 불안감

국제 무역 형태의 변화로 인해 아태 지역의 해상로에 대한 확실한 접근이 점점 중요해질 것이다. 또한 접근·지역 거부 문제의 전략적 중요성도 강조된다. 요즘 세계에서 가장 변화한 항구는 아태 지역에 위치해 있다. 처리량을 기준으로, 세계 10대 컨테이너 부두 중 8개는 아태 지역 부두이다.¹⁵ 예를 들어, 독일의 경우, 인도와 중국, 일본과의 무역 중 60% 이상이 이 아태 지역의 부두에서 선적되므로 이 부두와 해당 해로에 대한 접근은 필수적이다.¹⁶

해양 자원에 대한 접근은 근접한 배타적 경제 수역(EEZ)을 둘러싼 영유권 분쟁을 촉발하는 또 다른 요소이다. 스프래틀리 군도와 파르셀 제도 주변에서는 주로 석유와 가스 자원 때문에 이해관계가 충돌한다. 추정치는 각기 다르지만 미국 에너지 정보기관은 중국과 기타 출처에 대해 인용하여 석유 매장량이 1m²당 최대 1,050억 배럴, 가스는 최대 900조 배럴에 달한다고 보고한다.¹⁷ 이 자원의 매장량이 실제로 입증될 경우, 이는 현재 쿠웨이트 석유와 카타르 가스 예비량과 거의 맞먹는다.¹⁸ 아태 지역의 석유 에너지에 대한 수요가 증가하면서, 에너지에 대한 접근을 두고 영유권 분쟁이 더욱 치열해지고 아태 지역이 불안정해질 것으로 예상된다.

15) Shanghai leads the list followed Singapore and Hong Kong. 참조: United Nations Conference on Trade and Development, Review of Maritime Transport (Geneva: UNCTAD, 2011), p.89.

16) 2010년, 독일은 중국과의 무역 1천300억 유로, 일본과 350억 유로, 인도와 150억 유로에 달했다. 참조: Jahresbericht 2011, Flottenkommando, Fakten und Zahlen zur maritimen Abhängigkeit der Bundesrepublik Deutschland (Glücksburg: Flottenkommando, 2011), p.95.

17) <http://www.eia.gov/countries/regions-topics.cfm?fips=SCS> (accessed October 17, 2012).

18) BP, BP Statistical Review of World Energy (London: BP, 2012), pp.6, 20.

4. 도시화

유엔의 예측에 따르면, 세계 인구는 오늘날 약 70억 명에서 2050년 약 91억 5천만 명으로 늘어날 것이다.¹⁹ 동시에, 도시와 지방의 인구 분포는 급격히 변할 것이다. 2009년 도시와 지방의 인구 분포는 거의 비슷했으나 2050년경 약 62억 9천만 명이 도심 지역에 거주하고, 28억 6천만 명이 지방에 거주할 것으로 예상된다. 2025년 세계 10대 도심지의 인구는 약 2억 3천만 명이 될 것이다. 이 중 7개 도시는 아태 지역 도시이다.²⁰ 이로 인해, 도시의 정치, 경제, 운송 기반시설은 엄청난 압박을 받을 것이다.²¹ 이런 면에서, 조지 카플란(George Kaplan)은 “인간미 없는 도심 생활”은 경제적 성공과 보다 나은 삶 때문에 도시에 매료된 사람들의 급진화를 부추킨다고 지적했다. 그 결과, 지정학적으로 균중심리가 가장 큰 영향을 갖는 곳이 바로 유라시아의 대도시들이다.²² 따라서, 인구가 밀집한 불안정한 해안 지역 대도시의 몰락이라는 위협적인 시나리오가 향후 안보와 방위 요건을 추진하게 만드는 주요 요소가 될 수 있다.

5. 기후 변화

기후 변화 또한 위협 증가 요소로 작용한다. 유엔 인간거주센터(UNHABITAT)의 최근 보고서에 따르면, 해수면 상승에 취약한 지역에 사는 모든 인구의 75%가 아시아 인

19) 유엔사무국 경제사무국(Department of Economic and Social Affairs), World Urbanization Prospects: The 2009 Revision (New York: United Nations 2009).

20) 37,100,000명 인수로 아태 지역에서 도쿄가 메가시티 1위이며, 델리, 뭄바이가 그 뒤를 잇는다. 다카는 5위이며 캘커타, 상하이, 카라치가 8위에서 10위까지다.

21) 참조: UN-HABITAT, The State of Asian Cities 2010/11 (Fukuoka: United Nations Human Settlements Program, 2010), <http://www.unhabitat.org/pmss/listItemDetails.aspx?publicationID=3078> (accessed October 17, 2012).

22) Robert D. Kaplan, The Revenge of Geography: What the Map Tells Us About Coming Conflicts and the Battle Against Fate (New York: Random House 2012), p.123.

구이며, 가난한 국가일수록 가장 위험하다고 한다.²³ 기후 변화로 인해 이재민과 이주민들이 발생하고, 대도시는 더 많은 부담을 떠안게 될 수도 있다. 또한, 기반시설에 미치는 해안가 범람의 영향을 분석한 OECD 보고서는 해안가 범람의 영향을 받은 20개 도시 중 15개가 아시아 도시였다고 지적한다.²⁴ 실례로, 중국은 자국의 액화천연가스(LNG) 공급을 위한 수입 터미널 대부분을 동해안에 만들었고, 이는 해수면 상승의 영향을 받기 쉽다. 결국, 기후 변화는 북극 지역에 영향을 주면서 동시에 아태 지역에 양면적인 결과를 가져다 줄 것이다. 한편으로는, 북극해로 개방으로 인해 유럽과 아시아 간 이동 거리가 최대 20일 가량 줄어들 것이다.²⁵ 다른 한편으로는, 유럽에서 아시아로 가는 물품이 북극을 통해 가게 됨으로써, 현재 선적 형태는 북쪽에 있는 항구로 옮겨가고 그에 따라 주로 동남아시아에 거주하는 현 항구 종사자에게 부정적인 영향을 줄 것이다.²⁶

오늘날, 이를 비롯한 기타 동향의 부정적인 결과에 대한 우려 때문에 아태 지역의 군비가 증가하게 되었다. 그러나 아태 지역 국가는 경제 발전이 지속될 경우 오늘날과 같은 군비 확대를 감당할 수 있다. 최근, 아시아개발은행(ADB)은 여러 아태 지역의 국가에 대한 예상 성장률을 낮게 책정하였다.²⁷ 성장 둔화가 일시적인 것인지 구조적인지는 불분명하다. 어떤 경우이든, 아시아개발은행의 전망은 꾸준한 경제 성장을 보장할

23) UN-HABITAT, *The State of Asian Cities 2010/11*, p.184.

24) R. J. Nicholls et. al., *Ranking Port Cities with High Exposure and Vulnerability to Climate Extremes: OECD Environment Working Papers No. 1* (Paris: OECD, 2008), pp.23~27.

25) Charles Emmerson and Glada Lahn, *Arctic Opening: Opportunity and Risk in the High North* (London: Chatham House, 2012), p.30; Svend Aage Christensen, *Are the Northern Sea Routes Really the Shortest? Maybe a Too Rose-Coloured Picture of the Blue Arctic Ocean: DIIS Brief* (Copenhagen: Danish Institute for International Studies, 2009).

26) Joshua H. Ho., "The Arctic Meltdown and its Implication for Ports and Shipping in Asia", in *Arctic Security in an Age of Climate Change*, ed. James Kraska, (Cambridge, UK: Cambridge University Press, 2011), pp.39~40.

27) 아시아 개발은행(Asian Development Bank), *Asian Development Outlook 2012 Update. Services and Asia's Future Growth* (Manila: Asian Development Bank, 2012), <http://www.adb.org/sites/default/files/pub/2012/adou2012.pdf> (accessed October 17, 2012).

수 없음을 다시금 상기하는 역할을 한다. 따라서 국방비 축소의 영향에 대응하려는 현재 유럽연합과 나토의 활동에 대해 보다 자세히 살펴보는 것이 필요할 것이다.

III 유럽의 안보 및 방위 : 현명한 대안 모색

나토와 유럽연합 내부에서 통합과 공유, 역할 특화 전략에 대한 논의는 꽤 오랫동안 진행되어 왔다. 이러한 접근법에 의해 정치적 탄력을 받음으로써 두 조직은 현재 국제 활동에서 제 기능을 발휘하고 있다.

군에 있어서 기술은 매우 중요하며, 기술의 격차는 다자간 군사 협력을 상당히 저해할 수 있다. 이 교훈은 1991년 걸프전 이후 모든 국제 활동을 통해 재차 확인되었다. 1990년대부터 유럽 국가는 발칸 반도의 안정을 위한 국제적 활동에 군사 지원을 제공하기 위해 계속 고군분투했다. 1999년 코소보 사태에 대한 나토 연합군 작전을 통해 유럽 군사력의 비효율성이 날났이 밝혀졌고,²⁸ 그 결과 1999년 나토-미국 간 정상 회담은 5가지 분야에서 격차를 좁히기 위한 방위 역량 구상을 채택했다. 5가지 분야는 배치와 기동성, 지속가능성과 실행 계획, 지휘통제정보시스템, 효율적 개입, 군사 생존 가능성 등이다.²⁹

2001년 9월 11일 이후, 추는 이제 다른 방향을 향해 가고 있다. 이제 중점은 유럽에서 멀리 떨어진 지역의 전쟁 수행과 테러와의 전쟁이다. 이라크와 아프가니스탄 내 미국-유럽 동맹은 기존에 드러났지만 해결되지 않은 군사력 격차 때문에 유지하기 힘들게 되었다. 게다가, 전반적인 전략지정학적 환경도 변하기 시작했다. 두 지역에 대한 국제적 개입은 조정에서 안정화로 변하면서 미국이 국제적 연합 군사 작전에 관해 조

28) Anthony H. Cordesman, *The Lessons and Non-Lessons of the Air and Missile War in Kosovo: Executive Summary* (Washington, DC: Center for Strategic and International Studies, 1999).

29) 세부사항은 다음을 참조: Department of Defense, *Strengthening Transatlantic Security: A U.S. Strategy for the 21st Century* (Washington, DC: Department of Defense, 2000), p.15.

심스러운 태도를 취함과 동시에 이미 1990년대부터 논의해왔던 아태 지역에 대한 군사력 재정비를 준비하고 있음이 분명해졌다. 리비아의 모아마르 카다피 군대에 대한 2011년 전반기 나토군의 통합 보호자 작전 중, “조정된 개입”이라는 미국의 새로운 접근법³⁰이 도입되었다. 작전 이후 평가에 따르면, 연합세력 작전 중 많은 부분에서 군사력 부족이 드러났고, 특히 정보와 감시, 정찰, 지휘 및 통제, 특정 공격 자산, 기타 주요 군사력에서 부족함이 두드러졌다.³¹ 현대의 합동전에 나타난 다루기 힘든 양상을 매우 잘 보여주는 예가 한 국제회의에서 유럽 내 미 공군 중령 크리스토퍼 배넷(Christopher Bennet)이 한 말인데, 그는 통합 보호자 작전에서 “9개국이 16개국의

표 2 : NATO 스마트 국방 사업 24종

■ 나토 범세계적 무기 인터페이스	■ 컴퓨터 정보 서비스 E-Learning 교육 센터 네트워크
■ 급조폭탄 제거 원격조종 로봇	■ 개인 교육훈련 프로그램
■ 해상초계기 통합	■ 울름 다국적 합동 본부
■ 다국적 탄약 협력	■ 안보 국방 분야 여성 리더
■ 다국적 항공훈련센터	■ 합동군수지원단
■ 다국적 의료시설 통합 및 공유	■ 전개 가능 공군기지 지원 통합
■ 연료취급을 위한 다국적 군수 파트너십	■ 전구개방능력
■ 지뢰방호장갑차 정비 다국적 군수 파트너십	■ 군사장비 해체, 비무장 및 제거
■ 전개 가능 계약전문그룹	■ 다국적 군 항공승무원 훈련
■ 헬기 정비 다국적 군수 파트너십	■ 급조폭발물 제거-생체인식
■ 실전적 훈련 환경	■ 다국적 지리 지원단 설립
■ Centers of Excellence 교육훈련 허브	■ 다국적 사이버방어 능력 발전

출처 : Multinational Projects (Brussels: NATO, 2012), http://www.nato.int/nato_static/assets/pdf/pdf_2012_10/20121008_media-backgroundunder_Multinational-Projects_en.pdf

30) George Friedman, “The Emerging Doctrine of the United States”, Stratfor, 2012년 10월 9일.

31) Tom Withington, “Libya Lessons: NATO hears Calls for Better C2, More Targeting Experts,” Defense News, January 25, 2012, <http://www.defensenews.com/article/20120125/C4ISR02/301250006/Libya-Lessons-NATO-Hears-Calls-Better-C2-More-Targeting-Experts>

27기종 항공기에 공중 급유를 지원했다.”라고 말했다.³²

나토와 유럽연합 국가는 이러한 작전의 배후 사정과 현재 경제·재정 위기라는 심각한 상황을 고려하여 현 군사력 부족을 타개하기 위해 다시 통합과 공유, 역할 특화라는 접근법을 택하기 시작했다. 2012년 열린 워싱턴 정상회담에서, 나토 회원국은 스마트 국방 구상을 채택했다.³³ 스마트 국방 구상은 세 가지 주요 원칙 위에 마련되었다. 그 세 가지 원칙은, 나토의 요구와 함께 국가의 군사력 우선 사항을 고려하고, 나토 회원국이 국력에 주력하고 각각의 활동을 편성할 수 있게 “계획적으로” 특화하고, 각각의 능력을 제공할 수 있는 경제력을 가지기 위해 협력하는 것이다. 스마트 국방 구상을 진전시키기 위해, 동맹변혁 최고사령관 스테판 아브리엘(Stéphane Abrial) 장군과 사무차장 알렉산더 버시바우(Alexander Vershbow) 대사를 특별 대표로 임명했다. 유럽연합과 방위 산업과 함께, 나토 회원국은 스마트 국방 구상을 통해 <표 2>에 요약된 부분에서 진전하고자 한다.

유럽연합 회원국의 경우, 2010년 겐트 구상을 통해 통합과 공유를 정치적으로 뒷받침했다.³⁴ 독일 정부와 스웨덴 정부가 상정한 “생각의 양식 논문”에서는 협력 증진을 위한 세 가지 분야를 지정했다 : 첫째는 각 국가에 필수적인 국력과 지원 구조의 상호 운용성을 향상시키는 것이고, 둘째는 “서로 너무 의존하지 않고 더 긴밀히 협력(예 : 전략적 및 전술적 공수)”하는 공동 조치의 기회를 모색하는 것이며, 셋째는 “상호 의존과 의지가 국제적 역할과 임무 공유의 틀(예 : 군사 훈련·집회·평가시설)”에 수용되는 국력과 지원 구조를 찾는 것이다.³⁵ 이러한 구상은 2010년 유럽 위원회의 군사력 강화에 관한 결론에서 채택되었고 유럽방위청(EDA)이 실행에 옮겼다. 유럽방위청

32) Quoted in: Gareth Jennings, “US tanker force looks to learn Libyan lessons,” Jane’s Defence Weekly, 2012년 10월 3일, p.5.

33) 세부사항은 다음을 참조: http://www.nato.int/cps/en/natolive/topics_84268.htm?

34) Ghent Initiative 이전에, 영국 및 프랑스는 방산업 관련 긴밀한 협력을 강조하는 새로운 양자 국방협력 조약을 채택했다. 참조: UK-France Summit 2010 Declaration on Defense and Security Cooperation, 런던, 2010년 11월 2일, <http://www.number10.gov.uk/news/uk-france-summit-2010-declaration-on-defence-and-security-co-operation/>

35) Intensifying Military Cooperation in Europe. Ghent Initiative. Food for Thought Paper, pp.1~2, <http://www.robert-schuman.eu/doc/actualites/papsweallpoolsharingnot.pdf>

은 2011년 내내 <표 3>의 통합 및 공유 프로젝트를 모색하기 위해 노력했으며, 이러한 프로젝트 중 일부는 이미 실행되고 있다. 일례로 유럽방위청은 2012년 9월 유럽 위성 통신 조달 계획을 위해 최초로 상용 위성통신(SATCOM) 제조사인 아스트리움(Astrium)과 계약을 체결했다.³⁶ 2012년 9월 27일 열린 유럽연합 회원국 국방부장관 회담에서는 통합과 공유의 중요성을 다시 한 번 강조했고 자발적인 행동 강령의 제안에 합의했다.³⁷

표 3 : 유럽방위청 통합 및 공유 사업

■ 헬기 훈련 프로그램	■ 정보/감시/정찰(우주상황판단 포함)
■ 해상 감시 네트워크	■ 조종사 훈련
■ 유럽 위성통신 조달반	■ 유럽 수송 허브
■ 야전 의료병원	■ 스마트 탄약
■ 공중 재급유	■ 해상 군수 및 훈련
■ 미래 군 위성통신	

출처 : 유럽방위청 통합 및 공유(브뤼셀: 유럽방위청, 2011), http://www.eda.europa.eu/docs/documents/factsheet/_pooling_sharing_-_301111

역할 특화는 물론 통합과 공유도 비슷한 구상에서 출발했지만 서로 다른 논리를 촉발할 수 있다. 이 때문에 유럽연합과 나토 회원국의 방위 계획을 촉진하고 조정하기 위해서는 설득력 있는 전략적 근거와 체계적 기반이 필요하지만 아직 부족한 실정이다. 유럽연합은 회원국 간 방위 협력 제도를 공평하게 마련하기 위해 노력했고, 나토 역시 진전을 보였다(표 4). 문제는 현재 대부분의 조치가 하향식이 아니라 상향식이라는 점이다. 따라서 주요 전략적 군사력의 부족은 아직도 해결되지 않았다.

36) http://eda.europa.eu/news/12-09-28/European_Defence_Agency_facilitates_access_to_commercial_SatCom_services_for_Member_States (accessed October 17, 2012).

37) http://eda.europa.eu/news/12-10-02/Ministers_of_Defence_welcome_EDA_s_Pooling_Sharing (2012년 10월 17일 접속).

표 4 : 통합과 공유, 역할 특화를 촉진하기 위한 전반적인 유럽연합-나토의 기반

- **전략, 개념 및 위험분석** : 협력을 강화하기 위해서는 국가가 추구하는 가치, 국익, 규범에 대해 합의하는 것이 필수적이다. 지금까지 나토와 유럽연합은 향후 다루어야 할 당면과제와 공통 해결책 마련 방안에 대한 공동이해를 도출해내는 중요한 역할을 해왔다. 신나토개념 또는 유럽 안보전략과 같은 합동 전략은 국가적 사고를 정리하는 중요한 기반 문서이다.
- **기구** : 유럽연합과 나토는 국방협력을 위한 제도적 기반을 제공한다. 조직체와 정기적인 회의의 운영을 통해 신뢰를 형성하고 협력을 조장한다. 이러한 기구들은 특정 과업을 수행할 수도 있기 때문에 조달, 국방 과학 및 기술 등의 분야 내 합동 국제 활동을 지원한다고 할 수 있다. 정치적 제도뿐만 아니라 나토와 유럽연합은 합동 군사조직(본부, 합동 부대 등)을 수립, 군 의사결정과 작전상의 모든 수준에서 중요한 조율 역할을 부여한다.
- **작전** : 냉전 종식 이후, 나토와 유럽연합은 유럽, 아프리카, 중동, 지중해, 인도양 등에서 합동군사작전을 수행하기 위한 기틀을 제공해왔다.
- **수단** : 유럽연합과 나토는 국방계획을 지원하기 위한 군사계획 수단을 제공한다. 두 기구는 합동군 목표에 부합하는 시나리오를 발전하고, 전투력창출 회의를 조직하고, 계획 및 검토 절차를 제공하는 등 회원국들 간 국방계획의 조화를 도모한다. 더불어 군사 표준을 위한 연합차원의 노력은 군사 상호운용성 발전을 위한 중요한 역할을 한다.
- **국방 무역** : 유럽연합과 나토는 회원국들 간의 국방 무역을 조장하기 위해 오랜 시간 노력해왔다. 특히 유럽연합 내에서 회원국들은 상호 국방세출을 촉진하고 국가 간 국방사업의 장벽을 완화하는 목표를 위해 노력해왔다. 부록 1에서 볼 수 있듯이, 2005년부터 2011년까지 유럽연합 27개국 간의 내부 국방세출은 전체 국방수입의 62%를 차지하였다. 국가 단위로 보면 미국이 최대 공급국(30%)이며 그 밑으로 독일(24%), 네덜란드(9%), 프랑스(8%), 스웨덴(7%), 이탈리아(6%) 등이 있다. 유럽연합 기반의 국방세출 비율이 높음에도 불구하고, 전체적으로 공동 국방장비 조달은 상대적으로 낮은 수준이며 회원국들 간 격차가 상당한 것으로 드러났다. 2010년 수치에 따르면 영국과 프랑스가 가장 많은 지출을 하였고, 그 다음으로 이탈리아, 독일, 스페인 순이다.³⁸

38) 영국: 2,760,000,000 유로, 프랑스: 1,847,000,000유로, 독일: 1,398,000,000유로, 스페인: 703,000,000유로. 참조: Defence Data: EDA participating Member States in 2010 (Brussels: European Defence Agency, 2012), p.24, http://www.eda.europa.eu/docs/documents/National_Defence_Data_2010_4.pdf

통합과 공유 전략은 규모의 경제에 기반을 둔다. 많은 국가는 군사력을 모아 현재의 군사력을 유지하거나 더 증강하고자 한다. 또한 부담을 덜어냄으로써, 각국은 추가적인 재량을 얻게 되고 통합은 새로운 부가가치를 창출한다. 영유권 이전의 범위는 각기 다르다. C-17 글로브마스터 III(C-17 Globemaster III) 수송기와 동맹군의 공중 조기경보통제기(AWACS) 함대, 유럽 공군사령부에 기반을 둔 나토의 전략적 공수 작전력은 통합과 공유의 성공적인 예로 볼 수 있다. 역할 특화는 경쟁 우위에 중점을 둔다. 각 국가는 특정 능력에 전략적 이해관계를 갖고 있고 그 능력을 제공함으로써 명성을 쌓기 때문에, 또는 양자 간 및 다자 간 합의의 일환으로 역할 특화에 합의했기 때문에 특정 능력을 제공하기 위해 노력한다. 그러나 계획적인 특화라고 불리는, 양자 간 또는 다자 간 합의의 일환인 역할 특화는 아직 실행된 바 없지만, 체코의 나토 화생방방호 부대는 역할 특화의 한 예이다.³⁹

39) 기타 사항 관련, 다음을 참조: Tomas Valasek, *Surviving Austerity. The case for a new approach to EU military cooperation* (London: Centre for European Reform, 2012); Jakob Henius and Jacopo Leone MacDonald, *Smart Defense: A Critical Appraisal* (Rome: NATO Defense College, 2012); “The European Air Transport Command. A Successful Example for Pooling and Sharing. Interview with Major-General Jochen Both, first Commander of the EATC 2010–2012,” *The Journal of the JAPCC* (Autumn/Winter 2012): 34–38; Jean-Pierre Maulny and Fabio Liberti, *Pooling of EU Member States Assets in the Implementation of ESDP* (Brussels: European Parliament Subcommittee on Security and Defense, 2008); Heiko Borchert and René Eggenberger, “Rollenspezialisierung und Ressourcenzusammenlegung: Wie Europas sicherheitspolitische Fähigkeiten gestärkt werden können” [Specialization and Pooling: How to Strengthen Europe’s Security and Defense Capabilities] in Hans-Georg Erhart und Burkhard Schmitt, eds., *Die Sicherheitspolitik der EU im Werden: Bedrohungen, Aktivitäten, Fähigkeiten* (Baden-Baden: Nomos, 2004), 230–244; Rachel Lutz Ellehuus, *Multinational Solutions versus Intra-Alliance Specialization* (Copenhagen: DIIS, 2002); Gilles Andréani, Christoph Bertram, and Charles Grant, *Europe’s Military Revolution* (London: Centre for European Reform, 2001).

통합, 공유, 역할 특화는 영구적으로 또는 임시적으로 마련될 수 있으므로 중점이 각기 다를 수 있다(표 5). 임시 대책은 대부분 작전상 필요에 의해 나오고 그 대책 구성은 정치적 최우선과제에 따라 달라진다. 그러나 현재의 재정적 상황으로 인해 군사력의 범위가 축소됨에 따라 임시적인 통합과 역할 특화 측면에서 국가별 재량을 제한할 가능성이 크다. 따라서 오늘날 국방 예산 축소는 의도치 않게 “자동적인 구조적 특화”를 초래할 수 있다.

표 5 : 통합과 공유, 역할 특화를 위한 4가지 중점

- **임무 중점** : 이 경우, 국가의 군사행동에 대한 의지를 규정하는 국가적 수준의 목표가 원동력이다. 예로, 어떤 국가는 조기전력 투입에 초점을 둘 수도 있고, 정보/감시/정찰 또는 타격 자산에 초점을 둘 수 있다. 파트너국과 통합하고 공유하는 노력을 함에 있어서 각 국은 정치적 목표, 전략 문화, 해당 과업을 지지하는 여론 등의 유사점에 중점을 두어야 한다.
- **수명주기 중점** : 국방능력의 수명주기는 준비(계획, 교리, 과학기술 등), 조달, 보충, 교육 훈련, 방위산업 역량 발전 및 유지, 운영/보수, 그리고 국방 기구를 운영하기 위해 소요되는 모든 절차와 구조에 대한 관리 및 발전 측면까지 포함한다. 국가들은 수명주기에 따라서 훈련 시설 또는 군수 등 특정분야에 초점을 맞추어 통합, 공유, 전문화 노력을 수행할 수 있다.
- **의사결정 중점** : 의사결정의 대비태세는 중점분야에 따라 매우 달라진다. 조기에 전력투입을 하고자 하는 국가는 신속한 정치 대응 장치를 필요로 할 것이다. 이는 국가별 의사결정 간 차이점들이 합동 전개를 지연시키고 불가능하게 할 수도 있기 때문에 파트너국을 선정할 때 필수적으로 고려해야 하는 것이다.⁴⁰
- **지리적 중점** : 지리적 근접성과 지리-전략적 이익은 합동운영능력 형성으로 이어질 수 있으며(스칸디나비아 반도 국가 등) 특정 능력 증강을 유발할 수 있다(문화인식, 주변국 상황 이해 등).

출처 : Borchert/Eggenberger, “Rollenspezialisierung und Ressourcenzusammenlegung”, pp.234~235.

40) Marc Houben and Dirk Peters, The Deployment of Multinational Military Formations: Taking Political Institutions into Account (Brussels: CEPS, 2003), <http://www.ceps.eu/book/deployment-multinational-military-formations-taking-political-institutions-account>

영구적인 해결책을 이끌어낼 구조적 합의는 대부분 전략적 포부를 공유하고 비슷한 정치·행정적 틀을 갖고 있고 유사한 자산을 가진 국가들 간에 이뤄진다. 영국과 프랑스 간 향후 항공모함 공유에 대한 합의는 가장 파격적인 구조적 조정 중 하나이다. 네덜란드와 벨기에, 스칸디나비아반도 국가 등 다른 국가는 주변국과 군부대를 상당 부분 통합하여 협력을 한층 강화했다.⁴¹

현재까지의 통합과 공유, 역할 특화의 실질적인 진전은 “단편적으로”만 진행되었다.⁴² 그 결과, 유럽연합과 나토 회원국은 아직 공동으로 군사력을 구축하지 못했다.⁴³ 이는 정치적 의지의 부족을 반영하는데, 즉 유럽연합과 나토 간 방위 협력을 저해할 전략적 사안에 관한 양측의 점점 커지는 의견 차이 때문이다. 더 나아가 기존의 틀은 국방의 자주권을 더 많이 포기하는 것에서 오는 위험 요소를 줄이는 데 도움이 되지 못한다. 예를 들어, 모든 국가가 기존의 약속을 지키고 다국적 군대를 무용지물로 만들 수 있는 병력 철수를 지양할 것이라는 보장은 없다. 조직적이지 않은 국가 지출 축소가 진행되는 마당에, 현재 군사력 부족을 해결할 유럽 공동의 대책을 도출해낼 수 있을지 여부는 여전히 불분명하다. 공동으로 합의한 유용성과 배치, 준비 태세 면에서 통합과 공유 구상에 대한 국가별 기여를 평가할 견실한 통제 및 감사 과정은 아직 합의되지 않았다.⁴⁴

41) 유럽의 구조적 통합의 현존하는 사례로는 다음을 참조: Valasek, *Surviving Austerity*, pp.18~19.

42) Valasek, *Surviving Austerity*, p.8.

43) Sven Biscop and Jo Coelmont, *Pooling & Sharing: From Slow March to Quick March?* Egmont Security Policy Brief (Brussels: Egmont Royal Institute for International Relations, 2012), p.2.

44) 추가 사항 관련, 다음을 참조: Valasek, *Surviving Austerity*, pp.21~27; Henius/MacDonald, *Smart Defense*, pp.32~47; Maulny/Liberti, *Pooling of EU Member States Assets in the Implementation of ESDP*, pp.16~18; Claudia Major, Christian Mölling, and Tomas Valasek, *Smart But Too Cautious: How NATO Can Improve Its Fight Against Austerity* (London: Center for European Reform, 2012); Bastian Giegerich, “NATO’s Smart Defense: Who’s Buying?” *Survival*, Vol. 54, No. 3 (June–July 2012), pp.69~77.

IV 아태 지역과 유럽·미국의 스마트 국방 협력

아태 지역의 실현 가능한 스마트 국방 대책 방안에 대한 논의는 범지역적 신뢰가 낮다는 전제에서 출발해야 한다. 아태 지역 일부 국가는 주변국과 아태 지역 내 다른 국가와 원만하고 안정적인 관계를 갖고 있으나 전반적으로 적대감이 만연해 있다.⁴⁵ 따라서 당장은 강력한 양자 관계를 제외하고, 아태 지역에서 방위 관련 계획적인 역할 특화를 시도하기는 이르다. 따라서 본 논문은 이 사안에 대해서는 다루지 않을 것이며, 아태 지역의 다자 간 협력에 기반한 통합과 공유를 집중적으로 다룰 것이다.

아태 지역의 다자 간 안보 및 방위 협력의 역사는 복잡하다. 예를 들어, 동남아국가연합(ASEAN) 회원국이 남중국해 분쟁에 대한 합의에 도달하지 못함으로써 동남아국가연합은 상당한 타격을 받았다.⁴⁶ 방위비 조달을 통합하고자 한 동남아국가연합의 지난 노력은 주요 회원국 간 의견 차이로 인해 제한적인 성공만 거두었다.⁴⁷ 반면, <표 6>에서 보듯이 아시아 해적퇴치협정(ReCAAP)과 공동인식 및 무력방지 회의(SHADE)와 같은 구상을 통해 성공적인 범아태 지역 구상이 있다는 것을 증명한다. 이러한 “일련의 성과”에도 불구하고, 통합과 공유 구상은 범아태 지역 접근법이라고 부르기보다는 일부 파트너 국가를 기반으로 마련된 방안이라고 부르는 것이 더 합당하다.

45) 한국과 일본 관계가 급격히 악화되는 것은 구체적인 예이다. See: Brendan Taylor, “Japan and South Korea: The Limits of Alliance,” *Survival*, Vol. 54, No. 5 (2012년 10월~11월), pp.93~100.

46) Ian Storey, “China pushes on the South China Sea, ASEAN unity collapses,” *China Brief* XII, No. 15 (2012년 8월 4일), pp.8~10.

47) 2010년 5월, ASEAN 국가는 adopted the Concept Paper on Establishing ASEAN Defence Industry Collaboration을 채택, <http://www.aseansec.org/documents/18471-k.pdf>. See also: Sneha Raghavan and Guy Ben-Ari, “ASEAN Defense Industry Collaboration,” CSIS Defense-Industrial Initiatives Group Current Issues No. 25 (2011년 7월), <http://csis.org/publication/diig-current-issues-no-25-asean-defense-industry-collaboration>; Trefor Moss, “ASEAN’s slow security evolution” *Jane’s Defence Weekly*, 2012년 2월 29일, pp.30~32.

표 6 : 아태 지역 방위 및 안보 협력 증진을 위한 정보 통합

- **아시아 해적퇴치협정(ReCAAP)** : 아시아 해적퇴치협정은 소통 조장, 사태 분석, 역량발전 노력 촉진, 합동연습 협력 및 기타 활동들을 통해 해적을 퇴치하는 정보 교류의 장으로써의 역할을 해왔다. 동 협정은 2006년에 17개국(방글라데시, 브루나이, 캄보디아, 중국, 덴마크, 인도, 일본, 한국, 라오스, 미얀마 등)이 가입함에 따라 발효되었다. ReCAAP 정보공유 센터(ISC)는 매일 24시간 가입국들에게 정보를 배포할 수 있도록 하는 인터넷 기반 정보체계를 운영하고 있다.
- **공동 인식 및 무력방지 회의(SHADE)** : SHADE 회의의 목적은 아덴만과 서인도양에서 수행하는 대해적 작전에 대한 협력을 증진하기 위함이다. SHADE는 공동 상황판단과 공동 상황이해를 증진시키기 위한 정보교류에 초점을 두고 있다. 이 회의에는 국제기구와 해상산업체 또한 참여한다. 회의는 바레인에 위치한 연합해군사(CMF)에서 개최되며 27개국(호주, 바레인, 벨기에, 캐나다, 덴마크, 프랑스, 독일, 그리스, 이탈리아, 일본, 요르단, 한국, 쿠웨이트, 말레이시아, 네덜란드, 뉴질랜드, 파키스탄, 포르투갈, 사우디아라비아, 세이셸, 싱가포르, 스페인, 태국, 터키, 아랍에미리트, 영국 및 미국)이 SHADE와 CMF를 지원하고 있다.

출처 : <<http://www.recaap.org/Home.aspx>>; <<http://combinedmaritimeforces.com>>

통합과 공유가 아태 지역에서 제대로 적용되려면, 유럽과는 다른 근거를 마련해야 한다. 유럽은 긴축 재정 시기이므로 군사력 제공이 주요 동기가 된다. 따라서 유럽연합과 나토 회원국 간 현존하는 방위 협력의 재조정에 주력하는 것이 더 효율적이다. 그러나 아태 지역의 상황은 다르다. 아태 지역은 경제 성장과 현재 안보 과제에 따라 방위비 지출을 늘리고 있다. 적어도 현재로서는 경제적 효율성은 둘째 문제이다. 또한 파트너 국가들은 지역 안보를 강화할 필요성을 느낀다. 아시아에서 미국이 중심축 역할을 하기 때문에, 아태 지역 국가는 아태 지역 내 강국으로 떠오르는 일부 국가 간 격차를 줄이기 위해 미국이 이 지역에서 계속 균형잡는 역할을 하도록 미국 정부와 공동의 군사력을 구축할 수 있다.

현재 미국의 외교 정책은 변화하는 중이다. 미국 정부는 아태 지역을 새로 주목해야 할 곳으로 지정했다. 그러나 미국의 약속이 2차대전 이후 미국이 유럽에 전략적으로 개입했던 그 수준과 비슷할지는 지켜봐야 한다. 따라서 적어도 일부 아태 지역 국가는

미국과의 관계를 강화하고자 하며, 이들 국가는 양자 간 통합과 공유를 공동 방위 구상의 연계망을 만드는 방법으로 사용할 수 있다. 만약 이 구상이 결실을 맺는다면 유럽 국가들도 유럽연합 27개 회원국의 무역 관계에 매우 중요한 이 지역에서 방위 및 안보 관계를 맺기 위해 노력할 것이다. 따라서 아태 지역과 미국 간 통합과 공유는 유럽 국가와의 협력에도 촉진제 역할을 할 것이다. 유럽연합 회원국이 자금난을 겪고 있다는 사실은 상황을 더욱 악화시킬 수도 있지만 아태 지역 국가와 새로운 자금조달 체계를 마련할 기회이기도 하다.

통합과 공유를 고려할 때, 현재 군사력과 현지 방위산업체의 생산 역량과 포부, 외부 방위업체의 역할은 반드시 분석해야 하는데, 분석 결과는 복합적이다:

1. 유럽 국가와 달리, 아시아-유럽 정상회의 회원국은 주로 외부 방위업체에 의존하고 있다(첨부 2 참조). 2005년부터 2011년까지 아시아-유럽 정상회의 회원국의 방위물품 총수입액은 미화 6,295만 9천 달러에 달한다. 이 중 가장 큰 몫은 러시아로부터 수입하는 물품이며, 2,726만 7천 달러로 약 42%를 차지한다. 미국은 25%(미화 1,594만 3천 달러), 유럽연합 27개 회원국은 미화 1,315만 2천 달러로 21%를 차지한다. 반면, 아시아로부터 수입하는 방위물품은 미화 415만 8천 달러로 7%에 불과하고 이 중 중국이 1위(미화 344만 달러)이다. 공동 방위 조달에 대한 관심이 점점 늘어나는 조짐이 보이지만,⁴⁸ 당분간 통합과 공유 적용 시, 반드시 외국 방위업체의 이해관계를 고려해야 한다. 자칫 잘못하면 유럽 정부는 다자 간 해결책을 찾기 더 어려워질 수도 있다.
2. 현재까지, 유럽의 방위업체는 아태 지역 방위 시장에 진입하기 위해 서로 경쟁하고 있고 미국 및 러시아와도 경쟁하고 있다. 통합과 공유가 유럽의 이해관계에도 부합한다면, 유럽 공동의 수출 활동도 고려해야 한다. <표 4>를 보면 알 수 있듯이, 적어도 이론상으로 아직 유럽 방위업체 간에는 협력의 여지가 있다. 유럽 업체들이 아태 지역 국가에 다양한 종류의 무기체계를 제공하기는 하지만, 여러 클러스터를 만들 수도 있다. 이에 대해서는 다음에서 더 언급할 것이다.

48) 인도네시아 및 한국에서 추구하는 차세대 전투기프로젝트가 한 예이다.. 참조: Trefor Moss, "Asia's Next Fighter Project," The Diplomat, 2011년 7월 14일, <http://thediplomat.com/flashpoints-blog/2011/07/14/asias-next-fighter-project/>

3. 그러나 방위 업체는 방정식의 한 부분일 뿐이다. 통합과 공유를 선택할 때, 아태 지역 방위산업체의 생산 역량과 포부도 고려해야 한다.⁴⁹

일본은 잘 알려진 대로 첨단 기술 기반을 갖추고 있음에도 불구하고, 지금까지 일본의 방위 산업은 어려움을 겪어왔다. 그러나 일본 정부의 방위 태세는 변하고 있는 것으로 보이며, 최근 일본은 훨씬 적극적으로 변했다. 필리핀에 대한 방위 지원, 호주와의 방위 관계 강화, 방위물품 수출에 대한 규율 완화 등이 그 예이다. 장관급인 방위생산 및 기술기반 연구 위원회의 최근 보고에 따르면, 일본은 국가 방위 산업 기반을 재조정하고 있으며, 현재 추진하고 있는 주요 조달 프로젝트에는 새로운 육·해·공 공동 자산 조달은 물론 차세대 전투기 경연과 잠수함 병력 확장 등이 있다고 한다.

인도네시아의 방위 산업은 지금까지 라이선스 제조에 집중되어 있었다. 군사 플랫폼을 설계하고 개발하는 인도네시아의 역량은 제한적이다. 그럼에도 불구하고, 인도네시아의 방위 관련 포부는 커지고 있고, 특히 해상에서 두드러진다. 인도네시아는 한국의 잠수함을 주문했고, 중국과 함께 대함미사일을 개발하고 있으며, 전자 시스템 개발과 관련된 감시 기술에도 주력하고 있다.

49) Paul Kallender-Umezu, "Japan Strives to Overcome Defense Industrial Base Crisis," Defense News, June 24, 2012, <http://www.defensenews.com/article/20120624/DEFREG03/306240003/Japan-Strives-Overcome-Defense-Industrial-Base-8216-Crisis-8217->; Trefor Moss, "Japan's Defense Industry Lifeline," The Diplomat, December 31, 2011, <http://thediplomat.com/2011/12/31/japan's-defense-industry-lifeline/> (accessed November 19, 2012); Jon Grevatt, "Japan looks to new defence policy to boost defence industry," Jane's Defence Weekly, October 30, 2012, p.23; Indonesia. IHS Jane's Navigating the Emerging Markets (Surrey: IHS Jane's, 2012); Malaysia. IHS Jane's Navigating the Emerging Markets (Surrey: IHS Jane's, 2012); Republic of Singapore. IHS Jane's Navigating the Emerging Markets (Surrey: IHS Jane's, 2011); South Korea. IHS Jane's Navigating the Emerging Markets (Surrey: IHS Jane's, 2012); Vietnam. IHS Jane's Navigating the Emerging Markets (Surrey: IHS Jane's, 2012); Guy Anderson and Jon Grevatt, "Rich pickings. Emerging markets: Southeast Asia," Jane's Defence Weekly, September 19, 2012, pp.20~29; Guy Anderson, "A Changing Game Board: How Competition on the International Defence Market is Shifting" (Surrey: IHS Jane's, 2012); IISS, The Military Balance 2012 (London: Routledge, 2012), pp.206~208.

말레이시아는 항공기의 수리, 정비, 개조(MRO)와 같이 자국 기술 수준이 낮은 분야의 국방 기술을 처분하고 소형 무기와 군수품을 생산하고 조선업에 참여하고 있다. 미래를 위해, 말레이시아는 C4ISR(지휘통제·통신·컴퓨터·정보 및 감시·정찰, Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) 기술 개발을 최우선 과제로 하고 무인 항공 시스템에도 관심을 보이고 있다. 위성 서비스와 정보기술, 시뮬레이션 시스템도 말레이시아가 박차를 가하고 있는 분야이다. 그러나 최근 말레이시아는 새로운 만능 전투기 등 여러 개의 주요 플랫폼의 조달을 연기한 반면, 새로운 스코르펜급 잠수함(Scoprene submarines)을 배치하기도 했다.

싱가포르는 자국 방산 역량 면에서 아태 지역의 선두 주자임이 분명하다. 현재 싱가포르의 역량은 해군, 육군, 공군(엔진 기술뿐만 아니라 항공기의 수리, 정비, 개조 포함)에서부터 감시 및 레이더, 센서 시스템뿐만 아니라 통신 시스템까지 두루 섭렵하고 있다. 무인 시스템은 싱가포르의 방위 산업 역량의 정점이다. 또한, 싱가포르의 KC-135 대형선박 교체, F-35 제트 전투기, 잠수함과 같은 외국산 시스템에도 투자하고 있다.

한국은 지휘 통제 시스템은 물론 C4ISR에 주력한 방위 전자제품뿐만 아니라 공군, 육군, 해군 시스템을 활발히 개발하며 국방 산업 기반이 발달되어 있다. 그러나 방산 자립이라는 목표를 천명한 후에도, 한국은 주로 미국산인 차세대 전투기와 공격용 헬리콥터 등 외국산 플랫폼에 여전히 투자를 계속하고 있다.

태국은 공군 및 육군용 항공기의 수리, 정비, 개조 분야에서 국방력을 갖추고 있고 조함을 진행 중이다. C4ISR과 무인 시스템과 함께 중국 기술을 사용해 미사일 시스템을 개발하는 것이 태국의 최우선 과제다.

베트남의 현재 방산 역량은 공군과 해군 시스템에 있어 가장 기초적이다. 베트남의 국방 산업에 대한 포부는 제한적이나, 최근 해군 및 공군 역량을 향상시키는 데 많은 노력을 쏟아 붓기 시작했다.

이 같은 간략한 개요를 바탕으로, 스마트 국방협력을 위해 아래와 같은 클러스터를 고려해 볼 수 있다:

추진 장치의 경우, 독일은 말 그대로 아태 지역에 디젤 엔진을 제공하는 “강대국”이다. 프랑스와 영국도 특히 항공기 엔진 면에서 큰 역할을 한다. 치솟는 유가로 인해 에너지 의존을 줄이고 비용을 아끼기 위해, 군대에 있어 에너지 효율성은 매우 중요하

다. 따라서 각 회사가 이미 그 서비스를 제공하고 있지 않다면, 항공기의 수리, 정비, 개조(MRO) 허브를 구축할 흥미로운 기회가 생긴다. 아시아 국가들이 자동차와 조선 산업에서 주요 선도국가라는 사실을 고려할 때, 에너지 효율을 위한 연구개발은 더욱 유용하다. 아태 지역의 효율적인 추진 장치 클러스터를 위한 스마트 협력은 서로 다른 공공 및 민간의 이해당사자에게 매력적인 동기가 될 것이다.

미사일 분야에서는 프랑스가 중심축이다. 아태 지역 국가에 납품되는 미사일 시스템의 대부분은 EADS와 BAE 시스템, 핀메카니카(Finmeccanica)가 공동 소유한 MBDA사⁵⁰가 제작한 것이다. 효율적인 접근·지역거부 문제 해결을 위한 미사일 사용, 미사일 확산 문제, 아태 지역 미사일 방어에 대한 필요성 때문에 미사일을 구매한 국가는 미사일 개발에 관심을 갖는 경향이 있다. 따라서 이 분야에 대해 유럽의 이해관계가 늘어남으로써 미국과 중국, 러시아에 대한 유럽의 공급 능력이 고취될 수 있다. 유럽 국가가 미사일 납품에 필요한 주요 플랫폼(예 : 선박, 공격기)을 공동으로 판매하는 데 합의한다면 기회는 한층 많아질 수 있다. 추가적으로 미사일 방어는 미국 및 러시아와의 성공적인 협력 기회를 만들 수 있다.

미사일 시장과 달리, 어뢰와 같은 수중 물품 시장에서 유럽 업체 간 경쟁은 치열하다. 독일의 아틀라스 일렉트로닉(Atlas Elektronik)과 프랑스의 디씨엔에스(DCNS), 이탈리아의 와스(WASS), 핀메카니카(Finmeccanica) 자회사가 서로 경쟁하고 있다. 뒤에서 언급하겠지만, 수중 물품에 대해서는 대체로 공급업자와 고객, 양자 간의 협력이 이뤄질 것으로 보인다. 그러나 유럽 기업이 아태 지역 어뢰 시장을 공략하기 위해 보다 협력하는데 합의한다면 상황은 변할 것이다.

클러스터를 만들 기회는 레이더 시장에서도 찾아볼 수 있다. 접근·지역거부 문제에 대해 점점 커지는 우려를 고려할 때, 넓은 지역을 감지하는 센서에 대한 수요가 많아질 것이다. <표 7>은 프랑스와 네덜란드, 스웨덴이 아태 지역에 서로 다른 종류의 레이더와 전자광학 시스템을 납품하고 있음을 보여준다. 이 분야의 대부분을 차지하는 납품업체는 탈레스(Thales) 또는 사브(Saab)이다. 따라서 아태 지역은 향후 레이더 기술을 진전시키기 위해 항공기 수리, 정비, 개조(MRO)에 대한 공동의 접근법과 협력을 고려해 볼 수 있다.

C4ISR은 싱가포르, 한국, 일본과 같이 아태 지역의 최고 국방 산업 국가만 협력할

50) 예를 들어, 유럽연합 공급자로서 Thales 및 Saab도 있다.

수 있는 분야이다.⁵¹ 현재 전자광학 부품 전문회사는 물론 유럽의 레이더 업체와도 협력 가능한 분야이다.

표 7 : 유럽연합 27개 회원국 업체의 일부 아시아-유럽 정상회의 회원국에 대한 무기 시스템 납품 현황(2000~2011년)

	IND	IDN	JPN	MYS	PHL	SGP	ROK	THA	VNM
공군 체계									
공중 조기경보통제기								SWE	
지상공격 전투기	FRA UK	UK						SWE	CZE
소형 수송기	DEU								POL
소형 항공기		FRA						AUT	
해상초계기	DEU	FRA ESP					UK	DEU	POL
훈련기	POL	DEU			ITA				ROM
훈련/전투기	UK			ITA		ITA		DEU	CZE
		ESP		DEU				SWE	
수송기				ESP FRA UK					
신호정보수집 항공기								FRA	
대잠수함 열기								UK	
열기		FRA	UK	FRA UK	POL		FRA	UK	
소형 열기	FRA	FRA DEU	DEU	FRA ITA		FRA	DEU	FRA	
무인기		FRA							
해군 체계									
호위함		NDL		DEU			FRA		
외해 초계함								UK	
초계정		DEU							
잠수함	FRA			FRA ESP		SWE	DEU		
지원선	DEU ITA								
육군 차량/체계									
교황건설 체계					POL				
장갑 공병차					POL				
장갑 구난차	POL				POL		DEU		
인원수송 장갑차		FRA							
탱크					POL		DEU		
효과기 및 예하체계									
방공 체계		POL							
대전차 유도탄	DEU FRA			FRA		FRA			
장갑차 포탑		BEL							
박격포			FRA	FRA					
다연장로켓포		CZE							
원거리 공대공 미사일	FRA								
근접방어 무기체계							NDL		
휴대용 지대공 미사일	FRA	FRA POL					FRA	FRA	SWE
지대공 미사일				UK		FRA	DEU FRA		
대함 미사일	FRA	FRA		FRA			UK	SWE	
				ITA UK					

51) 아태 지역 많은 국가가 C4ISR자산을 획득하는 데에 관심이 있다. 하지만 그 중 몇몇 국가만 기술발전과 생산프로젝트를 수행할 필요 산업능력이 있다. 참조: Wendell Minnick, "In Asia, C4ISR Market is Growing," Defense News, November 12, 2012, pp.12~14. For a more general analysis, see: Michael C. Horowitz, "Information-Age Economics and the Future of the East Asian Security Environment," in Goldstein/Mansfield, eds., The Nexus of Economics, Security, and International Relations in East Asia, pp.211~235.

	IND	IDN	JPN	MYS	PHL	SGP	ROK	THA	VNM
대합 어뢰						SWE			
대잠수함 어뢰	ITA	ITA				ITA SWE			
대함/대잠 어뢰	ITA			ITA		ITA	DEU		
함포	ITA	ITA SWE	ITA	ITA	SWE	ITA	ITA	ITA	
자주포								FRA	
견인포								ITA UK	
전자광학 탐지/사격 통제					NDL			DNK NDL	
레이더/수중 탐지									
잠수함 수중음파탐지기	FRA	FRA					DEU		
기뢰대항책 수중탐지기			UK	FRA			UK		
공중/해상 탐색 레이더		NDL		DEU			NDL	DNK	
				ITA					
공중 탐색 레이더	FRA ITA NDL	FRA		FRA		FRA SWE	NDL	ITA SWE	
포병 위치탐색레이더				SWE		SWE	SWE		
사격통제 레이더	ITA	NDL		ITA UK			NDL SWE	ITA NDL SWE	
해상조계기 레이더		FRA	FRA	FRA			UK		
해상 탐색 레이더	NDL					DNK			
항공기 전자 광학 체계				FRA					
추진체									
공중급유 체계			UK	UK					
공기불요 추진엔진			SWE						
다젤 엔진	FRA DEU	DEU DNK FRA	FRA	DEU		DEU	DEU FRA	DEU UK	DEU
가스 터빈			UK						
터보사프트(엔진)		FRA							
터보팬			UK			DEU		SWE	
터보제트			UK						

국가코드: BEL 벨기에; CZE 체코; DNK 덴마크; DEU 독일; ESP 스페인; FRA 프랑스; IDN 인도네시아; IND 인도; ITA 이탈리아; JPN 일본; MYS 말레이시아; NDL 네덜란드; PHL 필리핀; POL 폴란드; ROK 대한민국; ROM 루마니아; SGP 싱가포르; SWE 스웨덴; THA 태국; UK 영국; VNM 베트남

출처 : <http://armstrade.sipri.org/armstrade/page/trade_register.php> (2012년 10월 18일 접속)

방위 산업 클러스터 구성에 대한 상향식 구상과 함께, 스마트 국방 협력을 진전시키기 위해서는 하향식 구상도 필요하다. 하향식 구상은 본 논문 첫 부분에서 언급한 장기적 안보 문제를 해결해야 하고 안보와 번영의 이해관계 간의 균형을 잡는데 필요하며, 이 목표를 달성하기 위해서는 공동의 상황 인식과 이해가 중요하다.

1. 글로벌 코먼즈 관련 공동 상황 인지 · 이해 체계 구축

아태 지역의 가장 심각한 전략적 문제는 접근 · 지역거부에 근거한 군비 확장 경쟁이다. 이는 다양한 정책 분야에서 맞대응 전략을 촉발하고 글로벌 코먼즈의 자유를 심각히 저해한다. 아태 지역의 전반적인 신뢰와 신용 결여를 고려할 때, 이는 개연성 있

는 위협 시나리오이다. 공동 상황 인지와 이해를 증진시키기 위한 활동은 각각의 위협을 경감시킬 수 있다.

포괄적인 안보와 방위 해결책에 대한 오늘날의 요구는 다양한 공공 및 민간 이해당사자 간의 공동 정보와 지식 개발 및 공유에 대한 요구로 해석된다. 공통작전 상황도(COP)의 진전은 이러한 경향을 전적으로 보여주는 예이다. 여러 가지 면에서, 오늘날 네트워크를 사용한 군대의 효율성은 공통작전 상황도를 기반으로 싸우고 작전을 수립하는 능력에 따라 달라진다.⁵² 지금까지 대부분의 공통작전 상황도는 한 가지 영역에만 집중되어 있었다. 글로벌 코먼즈의 자유를 위협하는 다면적인 접근·지역거부 문제를 고려할 때, 차세대 공통작전 상황도가 필요하다.

글로벌 코먼즈의 공통작전 상황도는 공공 및 민간 이해당사자에게 글로벌 코먼즈의 자유를 침해하는 다양한 활동을 전체적으로 보여줌으로써 다양한 영역의 정보를 한 데 모아야 한다. 그럼으로써, 글로벌 코먼즈의 공통작전 상황도를 통해 이해당사자들은 글로벌 코먼즈의 서로 다른 영역 간 상호 작용을 이해할 수 있게 된다. 또한, 글로벌 코먼즈의 공통작전 상황도는 서로 다른 결정이 글로벌 코먼즈의 각 이해당사자의 상대적인 입장에 어떤 영향을 미치는지를 평가하는 데 있어 필수적이다. 즉, 이해당사자의 향후 조치에 관한 역량을 증진시킬 수 있다. 요약하자면, 아태 지역 국가는 글로벌 코먼즈의 공통작전 상황도 개념을 ASEAN국가 간 신뢰구축조치 합의⁵³의 일환으로 정보교류의 필연적 지속 및 나토와 유럽연합과 같은 국제적 파트너와 함께 협력하는 데 사용할 전략적 수단으로 봐야 한다.

2. 수중 상황 인지·이해 체계 개선

본 논문의 첫 번째 장에서는 국가 간 심각한 균열을 야기할 가능성이 있는 다양한

52) 추가사항은 다음을 참조: Ralph Thiele, "Smart Defense in the 21st Century," *The Korean Journal of Security Affairs*, Vol. 17, No. 1 (2012년 6월), pp.83~99, in particular, pp.93~99.

53) "ADMM-Plus: Strategic Cooperation for Peace, Stability, and Development in the Region," Chairman's Statement for the First ASEAN Defence Ministers' Meeting-

수중 활동에 대해 논의했다. 자원에 대한 수요가 증가함에 따라 해저 광물과 화석 연료, 어류와 같은 해양 자원을 탐색하기 위한 수중 활동은 지속적으로 증가할 것이다. 이러한 활동 이외에도, 여러 국가는 수중 방위역량⁵⁴을 강화하고 있다. 따라서 특정 활동에 관한 신뢰성 있는 정보가 부족한 상황을 고려할 때, 공동 수중 상황 인지·이해를 향상시킬 프로젝트가 필요하다.

스프레틀리 군도와 같이 경쟁이 심한 지역에서 서로 다른 수중 활동을 파악하는 수중 공통작전 상황도가 가장 도움이 될 것은 말할 나위도 없는 일이다. 국제 원조 하에 각각의 프로젝트를 구축하는 방안을 고려하는 사람도 있겠지만, 이는 주요 지역 강국으로부터 지원을 얻기는 힘들어 보인다. 그러므로 아태 지역 국가는 현재의 공통작전 상황도에 더욱 강력한 수중 감시 모듈을 탑재하고자 할 것이다. 이는 중국과 홍콩, 싱가포르, 한국과 같은 세계에서 가장 변화한 컨테이너 터미널을 가진 국가에게 특히 의미가 있는 작업일 것이다. 해군과 해안 경비대와 더불어, 항구 오퍼레이터와 해양 물류 산업, 에너지 회사, 심해 광산회사 등이 각각의 프로젝트에 참여할 수 있다.

기술적인 면에서 볼 때, 몇 가지 분야만 간단히 언급하더라도, 센서와 수면-수중 간 통신, 대역폭, 데이터 융합, 변화 탐지기 등에서 새로운 과제를 안고 있기 때문에 넓은 지역의 수중 공통작전 상황도를 만드는 것은 어려운 일이다. 넓은 지역의 수중 공통작전 상황도를 만들면, 후에 다양한 시장에서 요구될 귀중한 이중용도 기술을 동시에 개발할 수 있게 되므로 산학은 이 같은 구상에 관심을 가져야 한다. 여러 아태 지

Plus, 하노이, 2010년 10월 12일, para. 17, <http://www.asean.org/news/item/chairman-s-statement-of-the-first-asean-defence-ministers-meeting-plus-admm-plus-strategic-cooperation-for-peace-stability-and-development-in-the-region-ha-noi-12-october-2010>. Among other things, Expert Working Groups address issues like counter-terrorism, maritime piracy, and peacekeeping. I thank Brigadier Jacques Lemay for bringing this to my attention.

54) For example, the United States is exploring the idea of an underwater shield network to protect naval ships. However, this would likely only be the first step in a more sophisticated underwater defense system. See: Michael Fabey, "U.S. Navy Seeks Undersea Aegis-like System," Aviation Week, October 24, 2012, http://www.aviationweek.com/Article.aspx?id=/article-xml/asd_10_24_2012_p03-02-509975.xml (accessed November 1, 2012).

역 국가는 C4ISR 기술에 주력하면서 각각의 통합과 공유 프로젝트의 핵심을 형성할 수 있다.

3. 주요 수중 기반시설 보호

주요 수중 기반시설 보호를 개선하기 위한 통합 역량은 필연적으로 수중 자산에 대해 점점 커지는 국제적 관심에 뒤따른다. 향후 주요 수중 기반시설에 대한 직접적인 공격이 발생할 것이란 위협 시나리오도 고려해야 한다. 이 같은 공격은 환경 파괴와 공공의 분노를 불러일으키고 재정 및 평판에 피해를 입히는 등 다양한 목적으로 이용될 수 있다. 가해자의 동기와 자원, 전문성에 대해 의심하는 사람도 있겠지만, 광범위한 위협(예 : 자연 재해, 기술적 취약성, 무기 사용)으로부터의 보호는 진지하게 고려해 봐야 할 사안임이 분명하다. 많은 수중 기반시설이 여러 해안 당사자들의 이해관계에 영향을 줄 가능성이 크기 때문에, 각각의 위협을 관리할 필요성으로부터 협력의 기회가 생긴다.

특정 수중 기반시설을 예로 들어 현존 심해 통신 케이블의 지도를 보면(그림 1 참조), 동아시아와 동남아시아, 미국 서부 해안 간 국제 통신 소통량이 몇 개의 분쟁 지대에 매립된 케이블에 의존하고 있음을 분명히 알 수 있다.⁵⁵ 이 매립지를 대체할 곳이 있을 수도 있고 기존에 케이블이 매립된 곳에 중복 매립하는 것도 가능할 것이다. 그러나 케이블은 매립지에 발생하는 공격에 취약하다는 것은 변함없는 사실이다. 이 사안이 전 지역에 있어 중요하기 때문에, 각국은 이러한 중요한 자산을 적절히 보호할 방법을 제공하기 위해 케이블 업체와 함께 자원을 모으는 방법을 고려할 것이다.

55) For more on this, see: Ronald J. Rapp et. al., "India's Critical Role in the Resilience of the Global Undersea Communications Cable Infrastructure," Strategic Analysis, Vol. 36, No. 3 (May-June 2012), pp.375~383.

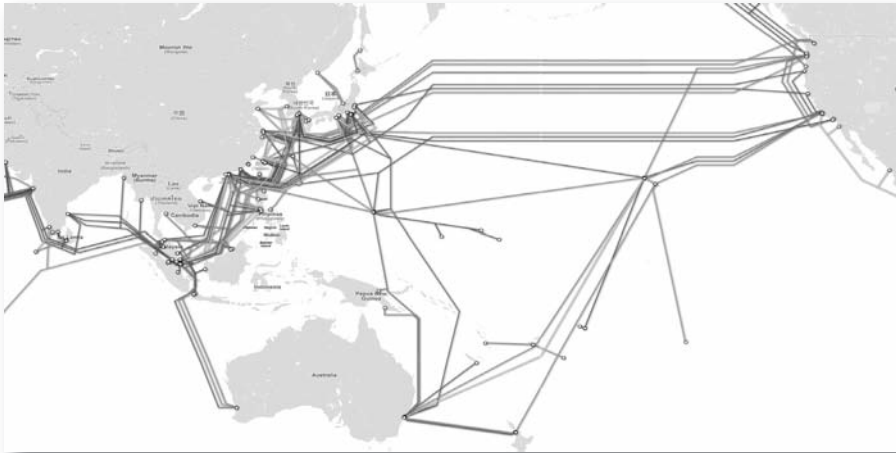


그림 1 : 일부 심해 통신 케이블 매립지

출처 : <<http://www.submarinecablemap.com>>

4. 해양 무역 안보 개선

해양 무역은 아태 지역 번영의 일등 공신이다. 해적과 도둑으로 인한 위협 때문에, 이미 여러 국가가 통합 군대를 조성하고 자원을 모아 각각의 경우에 대응하고 있다. 공공 및 민간 이해당사자 간 통합과 공유도 점차 심각해지는 두 가지 문제를 해결하는데 도움이 될 것이다.

■ **해양 사이버 위기** : 다른 많은 주요 기반시설과 마찬가지로, 해양 무역은 정보 통신기술(ICT)에 의존하고 있다. 정보통신기술 없이, 선박 자동식별 장치와 운항 시스템, 물류 시스템, 선박은 운영될 수 없다. 해양 전용 통신 시스템⁵⁶을 제외하고, 해양 사이버 기반시설은 아직까지 사이버 공격으로부터 큰 피해를 입지 않았다. 그러나 상황은 급격히 변할 수도 있다. 세계에서 가장 변화한 컨테이너 터미널과 더불어, 세계 3대

56) “China hackers enter Navy computers, plant bug to extract sensitive data,” The Indian Express, 1 July 2012, <<http://www.indianexpress.com/news/china-hackers-enter-navy-computers-plant-bug-to-extract-sensitive-data/968897/0>> (accessed 18 October 2012).

컨테이너항 오퍼레이터인 PSA 인터내셔널(PSA International)과 후친슨 항구 지주 회사(Hutchinson Port Holding), 코스코(Cosco)의 소재지는 아태 지역이다. 이 기반 시설 오퍼레이터들에 대한 조직적인 사이버 공격은 아태 지역 너머 멀리까지 파급효과를 가질 것이다. 해양 사이버 공격의 위협을 해결하는 데 있어 해결해야 할 주요 과제는 국제 선박 및 항만시설 보안규칙(ISPS Code)이 디지털 보안 위협보다는 물질적인 위협에 중점을 두고 있다는 사실이다. 이 우려를 고려해, 아태 지역 각국은 주요 해양 기반 시설의 국제적 보안 증진을 도와야 한다. 아태 지역 국가는 해양 사이버 보안 관련 사건에 대해 국제적으로 정보를 교환하고자 설립한 말레이시아 소재 “사이버 위협에 대항하는 다자 간 국제 파트너십(IMPACT)⁵⁷⁾”의 국제 대응 센터를 이용할 수도 있다.

■ **화물의 원격 감시** : 국제 제재의 위반과 불법 물품의 이송은 해양 무역에 직접 영향을 주는 가장 시급한 안보 과제에 속한다. 많은 해양 운송량을 고려할 때, 승선 및 하선 시 화물을 검사하는 것은 실질적으로 문제를 일으킬 수 있다. 따라서 화물 감시는 항구가 아니라 선박이 항구로 접근하는 동안 바다 위에서 실시해야 한다. 해상 화물 감시를 위한 원격 기술에 투자하면, 항구 오퍼레이터는 보다 효율적으로 일할 수 있고 번잡한 항구보다 덜 취약한 환경에서 충분히 일찍 불법 물품을 살펴볼 수 있게 될 것이다. 우리도 알다시피, 여러 아태 지역 국가는 공해상 및 우주기반 감지 기술은 물론 C4ISR에도 투자하고 있다. 이 국가와 함께 원격 화물 감시 클러스터의 핵심을 구축할 수도 있다. 결국, 군사력은 센서와 각 센서를 처리하는 플랫폼에만 의지하지는 않게 될 것이다. 그러나 이를 위해서는 변화 감지와 형태 인지를 위한 첨단 분석기술도 필요하다. 결국, 이 작업을 완수하기 위해서는 화물 오퍼레이터와 공공 기관 간의 순조로운 정보 교환이 필요하고, 이에 따라 공공-민간 정보 교환을 지원할 개념과 기술이 필요하게 된다.

5. 북극해로 개방 준비

북해로의 개방은 아태 지역에 위협과 기회를 동시에 제공한다. 오늘날 여러 국가는 이미 이 기회를 잡고 최북단에 대한 각국의 이해관계도 관찰시키기 위해 준비 중이다. 이로 인한 분명

57) <<http://impact-alliance.org/home/index.html>> (accessed 18 October 2012).

한 경쟁 구도에도 불구하고, 두 가지 사안은 각국이 현명한 해결책을 내놓도록 할 수도 있다:

■ **쇄빙선** : 아무리 긍정적으로 생각해도 북해로는 연중 내내 개방될 수 없다. 해로를 계속 개방하기 위해서는 지속적인 자산 투자가 필요하다. 현재, 러시아는 세계 최대의 원자력 쇄빙선을 보유하고 있다.⁵⁸ 가장 강력한 원자력 쇄빙선의 경우 평균 8~10년의 건축 기간과 10억 달러 이상의 투자비가 든다는 점을 고려할 때, 이러한 쇄빙선은 통합 구상에 완벽히 적합한 것으로 보인다.⁵⁹ 한국, 일본, 및 중국은 세계 최고의 조선업체를 보유하고 있지만⁶⁰ 현재의 정치적 상황으로 볼 때 협력은 불가능해 보인다. 그러나 유럽연합 27개 회원국 또는 미국과 협력하면, 원자력 쇄빙선 건조를 위한 공동 투자 기금의 가능성도 모색할 수 있을 것이다. 나토의 C-17 전략적 공수 작전 기금이라는 구상에 기반해, 원자력 쇄빙선 소함대를 개발해 그 기금에 투자한 모든 파트너 국가에 서비스를 제공할 수 있고, 심지어 예를 들자면, “시간대별 작동” 운영 방안을 통해 기금에 투자하지 않은 국가에도 서비스를 제공할 수 있을 것이다.

58) Baltic Icebreaker Management, *The World Icebreaker and Icebreaking Supply Vessel Fleet* (Helsinki: Baltic Icebreaking Management, 2008).

59) Charles K. Ebinger and Evie Zambetakis, “The geopolitics of Arctic melt,” *International Affairs*, Vol. 85, No. 6 (November 2009), p. 1220; Natalya Kovalenko, “Russia to build new nuclear icebreaker,” *The Voice of Russia*, July 4, 2012, http://english.ruvr.ru/2012_07_04/Russia-to-build-new-nuclear-icebreaker/ (accessed October 18, 2012).

60) In June 2009, the Republic of Korea launched the first icebreaking research vessel, which was built by Hanjin Heavy Industries. See: http://www.hanjinsc.com/eng/pr/notice/notice_view.aspx?noticeID=128&SearchField=&SearchWord= (accessed December 2, 2012). Japan’s Maritime Self-Defense Forces also operate icebreakers, mostly for research purposes. These platforms are built by United Shipping Corporation. See: http://www.u-zosen.co.jp/en_u-zosen/gaiyou.html (accessed December 2, 2012). The Chinese icebreaker Snow Dragon passed the Arctic Ocean from Asia along the coast of Russia to Iceland, where it arrived in mid-August 2012. See: Jon Viglundson and Alister Doyle, “Chinese icebreaker crosses Arctic Ocean. Thaw could open region to oil exploration, shipping,” *Reuters*, August 18, 2012, <http://www.vancouversun.com/technology/Chinese+icebreaker+crosses+Arctic+Ocean/7110681/story.html> (accessed October 18, 2012).

■ **북극의 전자제품** : 북극의 환경은 냉혹하다. 북극에서 운영되는 모든 자산은 반드시 매우 힘든 여건을 접하게 된다. 북극은 특히 현대 방위 장비의 중심 역할을 하는 전자 제품에 가혹하다. 따라서 최첨단 센서와 전자제품, 통신 시스템의 일부는 북극에서는 제대로 작동하지 않는다. 게다가, 북극 환경 하의 에너지 관리는 특히 더욱 어렵다. 또한, 이러한 현상 때문에 북극 환경에 맞게 제품을 개발해야 한다. 일본과 싱가포르, 한국과 같이 최고 방위 전자기술을 갖춘 아태 지역 국가는 이 기회를 탐색하는 데 관심을 가질 것이다. 이 국가들은 미국이나 유럽, 러시아와 협력해 연구개발 활동을 할 수도 있다.

V 결 론

본 논문에서는 안보 역량을 통합하고 공유하면 아태 지역 국가들이 공동으로 협력할 수 있을 것이라 주장했다. 많은 국가들은 재정적 압박 때문에 적절한 방위 역량을 갖춰야 하는 부담감을 나눠서 짊어지기 위해 통합과 공유 방안을 선택할 수도 있다. 그러나 보다 중요한 점은, 통합과 공유를 통해 지역 안정에 중요한 역할을 하는 국가들은 안정화에 동참하거나 계속 기여할 수 있게 된다는 것이다. 이것이 아태 지역의 통합과 공유의 최우선 근거가 되어야 한다. 이 논쟁에 뒤이어, 아태 지역 국가는 미국을 이 지역의 균형을 궁극적으로 잡아주는 국가로서 꼭 붙드는 데 성공할 수도 있다. 이는 즉, 유럽의 주의를 환기시키는 역할을 할 것이다. 만약 유럽이 대서양 연안 국가의 파트너로 남고자 한다면, 유럽연합 27개 회원국은 반드시 아시아 내 미국의 중심 역할에 자극을 받아 아태 지역에서 유럽이 취하고 있는 방위·안보 입장을 다시 검토해 보아야 한다. 결과적으로 통합과 공유는 아태 지역의 장기적 안정과 번영에 이해관계를 가진 새로운 파트너를 끌어들이므로써 아태 지역에 가장 좋은 결과를 가져다 줄 것이다.

이 중요한 비전을 실행하기 위해서는 세 파트너 모두 현재 협력 수준과 틀에서 벗어나 생각해야 한다. 아태 지역 국가는 지역 내 적대감 때문에 고군분투하고 있고 따라서 상호 신뢰와 신용을 갖기 위해서는 갈 길이 멀다. 미국 및 유럽 파트너와의 양자 간 협력은 오늘날 현존하는 문제의 일부분을 타개하는 방법이 될 수 있다. 즉 앞서 언급

한 대로 스마트 국방 구상이 실현될 가능성이 있다. 상호 무역 관계는 양자 간의 관계를 강화했다. 방위와 안보의 통합과 공유는 지역 발전의 기반 역할을 하기 때문에 이러한 관계를 왜곡해서는 안 된다. 그러나 대부분의 아태 지역 국가는 방위 물품의 납품 문제 때문에 미국이나 유럽 국가에 의존하기 쉽다. 따라서 통합과 공유를 고려할 때, 아태 지역 국가는 전략적으로 주의해야 한다.

유럽연합 27개 회원국은 가장 큰 과제에 직면할 것이다. 지금까지, 유럽연합의 전략적 사고는 유럽과 주변국에 집중되었다. 따라서 아태 지역이 유럽연합의 장기적인 경제적 안녕에 있어 중요하다라는 사실로부터 전략적 결과를 도출하기는 쉽지 않다. 또한 유럽연합 회원국은 재정이 빠듯하다. 그러나 유럽연합 회원국이 아태 지역 국가와의 통합과 공유에 대해 진지하게 생각한다면 현 상황을 유리하게 활용할 수 있을 것이다. 공동 구상을 통해, 아태 지역 국가의 정치·재정적 지원에 대한 보답으로 특정 자산은 물론 필수 방위 조직 기반 면에서 유럽연합과 나토가 가진 경험을 공유할 수도 있다. 또한, 유럽연합은 각 프로젝트에 대한 출자를 위해 현재 진행 중인 과학 및 기술 기금을 활용할 수도 있다. 전반적으로 유럽연합 회원국은 국방 산업체의 경쟁적인 수출 비전에서 합의를 봐야 한다. 아태 지역 시장에 공동으로 접근하기 위한 최소한 일부 전략적 지침이라도 합의하지 않는다면 결국 치열하게 경쟁하게 될 것이고, 이에 따라 통합과 공유의 가치는 휴지조각이 될 것이다. 또한, 유럽연합 회원국은 아태 지역 내 미국의 중심축 역할이 아태 지역 내 유럽의 전략적 이해관계와 동일한지를 분석해야 하고, 서로 같은 포부를 갖고 있을 경우 어떤 적절한 조치를 취할지 고려해야 한다.

비록 미국 정부가 이 “현명한 삼각 지대”에서 가장 편안한 위치를 차지하고 있는 것으로 보이지만, 미국도 어려운 문제에 직면하게 될 것이다. 통합과 공유는 아태 지역의 기존 동맹국 순위를 없애고 새로운 협력 형태를 만들 것이다. 그러나 미국은 항상 중국⁶¹과 인도, 러시아와 함께 전반적인 권력 분배에 대한 특정 협력 프로젝트의 영향을 평가하고자 할 것이다. 이 과정에서 미국 정부는 통합과 공유를 통한 보다 긴밀한

61) For a critical assessment of the current U.S. strategy vis-à-vis the Asia-Pacific region, see for example: Lanxin Xiang, “China and the ‘Pivot,’” *Survival*, Vol. 54, No. 5 (October–November 2012), pp.113~128; Robert S. Ross, “The Problem With the Pivot,” *Foreign Affairs*, Vol. 91, No. 6 (November–December 2012), pp.58~69. Among others, Xiang argues that “from Beijing’s perspective,

협력이 아태 지역의 한 국가에 적대적인 인상을 주지 않기 위해 노력해야 한다. 결과적으로 미국은 아태 지역의 모든 이해당사자의 이해관계를 만족시킬 수 있는 전반적인 기반에 대해 고민해야 할 것이다.

Washington's strategy towards Asia has most of the key features of a cold-war strategy" (p.117). Similarly, Ross believes that "the new U.S. policy unnecessarily compounds Beijing's insecurities and will only feed China's aggressiveness" (p.72).

첨부 1 : 일부 유럽연합 회원국의 2005~2011년 방산 품목 수입액

Importers	Suppliers																				Total						
	AUS	AUT	BEL	BRA	CND	CZE	DNK	ESP	FRA	FIN	DEU	ISR	ITA	NDL	NOR	POR	RSA	RUS	SGP	SVK		SWE	CHE	UKR	UK	USA	TRK
AUT											843	36										16					895
BEL						45	66	55	9	66	271	9	66	271		46						31			27		550
BUL			314			94	42	4	4			4	42											14		468	
CYP						20	15					15	15								14		5			140	
CZE		21			8	52	35	5				35	35		3						392		3	60		782	
DEU		3			4	75	42	466	27	42	466	27	42	466							60	64		347		1084	
DNK								47	1	25	1	1	25								125	60	175	133		566	
ESP						215	214	1188	65	214		214	214			18					32	135	52	193		2084	
EST						10	3	2			3	3	3								242	83	54	27		134	
FIN		108	3		6	39	8	66	44	70	11	7	11		7	35				6	6			86		386	
FRA					20	8	18	30	17	76	30	4	30		4						44		150	511		1743	
GRE						1027	8	2091	8	154	162	8	154	162			63				122			25		201	
HUN								5	5	38	5	38	38				2				368	10		83		499	
IRL								4	4	31	4	31	31		4						10			6		57	
ITA	3					40	40	767	39	30	30	30	30		22						44		309	511		1743	
LTU								15	15	42	15	42	42		2								73	25		201	
LUX								12	12	2	2	2	2											27		14	
LVA								5	5	3	88	3	88								13			8		140	
MLT										18	18	18	18											302		26	
NDL	18					2	2	101	12	217	119	3	119		33						301		11			1119	
POL						91	61	139	63	61	220	61	220	10	12						61			36	489	2565	
POR	61					195	33	550	33	190	503	33	190	503									36	220	184	2105	
ROU						1	95	168	95	73	199	95	73	199							8		220	184		976	
SVK						3										1										19	
SVN		8				26	2	16	2	2	2	2	2		2					3				2		84	
SWE						5	5	28	91	14	32	5	32		5	31					136		14	179		469	
UK	5	30				5	5	323	104	47	60	464	60	464	2	2	29				14			1819		3164	
Total	87	170	317	48	294	18	36	386	2105	232	6323	590	1460	2262	96	46	87	446	29	14	1905	407	10	1097	7819	26286	
in %	0%	1%	1%	0%	1%	0%	1%	8%	1%	24%	2%	6%	9%	0%	0%	0%	0%	2%	0%	7%	2%	4%	4%	30%	2		
Intra-EU		170	317			18	36	386	2105	232	6323		1460	2262		46				14	1905		1097		7819	16371	
US																									7819	7819	
Others	87			48	294				590			590			96		87	446	29			407	10		2	2094	

출처 : SIPRI Arms Transfer Database, Importer/Exporter TIV Tables, <http://armstrade.sipri.org/armstrade/page/values.php>

Keep the United States Locked In and Engage Europe: Smart Defense as a Way for the Asia-Pacific Region to Leverage its Strategic Role

Heiko Borchert¹

목 차

- I. Executive Summary
- II. Security and Defense Challenges for the Asia-Pacific
- III. European Security and Defense: Waiting for Smartness
- IV. Asia-Pacific's Road to Smart Defense Cooperation with Europe and the United States
- V. Conclusion

1) Dr. Heiko Borchert is the owner and managing director of Sandfire AG, a Swiss security and defense consultancy. He is a subject matter expert at the Hague Centre for Strategic Studies, co-editor of a series of books on the theory and practice of the Comprehensive Approach, and member of the editorial board of the journal *Zeitschrift für Aussen- und Sicherheitspolitik*. Heiko Borchert studied international relations, business administration, law, and economics at the University of St. Gallen, Switzerland, where he also earned his Ph.D. His main areas of work include security foresight, public-private security cooperation, critical infrastructure protection, energy security, maritime security, cyber security, defense planning, and security sector transformation

I Executive Summary

This paper argues that pooling and sharing of defense capabilities is about tying nations into joint collaborative endeavors. Financial pressure is a motive for pooling and sharing to shoulder the burden of providing adequate capabilities. More important, pooling and sharing can also help ensure that nations that play a critical role for the stability of a region become and remain engaged to help stabilize it. This should be the primary rationale for considering pooling and sharing in the Asia–Pacific region. By following this line of argumentation, Asian–Pacific nations lock in the United States as the region’s ultimate balancer. This, in turn, could serve as a useful wake–up call for Europe. If Europe wants to remain relevant as a transatlantic partner, the U.S. pivot to Asia must prompt the EU27 to reconsider its defense and security posture in the Asia–Pacific region. Pooling and sharing with Asia–Pacific partners might be the only way for Europe to engage in the region. As a consequence, pooling and sharing could prove to be most beneficial from an Asia–Pacific perspective, as it will help bring in new partners that have an interest in the long–term stability and prosperity of the region.

When it comes to defense and security, differences between the European Union (EU) member states and Asia–Pacific could hardly be bigger: Caught in the severest politico–economic crisis of the past decades, EU countries have turned inward to provide domestic stability. They are struggling to address the fallout of the crisis, not least by slashing defense budgets. This has prompted General Hakan Syren, the outgoing Military Committee Chairman, to warn that “a marginalized Europe is not a risk,

but a fact.”² As a consequence it is hardly surprising that European defense capability shortfalls that emerged during the international crisis management operations in the Balkans in the 1990s and have become even more prevalent since then still remain to be tackled. Despite these obvious problems, EU countries are operating in a state of relative geostrategic tranquility compared to other regions of the world.

The Asia-Pacific region, in contrast, is attracting the world's attention for different reasons. Economic progress has turned the region into the new geoeconomic center of gravity. With full pockets, the region's biggest defense spenders have embarked on a spending spree that is likely to overtake total European defense spending by the end of 2012.³ Asian-Pacific countries have managed to remain largely unaffected by the U.S.-European economic and financial crisis, although trade interrelations do not render the region immune to problems that affect its key trading partners. National antagonism, regional tensions, and nationalist policies are still very well alive in the Asia-Pacific region. In addition, several countries are beefing up military capabilities not only to deter neighbors but also for offensive and possibly pre-emptive purposes.⁴ As a consequence, the region looks fragile and in need of an overall security framework to

2) Hakan Syren, “Facing realities – in search of a more European mindset,” Keynote speech delivered at the Cyprus EU Presidency High Level Seminar, Brussels, September 19, 2012, p.3, http://www.consilium.europa.eu/media/1749978/ceumc_keynote_speech_cyprus_presid_seminar_19_sep2012_2012.pdf(accessed October 16, 2012).

3) <http://www.iiss.org/publications/military-balance/the-military-balance-2012/press-statement/> (accessed October 16, 2012). For a detailed assessment of current Asian defense spending patterns, see: Joachim Hofbauer, Priscilla Hermann, and Sneha Raghavan, *Asian Defense Spending, 2000-2011. A Report of the CSIS Defense-Industrial Initiatives Group* (Washington, DC: CSIS, 2012).

4) IISS, *The Military Balance 2012* (London: Routledge, 2012), pp.205~208.

smooth ruffled feathers.

Against this background, a cursory look at both regions might suggest that European insights on defense cooperation do not matter to Asia-Pacific. However, this first impression is wrong. No doubt: EU and NATO nations are talking about pooling, sharing, and role specialization in light of dire economic and financial conditions. But from an Asia-Pacific perspective, the strategic rationale that comes with the notion of Smart Defense – the NATO label for pooling, sharing, and role specialization – is about tying nations into joint collaborative endeavors. In Europe, pooling and sharing is discussed to jointly shoulder the burden of financing scarce defense and security capabilities. In the Asia-Pacific region, Smart Defense could be seen as a means to make sure that outside nations become and remain engaged in the region. This is important to help stabilize the Asia-Pacific region and organize joint activities to settle problems in other parts of the world that will be of growing importance to Asia-Pacific nations that are about to emerge as the world's economic powerhouse. So whereas EU and NATO nations are talking about Smart Defense among “insiders,” Asia-Pacific countries could seize the moment and use Smart Defense to strengthen bonds with “outsiders” from Europe and partners across the Pacific. This puts a particular spot on the role of the United States in both regions. The U.S. pivot to Asia can be seen as the ultimate strategic wake-up call for Europe to engage in pooling and sharing in order to remain relevant as a partner in the United States' key area of interest. Asia-Pacific countries could see value in pooling and sharing as a means to lock in the United States as the region's ultimate balancer and to solidify relations with Washington. As a consequence, both EU and Asia-Pacific countries might have a joint interest in pooling and sharing as a way to advance cooperation among them and with the United States.

II Security and Defense Challenges for the Asia-Pacific

Europe has at least three overriding strategic interests in the Asia-Pacific region. First of all, the region is an important trade partner. Last year, the EU27 exported goods worth €330 billion (21.6% of EU27 exports) to the members of the Asia-Europe Meeting (ASEM) and imported goods worth €532bn (31.6% of EU27 imports) from there.⁵ A more detailed look at bilateral trade relations reveals that the EU27 very much depend on high-technology products from Asian suppliers. ASEM countries, for example, provide over 80% of all EU27 imports of integrated circuits and electronic components and 78% of the EU's electronic data processing and office equipment imports.⁶ In addition, ASEM countries such as China, India, Indonesia, Japan, Singapore, and South Korea are important suppliers of critical raw materials in some case representing 70% and more of the EU's total critical raw material imports (e.g., rare earth elements).⁷

Second, given Asia-Pacific's trade relevance, Europe has a strategic interest in ensured access to the respective markets and the transport corridors leading to and from the region. Most recently, however, there is growing concern that access to the maritime and other domains that

5) Established in 1996, ASEM is an informal cooperation process involving the ten ASEAN countries and China, India, Japan, Mongolia, Pakistan, and South Korea.

6) Figures according to trade statistics provided by the Directorate General for Trade of the European Commission, http://trade.ec.europa.eu/doclib/docs/2006/september/tradoc_113472.pdf (accessed October 17, 2012).

7) European Commission, *Critical Raw Materials for the EU. Report of the Ad-hoc Working Group on Defining Critical Raw Materials* (Brussels: European Commission, 2010): 77~81.

constitute the global commons (e.g., air, space, and cyberspace) will become increasingly contested in the twenty-first century. Finally, developments leading to a deterioration of regional stability in the Asia-Pacific region can be seen as the ultimate threat scenario, because they will significantly affect Europe's other two interests.

Several different trends have the potential to seriously distort regional power relations and thus also affect European interest. From a European perspective, the following five trends can be singled out as the most important:

1. Shifting geostrategic and geoeconomic zones of influence

The reconfiguration of geostrategic and geoeconomic zones of influence in the Asia-Pacific region goes hand in hand with the region's growing economic clout. As Table 1 shows, trade relations with China and the United States matter most across the region. However, at the aggregate level the EU27 is the region's most important trade partner, with an overall trade volume of €775.433 million (2010).⁸

This is only a snapshot of the current situation, however. Future trade projections by the U.S. Citi Bank suggest that China's and India's rise will fundamentally alter trade patterns in the next 40 years. By 2050, China's and India's expected joint share of 27.2% of world trade will be almost three times larger than the combined future trade share of the United States and Germany. This will affect trade corridors. In 2010, intra-

8) Overall trade with the United States accounted for €679,190 million, whereas foreign trade with China was worth €609,732 million. See: http://trade.ec.europa.eu/doclib/docs/2006/september/tradoc_113472.pdf (accessed October 17, 2012).

European trade accounted for 19.9% of world trade, followed by trade among advanced and emerging Asian countries as well as emerging Asian countries and Western Europe. By 2050, trade among advanced and emerging Asian countries is expected to account for 14.9% of the world total, followed by trade among emerging Asian countries (12.5%) and trade between emerging Asian countries and Western Europe (8.3%). Interestingly, trade between Western Europe and North America, which accounted for 5.8% of world trade in 2010, is no longer listed among the world's top 10 trade partnerships in 2050!⁹

Table 1: Major Trade Partners of Selected Asian-Pacific Countries 2011 (in % of total imports and exports)

	Ranking of Trade Partners											
	No 1		No 2		No 3		No 4					
	Import	Export	Import	Export	Import	Export	Import	Export	Import	Export	Import	Export
IND	PRC 12.3	UAE 12.4	UAE 8.8	USA 10.7	CHE 6.3	PRC 7.9	USA 5.8	HKG 4.3				
IDN	PRC 18.7	PRC 13.3	JPN 14.1	JPN 11.3	SGP 7.5	USA 9.7	USA 7.8	IND 8.2				
JAP	PRC 21.5	PRC 19.7	USA 8.7	USA 15.3	AUS 6.6	ROK 8.0	SAU 5.9	TWA 6.2				
MYS	JPN 12.6	SGP 13.4	PRC 12.6	PRC 12.6	USA 10.7	JPN 10.4	THA 6.2	USA 9.5				
PRC	JPN 11.2	USA 17.1	ROK 9.3	HKG 14.1	TWA 7.2	JPN 7.8	USA 7.0	ROK 4.4				
PHL	JPN 11.0	JPN 18.5	USA 10.9	USA 14.8	SGP 8.1	PRC 12.7	ROK 7.3	SGP 8.9				
SGP	MYS 10.7	MYS 12.2	USA 10.7	HKG 11.0	PRC 10.3	PRC 10.4	JPN 7.2	IDN 10.5				
ROK	PRC 16.5	PRC 24.2	JPN 13.0	USA 10.7	USA 8.5	JPN 7.1	SAU 7.0	HKG 5.6				
THA	JPN 20.8	PRC 11.0	PRC 13.3	JPN 10.5	MYS 5.9	USA 10.4	USA 5.9	HKG 6.7				
TWN	JPN 18.6	PRC 27.2	PRC 12.8	HKG 13.0	USA 9.2	USA 11.8	ROK 6.3	JPN 5.9				
VNM	PRC 23.6	PRC 11.1	ROK 13.2	USA 10.9	JPN 10.4	JPN 10.8	TWN 8.6	ROK 4.7				

Country codes: AUS Australia, CHE Switzerland, HKG Hong Kong, IDN Indonesia, IND India, JPN Japan, MYS Malaysia, PHL Philippines, PRC People's Republic of China, ROK Republic of Korea, SAU Saudi Arabia, SGP Singapore, THA Thailand, TWN Taiwan, UAE United Arab Emirates, USA United States of America, VNM Vietnam

Source : <http://www.gtai.de/GTAI/Navigation/DE/Trade/Maerkte/wirtschaftsklima.html> (accessed October 16, 2012)

9) Willem Buiter and Ebrahim Rhabari, *Trade Transformed. The Emerging New Corridors of Trade Power* (New York: Citi Global Perspectives & Solutions, 2011), pp.22~24.

Up to now, trade relations have always been a strong indicator of security relations. Thus the big question is how emerging patterns of future trade corridors will affect security relations in and beyond the region.¹⁰ The Citi Bank study suggests that if the United States and Europe have an interest in remaining relevant actors in the region, now is the time to leverage existing trade partnerships to advance security cooperation.

2. Anti-access and area denial challenges (A2AD)

As the international geostrategic environment is in a state of transition, developments that endanger the freedom of the global commons have caught the attention of strategic communities around the world. The global commons bind together the sea, air, space, and cyberspace domains that are of paramount importance for the free flow of goods, people, resources, and information. Actors that are able to manipulate the quality and the direction of these flows exert strategic influence. This explains the importance of anti-access and area denial challenges (A2AD) that endanger unhindered use of the global commons.¹¹ Right now, Asia-Pacific is ripe with A2AD challenges: For example, rivaling sovereignty claims over marine resources in the South China Sea are threatening maritime stability in one of the world's busiest sea lanes. Chinese investments in dedicated anti-

10) For an in-depth look at possible future development paths, see: Avery Goldstein and Edward D. Mansfield, eds., *The Nexus of Economics, Security, and International Relations in East Asia* (Stanford: Stanford University Press, 2012).

11) For a similar argument, see: Andrew F. Krepinevich, "Strategy in a Time of Austerity: Why the Pentagon Should Focus on Assuring Access," *Foreign Affairs*, Vol. 91, No. 6 (November-December 2012): 58-69; Caitlin Lee, "Planning beyond the pivot," *Jane's Defence Weekly*, October 31, 2012, pp.26~32.

ship missiles and anti-satellite capabilities are reasons of concern with regard to the freedom of action at sea and in space.¹² In addition, ongoing disputes between China and Brazil over environmental standards and iron ore shipping make it clear that A2AD is not only a military problem but also will affect trade relations.¹³ Finally, cyber vulnerabilities that come with hardware and software products constitute another source of contention, with adverse effects on bilateral trade relations and the protection of critical infrastructures.¹⁴

12) Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012* (Washington, DC: Department of Defense, 2012): 6-10. For a more detailed assessment, see also: Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: Department of Defense, 2011), pp.28~32.

13) Leslie Hook and Robert Wright, "China blocks Vale's large iron ore carriers," *Financial Times*, January 31, 2012, <http://www.ft.com/cms/s/0/b0fa84e6-4bf6-11e1-b1b5-00144feabdc0.html#axzz29ZJ49Xlk>; Fayen Wong and Jeb Blount, "Vale/China iron ore ship dispute deepens," *Reuters*, February 2, 2012, <http://mineweb.com/mineweb/view/mineweb/en/page504?oid=144539&sn=Detail&pid=504>; Alison Leung and Randy Fabi, "China's ban on Vale's iron ore carriers costs Chinese firms," *Reuters*, May 10, 2012, <http://www.mineweb.com/mineweb/view/mineweb/en/page504?oid=151218&sn=Detail> (accessed October 17, 2012).

14) Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunication Companies Huawei and ZTE* (Washington, DC: U.S. House of Representatives, 2012); U.S.-China Economic and Security Review Commission, *The National Security Implications of Investments and Products from the People's Republic of China in the Telecommunications Sector* (Washington, DC: U.S.-China Economic and Security Review Commission, 2011).

3. Maritime instability and insecurity

Changing global trade patterns will reinforce the importance of ensured access to maritime sea-lanes in the Asia-Pacific region. This underlines the strategic importance of A2AD challenges. The world's busiest harbors today are in Asia-Pacific. Of the world's ten most important container terminals in terms of throughput, eight are located in Asia-Pacific.¹⁵ In Germany, for example, access to these ports and the respective sea routes is indispensable, as more than 60% of Germany's foreign trade (by value) with India, China, and Japan is shipped.¹⁶

Access to marine resources is another driver for conflicting sovereignty claims over neighboring Exclusive Economic Zones (EEZ). Interests clash mainly over oil and gas resources around the Spratly and Parcel Islands. Estimates vary greatly. Quoting Chinese and other sources, the U.S. Energy Information Agency reports possible oil resources of up to 105 billion barrels and possible gas resources of up to 900 trillion cubic feet.¹⁷ If these resources turned into proved reserves, they would equal approximately the current reserve capacity of Kuwait (oil) and Qatar (gas).¹⁸ As the overall demand for fossil energy in the region is on the rise, we can expect

15) Shanghai leads the list followed Singapore and Hong Kong. See: United Nations Conference on Trade and Development, *Review of Maritime Transport* (Geneva: UNCTAD, 2011), p.89.

16) In 2010, German total foreign trade with China accounted for €130bn, €35bn with Japan and €15bn with India. See: Jahresbericht 2011. Flottenkommando, *Fakten und Zahlen zur maritimen Abhängigkeit der Bundesrepublik Deutschland* (Glücksburg: Flottenkommando, 2011), p.95.

17) <http://www.eia.gov/countries/regions-topics.cfm?fips=SCS> (accessed October 17, 2012).

18) BP, *BP Statistical Review of World Energy* (London: BP, 2012), pp.6, 20.

sovereignty claims over access to these resources to become even fiercer, thus providing a serious source of instability in the region.

4. Urbanization

According to UN projections, the world population is to grow from roughly 7 billion today to around 9.15 billion in 2050.¹⁹ At the same time the distribution between urban and rural population will change dramatically. In 2009 the distribution was about equal. By 2050, around 6.29 billion people will live in urban areas and only 2.86 billion in rural areas. In 2025, the world's top 10 urban agglomeration areas will be home to approximately 230 million people. Of these 10 megacities, seven are to be found in the Asia-Pacific region.²⁰ This will put urban political, economic, and transport infrastructures under severe stress.²¹ In this regard, George Kaplan is right to point out that the “impersonal quality of urban life” can add to the radicalization of people that were attracted by urban areas promising economic success and a better way of living as a consequence, it “is in the megacities of Eurasia principally where crowd psychology will have its greatest geopolitical impact.”²² Prospects of failing megacities in densely

19) Department of Economic and Social Affairs, *World Urbanization Prospects: The 2009 Revision* (New York: United Nations 2009).

20) Tokyo leads the group of megacities in the Asia-Pacific region with 37.1 million inhabitants, followed by Delhi and Mumbai. Dhaka is fifth, followed by Calcutta, Shanghai, and Karachi at ranks eight to ten.

21) See in particular: UN-HABITAT, *The State of Asian Cities 2010/11* (Fukuoka: United Nations Human Settlements Program, 2010), <http://www.unhabitat.org/pmss/listItemDetails.aspx?publicationID=3078> (accessed October 17, 2012).

22) Robert D. Kaplan, *The Revenge of Geography: What the Map Tells Us About Coming Conflicts and the Battle Against Fate* (New York: Random House 2012), p.123.

populated instable coastal areas can thus be seen as a key future threat scenario that will drive future security and defense requirements.

5. Climate change

Climate change can act as a threat multiplier. According to a recent UN-HABITAT report, “75% of all people living in areas vulnerable to sea level rises are in Asia, with the poorer nations most at risk”.²³ If climate change leads to refugees and internal displacement, megacities might have to shoulder an extra burden. In addition, an OECD report analyzing the impact of coastal floods on infrastructures pointed out that 15 out of 20 cities that will be affected by coastal floods by 2070 are located in Asia.²⁴ The consequences are obvious: China, for example, has built most of its import terminals for the supply of liquefied natural gas (LNG) on the east coast, which is likely to be affected by raising sea levels. Finally, climate change could also affect the Arctic region, which would have mixed consequences for Asia-Pacific. On the one hand, the opening up of the Northern Sea route could shorten travel distances from Europe to Asian ports by up to 20 days.²⁵ On the other hand, shipping goods to Asia via the Arctic could shift current shipping patterns towards harbors in the North, there by adversely

23) UN-HABITAT, *The State of Asian Cities 2010/11*, p.184.

24) R. J. Nicholls et. al., *Ranking Port Cities with High Exposure and Vulnerability to Climate Extremes: OECD Environment Working Papers No. 1* (Paris: OECD, 2008), pp.23~27.

25) Charles Emmerson and Glada Lahn, *Arctic Opening: Opportunity and Risk in the High North* (London: Chatham House, 2012), p. 30; Svend Aage Christensen, *Are the Northern Sea Routes Really the Shortest? Maybe a Too Rose-Coloured Picture of the Blue Arctic Ocean: DIIS Brief* (Copenhagen: Danish Institute for International Studies, 2009).

affecting current harbor operators that are mainly located in Southeast Asia.²⁶

Today, concerns about the negative consequences of these and other trends are driving defense spending in the Asia–Pacific region. But the region’s countries can only afford to expand on the current spending spree, if economic progress continues. Most recently, the Asian Development Bank (ADB) has lowered its growth forecast for many Asian–Pacific countries.²⁷ It is unclear if slowing growth is temporary or structural. In any case, the new ADB outlook serves as a reminder that steady economic process is far from guaranteed. Therefore, it is useful to take a more detailed look at current EU and NATO activities to cope with the impact of financial shortages on defense.

III European Security and Defense: Waiting for Smartness

In NATO and EU circles, the ideas of pooling, sharing, and role specialization have been circulating for quite some time. The political momentum in favor of these approaches has been a function of the two organizations’ performance in ongoing international operations.

Technology matters to armed forces, and technology gaps can seriously

26) Joshua H. Ho., “The Arctic Meltdown and its Implication for Ports and Shipping in Asia”, in *Arctic Security in an Age of Climate Change*, ed. James Kraska, (Cambridge, UK: Cambridge University Press, 2011), pp.39~40.

27) Asian Development Bank, *Asian Development Outlook 2012 Update. Services and Asia’s Future Growth* (Manila: Asian Development Bank, 2012), <http://www.adb.org/sites/default/files/pub/2012/adou2012.pdf> (accessed October 17, 2012).

hinder multinational military cooperation. This lesson has been driven home again and again by all international operations conducted since the 1991 Gulf War. Throughout the 1990s, European nations struggled to provide military support for international stability operations in the Balkans. In 1999, NATO Operation Allied Force over Kosovo demonstrated Europe's military ineffectiveness almost brutally.²⁸ As a consequence, the 1999 NATO Washington Summit adopted the Defense Capabilities Initiative to focus on closing gaps in five key areas: deployment and mobility, sustainability and logistics, command and control information systems, effective engagement, and force survivability.²⁹

After September 11, 2001, the pendulum swung in a different direction. Now the focus was on war-fighting and combatting terrorism in regions far away from Europe. Cooperation between the United States and its European allies in Iraq and Afghanistan turned out to be difficult due to the capability gaps that had been identified before but had not been remedied. In addition, the overall geostrategic landscape began to change. As international engagements in the two regions turned from intervention to stabilization, it became amply clear that the United States would act more cautiously with regard to international military operations in coalitions while at the same time preparing a redistribution of its force posture vis-à-vis the Asia-Pacific region that had already been discussed in the 1990s. The new U.S. approach of "controlled engagement"³⁰ was on

28) Anthony H. Cordesman, *The Lessons and Non-Lessons of the Air and Missile War in Kosovo: Executive Summary* (Washington, DC: Center for Strategic and International Studies, 1999).

29) For more on this initiative, see: Department of Defense, *Strengthening Transatlantic Security: A U.S. Strategy for the 21st Century* (Washington, DC: Department of Defense, 2000), p.15.

30) George Friedman, "The Emerging Doctrine of the United States," *Strat for*, October 9, 2012, <http://www.stratfor.com/weekly/emerging-doctrine-united-states>.

display in the first half of 2011 during NATO Operation Unified Protector against Moammar Gaddafi's forces in Libya. Post-operation assessments suggest that many of the shortfalls identified during Operation Allied Force were still at play, in particular in the fields of intelligence, surveillance, and reconnaissance, command and control, specific strike assets, and other core capabilities.³¹ In a very illustrative example of the cumbersome modalities of modern joint warfare, LTC Christopher Bennet, U.S. Air Force

Table 2: NATO's 24 Smart Defense Projects

<ul style="list-style-type: none"> ■ NATO Universal Armaments Interface ■ Remotely controlled robots for clearing roadside bombs ■ Pooling Maritime Patrol Aircraft ■ Multinational Cooperation on Munitions ■ Multinational Aviation Training Center ■ Pooling & Sharing Multinational Medical Treatment Facilities ■ Multinational Logistics Partnership for Fuel Handling ■ Multinational Logistics Partnership-Mine Resistant Ambush Vehicle maintenance ■ Deployable Contract Specialist Group ■ Multinational Logistics Partnership-Helicopter Maintenance ■ Immersive Training Environments ■ Centers of Excellence as Hubs of Education and Training ■ Computer Information Services E- 	<ul style="list-style-type: none"> Learning Training Centers Network ■ Individual Training and Education Programs ■ Multinational Joint Headquarters Ulm ■ Female Leaders in Security and Defense ■ Joint Logistics Support Group ■ Pooling of Deployable Air Activation Modules ■ Theater Opening Capability ■ Dismantling, Demilitarization, and Disposal of Military Equipment ■ Multinational Military Flight Crew Training ■ Counter IED-Biometrics ■ Establishment of a Multinational Geospatial Support Group ■ Multinational Cyber Defense Capability Development
--	---

출처 : Multinational Projects (Brussels: NATO, 2012), http://www.nato.int/nato_static/assets/pdf/pdf_2012_10/20121008_media-backgrounder_Multinational-Projects_en.pdf (accessed October 16, 2012)

31) Tom Withington, "Libya Lessons: NATO hears Calls for Better C2, More Targeting Experts," Defense News, January 25, 2012, <http://www.defensenews.com/article/20120125/C4ISR02/301250006/Libya-Lessons-NATO-Hears-Calls-Better-C2-More-Targeting-Experts> (accessed October 17, 2012).

Europe, told an international conference that Operation Unified Protector saw “nine different countries with aerial refueling capabilities supporting 16 different receiver countries with 27 different types of receiver aircraft.”³²

Against this operational background and in light of the dire consequences of the current economic and financial crisis, NATO and EU countries are again turning to pooling, sharing, and role specialization to overcome existing capability shortfalls. At the 2012 Washington Summit, NATO nations adopted the Smart Defense initiative.³³ Smart Defense builds on the three core principles of prioritization to bring national capability priorities in line with NATO’s needs; specialization “by design” to enable NATO members to concentrate on national strengths and coordinate the respective activities; and cooperation to achieve economies of scale for the provision of the respective capabilities. To advance Smart Defense, General Stéphane Abrial (Supreme Allied Commander Transformation) and Ambassador Alexander Vershbow (Deputy Secretary General) have been appointed as special representatives. Together with the EU and the defense industry, NATO nations will use Smart Defense to achieve progress in the areas outlined in Table 2.

Among EU members, pooling and sharing received a political boost by the 2010 Ghent initiative.³⁴ The “food for thought paper” tabled by Berlin

32) Quoted in: Gareth Jennings, “US tanker force looks to learn Libyan lessons,” *Jane’s Defence Weekly*, October 3, 2012, p.5.

33) For more on this, see: http://www.nato.int/cps/en/natolive/topics_84268.htm? (accessed October 17, 2012).

34) Before the Ghent Initiative, London and Paris adopted a new bilateral defense cooperation treaty that underlined close cooperation in defense industrial matters. See: *UK–France Summit 2010 Declaration on Defense and Security Cooperation*, London, November 2, 2010, <http://www.number10.gov.uk/news/uk-france-summit-2010-declaration-on-defence-and-security-co-operation/> (accessed October 17, 2012).

and Stockholm identified three categories for advanced cooperation: increasing interoperability for capabilities and support structures that are essential for individual nations; exploring opportunities for joint action “where closer cooperation is possible without creating too strong dependencies” (e.g., strategic and tactical air lift); and identifying “capabilities and support structures where mutual dependency and reliance (...) is acceptable in an international role- and task-sharing framework (e.g., military training, test and evaluation facilities).”³⁵ These ideas were picked up by the 2010 EU Council Conclusions on Military Capability Development and have since been taken over for implementation by the European Defense Agency (EDA). Throughout 2011, the EDA worked on identifying possible pooling and sharing projects as outlined in Table 3. Some of these projects are already underway, such as the European Satellite Communication Procurement Cell, for which EDA signed a contract with Astrium as the first provider of commercial SATCOM in September 2012.³⁶ EU Defense Ministers meeting on September 27, 2012, reiterated the importance of pooling and sharing and agreed on developing proposals for a voluntary code of conduct.³⁷

35) *Intensifying Military Cooperation in Europe. Ghent Initiative. Food for Thought Paper*, pp.1~2, <http://www.robert-schuman.eu/doc/actualites/papsweallpoolsharingnot.pdf> (accessed October 17, 2012).

36) http://eda.europa.eu/news/12-09-28/European_Defence_Agency_facilitates_access_to_commercial_SatCom_services_for_Member_States (accessed October 17, 2012).

37) http://eda.europa.eu/news/12-10-02/Ministers_of_Defence_welcome_EDA_s_Pooling_Sharing (accessed October 17, 2012).

Table 3: EDA’s Pooling and Sharing Projects

■ Helicopter Training Program	■ Intelligence Surveillance Reconnaissance (including Space Situational Awareness)
■ Maritime Surveillance Networking	■ Pilot Training
■ European Satellite Communication Procurement Cell	■ European Transport Hubs
■ Medical Field Hospitals	■ Smart Munitions
■ Air to Air Refueling	■ Naval Logistics and Training
■ Future Military Satellite Communications	

Source : EDA’s Pooling and Sharing (Brussels: EDA, 2011), http://www.eda.europa.eu/docs/documents/factsheet/_pooling_sharing_-_301111(accessed December 2, 2012)

Pooling and sharing as well as role specialization build on comparable ideas but can ignite different logics. That is why a convincing strategic rationale and a systematic framework to drive and coordinate defense planning across EU and NATO nations would be needed, but it is still lacking. To be fair: The EU in particular has come a very long way to establish institutions for defense cooperation among its members, and NATO has achieved progress as well (Box 1). The problem is that for the time being, most actions have been driven bottom-up rather than top-down. Thus key strategic capability shortfalls remain unaddressed.

Box 1: The overall EU-/NATO framework to facilitate pooling, sharing, and role specialization.

<p>■ Strategies, Concepts, and Risk Analyses: Agreement about the values nations care for and the interests and norms that drive action is essential to foster cooperation. Up until now, NATO and the EU have played an instrumental role in framing a joint understanding of the challenges that need to be tackled and the ways to achieve common solutions. Joint strategies such as the new NATO Concept or Europe’s Security Strategy are important capstone documents to align national thinking.</p> <p>■ Institutions: The EU and NATO both provide an institutional framework for defense cooperation. Existing bodies and regular meetings facilitate cooperation by enabling the formation of trust. Institutions can also take over specific tasks</p>

and thus support joint international activities in the fields of procurement and defense science and technology. In addition to the political institutions, NATO and the EU also enabled the establishment of joint military structures (e.g., headquarters, joint units), which are an important facilitator at all levels of military decision-making and operation.

- **Operations:** Since the end of the Cold War, NATO and the EU have provided the framework for joint military operations in Europe, Africa, the Greater Middle East, the Mediterranean Sea, and in the Indian Ocean.
- **Tools:** The EU and NATO provide military planning tools to support national defense planning. By devising scenarios for the definition of joint force goals, organizing force generation conferences, and offering planning and review processes, the two organizations work toward the harmonization of defense planning among their members. In doing so, combined work on military standards plays an important role to advance military interoperability.
- **Defense Trade:** The EU and NATO have gone a long way to facilitate defense trade among member nations. Particularly within the EU, nations have worked towards the goal of facilitating mutual defense supplies and lowering barriers for cross-border defense projects. As Appendix A shows, Intra-EU27 defense supplies from 2005 to 2011 accounted for 62% of all defense imports. At the single-nation level, the United States was the biggest supplier (30%), followed by Germany (24%), the Netherlands (9%), France (8%), Sweden (7%), and Italy (6%). Despite the significant ratio of EU-based defense supplies, overall collaborative defense equipment procurement is relatively low and varies significantly among EU nations. In absolute terms (in 2010), the United Kingdom and France spent the most in this category followed by Italy, Germany, and Spain.³⁸

38) United Kingdom: €2,760 million, France: €1,847 million, Germany: €1,398 million, Spain: €703 million. See: *Defence Data: EDA participating Member States in 2010* (Brussels: European Defence Agency, 2012), p.24, http://www.eda.europa.eu/docs/documents/National_Defence_Data_2010_4.pdf (accessed December 2, 2012).

Pooling and sharing build on economies of scale. Several countries join forces either to maintain existing or acquire new capabilities together. By shouldering the burden, each partner is given additional leeway, and the combination creates new added value. The degree of sovereignty transfer varies. NATO's Strategic Airlift Capability based on C-17 Globe master III transport aircraft, the Alliance's AWACS fleet, and the European Air Transport Command can be seen as successful pooling and sharing examples. Role specialization builds on the idea of competitive advantages. A nation specializes in providing a specific capability either because it has a very strategic interest in this capability, has built a reputation in delivering it, or agrees to specialize as part of a bi-/multilateral accord. The latter option, however, which is also labeled specialization by design, has hardly occurred so far. The Czech NATO CBRN battalion is one example of role specialization.³⁹

39) On these and many other issues, see: Tomas Valasek, *Surviving Austerity. The case for a new approach to EU military cooperation* (London: Centre for European Reform, 2012); Jakob Henius and Jacopo Leone MacDonald, *Smart Defense: A Critical Appraisal* (Rome: NATO Defense College, 2012); "The European Air Transport Command. A Successful Example for Pooling and Sharing. Interview with Major-General Jochen Both, first Commander of the EATC 2010-2012," *The Journal of the JAPCC* (Autumn/Winter 2012): 34-38; Jean-Pierre Maulny and Fabio Liberti, *Pooling of EU Member States Assets in the Implementation of ESDP* (Brussels: European Parliament Subcommittee on Security and Defense, 2008); Heiko Borchert and René Eggenberger, "Rollenspezialisierung und Ressourcenzusammenlegung: Wie Europas sicherheitspolitische Fähigkeiten gestärkt werden können" [Specialization and Pooling: How to Strengthen Europe's Security and Defense Capabilities] in Hans-Georg Erhart und Burkhard Schmitt, eds., *Die Sicherheitspolitik der EU im Werden: Bedrohungen, Aktivitäten, Fähigkeiten* (Baden-Baden: Nomos, 2004), 230-244; Rachel Lutz Ellehuus, *Multinational Solutions versus Intra-Alliance Specialization* (Copenhagen: DIIS, 2002); Gilles Andréani, Christoph Bertram, and Charles Grant, *Europe's Military Revolution* (London: Centre for European Reform, 2001).

Pooling and sharing as well as role specialization can be organized on a permanent or ad-hoc basis, thereby following different focus areas (Box 2). Ad-hoc solutions are mostly driven by operational needs, and their configuration depends on overriding political calculations. However, the current fiscal environment is most likely to limit national leeways in terms of ad-hoc pooling or specialization, as the scope of existing military capabilities will be cut back. Thus today's defense budget reductions might inadvertently cause "structural specialization by default."

Box 2: Four different focus areas for pooling, sharing, and role specialization.

- **Task Focus:** In this case, the national level of ambition is the driving force, as it defines the risk that a nation is willing to take when engaging militarily. For example, a nation could focus on early entry forces, the provision of intelligence, surveillance, and reconnaissance or strike assets. When engaging in pooling and sharing with partners, the respective nation will put major emphasis on similarities of political ambitions, strategic culture, and public opinion in favor of the respective tasks.
- **Life Cycle Focus:** The life cycle of defense capabilities covers preparation (e.g., planning, doctrine, science and technology), procurement and recruitment, training and education, development and sustainment of defense-industrial capacities, operations and maintenance as well as all aspects pertaining to the management and development of the respective processes and structures that are needed to run defense establishments. Nations can pool, share, and specialize along the life cycle, for example by focusing on the provision of training facilities or engaging in logistics.
- **Decision-Making Focus:** Readiness in decision-making very much depends on the areas of engagement. Countries ready to support early entry forces will need quick political reaction mechanisms. This should be kept in mind when selecting a partner, as differences in national decision-making can slow and

even prevent joint deployment.⁴⁰

- **Geographic Focus:** Geographic proximity and geostrategic interests can lead to the formation of jointly operated capabilities (e.g., among Scandinavian countries) and can prompt a country to build up special capabilities (e.g., cultural awareness and understanding for what is going on in the neighboring region).

Source : Borchert and Eggenberger, "Rollenspezialisierung und Ressourcenzusammenlegung," pp.234~235.

Structural agreements leading to permanent solutions can mostly be found among nations that share strategic ambitions, work within comparable politico-administrative frameworks, and operate similar assets. The United Kingdom-France agreement on sharing future aircraft carriers is certainly one of the most striking structural arrangements. Other nations, such as the Netherlands, Belgium, and also the Scandinavian countries, have significantly integrated their military units with neighboring countries, which has pushed their cooperation to new levels.⁴¹

So far, progress on delivering tangible effects with pooling, sharing, and role specialization has been "episodic."⁴² As a consequence, EU and NATO nations have not yet succeeded in establishing the capabilities that they collectively do not have.⁴³ This outcome mirrors the lack of political will,

40) Marc Houben and Dirk Peters, *The Deployment of Multinational Military Formations: Taking Political Institutions into Account* (Brussels: CEPS, 2003), <http://www.ceps.eu/book/deployment-multinational-military-formations-taking-political-institutions-account> (accessed October 17, 2012).

41) For a very helpful overview of current examples of structural pooling in Europe, see: Valasek, *Surviving Austerity*, pp.18~19.

42) Valasek, *Surviving Austerity*, p.8.

43) Sven Biscop and Jo Coelmont, *Pooling & Sharing: From Slow March to Quick March? Egmont Security Policy Brief* (Brussels: Egmont Royal Institute for International Relations, 2012), p.2.

which can be explained by the growing divergence on strategic issues that is about to hamper intra-EU and NATO defense cooperation. Furthermore, the existing framework does not yet help to mitigate all risks that come with giving up more sovereignty in defense. For example, there is no guarantee that every nation will adhere to prior commitments and abstain from withdrawing troops that might render multinational capability pools useless; it is still unclear how uncoordinated national spending cuts should yield joint European solutions that close existing capability shortfalls; and robust controlling and auditing processes to evaluate national contribution to pooling and sharing initiatives with a view on jointly agreed availability, deploy ability, and readiness levels remains to be agreed upon.⁴⁴

IV

Asia-Pacific's Road to Smart Defense Cooperation with Europe and the United States

Discussions about possible avenues for smart defense solutions in the Asia-Pacific region should start from the premise that pan-regional trust is low. Some nations enjoy good and stable relations with neighboring partners and other countries across the region. But overall, antagonisms

44) For more on this, see: Valasek, *Surviving Austerity*, pp.21~27; Henius/MacDonald, *Smart Defense*, pp.32~47; Maulny/Liberti, *Pooling of EU Member States Assets in the Implementation of ESDP*, pp.16~18; Claudia Major, Christian Mölling, and Tomas Valasek, *Smart But Too Cautious: How NATO Can Improve Its Fight Against Austerity* (London: Center for European Reform, 2012); Bastian Giegerich, "NATO's Smart Defense: Who's Buying?" *Survival*, Vol. 54, No. 3 (June-July 2012), pp.69~77.

prevail.⁴⁵ For the time being and with the exception of strong bilateral ties, the Asia-Pacific region does not seem ripe for deliberate defense-related role specialization. The remainder of this paper will thus not address this issue. This puts the focus on pooling and sharing, which both depend on multilateral cooperation.

The current track record for multilateral security and defense cooperation in the region is mixed. For example, the failure of ASEAN states to come to an agreement over current disputes in the South China Sea has been interpreted as a serious blow for this regional organization.⁴⁶ Past efforts to use ASEAN to unify defense procurement were of limited success due to diverging views among key members.⁴⁷ By contrast, initiatives like ReCAAP and SHADE (Box 3) prove that successful pan-regional initiatives exist. Despite these “islands of success,” it seems fair to argue that pooling and sharing initiatives that build on a selected number of few partners might seem more appropriate than pan-regional approaches.

45) The sudden worsening of relations between Japan and South Korea is an illustrative case. See: Brendan Taylor, “Japan and South Korea: The Limits of Alliance,” *Survival*, Vol. 54, No. 5 (October–November 2012), pp.93~100.

46) Ian Storey, “China pushes on the South China Sea, ASEAN unity collapses,” *China Brief* XII, No. 15 (August 4, 2012), pp.8~10.

47) In May 2010, ASEAN countries adopted the *Concept Paper on Establishing ASEAN Defence Industry Collaboration*, <http://www.aseansec.org/documents/18471-k.pdf>. See also: Sneha Raghavan and Guy Ben-Ari, “ASEAN Defense Industry Collaboration,” CSIS Defense-Industrial Initiatives Group Current Issues No. 25 (July 2011), <http://csis.org/publication/diig-current-issues-no-25-asean-defense-industry-collaboration> (accessed October 18, 2012); Trefor Moss, “ASEAN’s slow security evolution,” *Jane’s Defence Weekly*, February 29, 2012, pp.30~32.

Box 3: Pooling of Information to Advance Defense and Security Cooperation in the Asia-Pacific Region.

- **Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (Re-CAAP):** ReCAAP serves as an information exchange platform to fight piracy and armed robbery by facilitating communication, analyzing incidents, facilitating capacity building efforts, and cooperating on joint exercises as well as other activities. Seventeen contracting parties established ReCAAP in September 2006 (Bangladesh, Brunei, Cambodia, China, Denmark, India, Japan, South Korea, Laos, Myanmar, the Netherlands, Norway, Philippines, Singapore, Sri Lanka, Thailand, and Vietnam). The ReCAAP Information Sharing Center (ISC) maintains a secure web-based information system for disseminating information among all contracting parties on a 24/7 basis.
- **Shared Awareness and Deconfliction (SHADE):** The goal of SHADE is to advance cooperation in the field of counter-piracy operations in the Gulf of Aden and the Western Indian Ocean. SHADE focuses on information exchange to improve joint situational awareness and joint situational understanding. The initiative also involves several international organizations and the maritime industry. SHADE meetings are held at the premises of the Combined Maritime Forces (CMF) in Bahrain. Twenty-seven nations support SHADE and the CMF (Australia, Bahrain, Belgium, Canada, Denmark, France, Germany, Greece, Italy, Japan, Jordan, Republic of Korea, Kuwait, Malaysia, the Netherlands, New Zealand, Pakistan, Portugal, Saudi Arabia, Seychelles, Singapore, Spain, Thailand, Turkey, UAE, United Kingdom, and the United States).

Sources : <http://www.recaap.org/Home.aspx>; <http://combinedmaritimeforces.com>(accessed: October 18, 2012)

For pooling and sharing to lift off in the Asia-Pacific, it is necessary to develop a different rationale than in Europe. In Europe, the provision of defense capabilities in times of fiscal austerity is the main driver. As a consequence, the focus is on reorganizing existing defense cooperation

among EU and NATO members to become more efficient. In the Asian-Pacific region, the situation is different. Economic progress and current security challenges are driving defense spending. Economic efficiency is a secondary issue, at least for the moment. In addition, there is a need for partners to help advance regional security. The U.S. pivot to Asia provides an opportunity for Asia-Pacific nations to join forces with Washington to make sure that the United States will remain engaged in the region as a balancer that could mitigate differences between some of the region's aspiring powers.

Currently, U.S. foreign policy is in a stage of transition. Washington has made it clear that the Asia-Pacific region will be the new focus area. But it remains to be seen whether the U.S. commitment will match the quality of its strategic engagement established in Europe after the Second World War. Thus, at least some Asian-Pacific nations have an interest in strengthening bonds with the United States. These nations could use bilateral pooling and sharing as a means to create an interlocking web of collaborative defense initiatives. If this idea were to bear fruit, it would also force European nations to come to terms with their defense and security posture in a region that is vital for EU27 trade relations. Therefore, pooling and sharing between Asian-Pacific nations and the United States could pull European nations towards cooperation as well. The fact that the EU nations are cash strapped could make things more difficult but might also open doors for new financing schemes with Asia-Pacific nations.

When considering areas for pooling and sharing, existing capabilities, local defense industrial capacities and ambitions, and the role of outside defense suppliers must be analyzed. The resulting picture is complex:

1. Unlike European nations, ASEM members depend mainly on outside defense suppliers (Appendix B). From 2005-2011, total defense imports by ASEM members were worth \$62,959 million. At around 42% the

lion's share fell on Russia, with deliveries worth \$26,267 million. U.S. supplies accounted for 25% (\$15,943 million), and the EU27's share was worth \$13,152 million (21%). In contrast, Intra-Asia-Pacific defense supplies only accounted for \$4,158 million or 7%, with China taking the lead (\$3,440 million). There are signs of growing interest in exploring joint defense procurement.⁴⁸ But for the time being, pooling and sharing must take into account the interests of these foreign suppliers – a situation that is likely to make it more difficult for local governments to find multilateral solutions.

2. So far, European defense suppliers have been competing among themselves and with the United States and Russia for access to Asia-Pacific defense markets. If pooling and sharing is to advance European interest as well, thought should be given to the idea of joint European export activities. Table 4 shows that at least on paper there is room for cooperation among European defense suppliers. Although European companies have supplied a broad spectrum of weapon systems to Asia-Pacific countries, several clusters could emerge, as will be discussed below.
3. Suppliers are only one part of the equation, however. We also need to take into account defense industrial capacities and ambitions of Asia-Pacific nations when considering pooling and sharing options:⁴⁹

48) A notable example is the Next Generation Fighter Project pursued by Indonesia and South Korea. See: Trefor Moss, "Asia's Next Fighter Project," *The Diplomat*, July 14, 2011, <http://thediplomat.com/flashpoints-blog/2011/07/14/asia-next-fighter-project/> (accessed October 18, 2012).

49) Paul Kallender-Umezu, "Japan Strives to Overcome Defense Industrial Base Crisis," *Defense News*, June 24, 2012, <http://www.defensenews.com/article/20120624/DEFREG03/306240003/Japan-Strives-Overcome-Defense-Industrial-Base-8216-Crisis-8217->; Trefor Moss, "Japan's Defense Industry Lifeline," *The Diplomat*, December 31, 2011, <http://thediplomat.com/2011/12/31/japan-s-defense-industry-lifeline/> (accessed November 19, 2012); Jon

- Despite the country's well-known high technology base, **Japan's** defense industry has been suffering so far. But Tokyo's defense posture seems to be changing. As of recently, the country has become much more active, for example by providing defense support to the Philippines, boosting defense ties with Australia, and relaxing rules on defense exports. A recent report by the ministerial Defense Production and Technology Base Research Committee also suggested restructuring the national defense industrial base. Current key procurement projects include the Next Generation Fighter competition, the expansion of its submarine force, and the procurement of new amphibious assets.
- **Indonesia's** defense industry has so far focused on licensed manufacturing. Local capabilities to design and develop military platforms are limited. Nonetheless, the country's ambitions are growing, in particular in the maritime domain. The country has ordered new submarines from South Korea and is working with China to build anti-ship missiles. In addition to developing electronic systems, Indonesia is also focusing on surveillance technologies.
- **Malaysia** disposes of indigenous defense capabilities in lower-level technology areas such as aerospace Maintenance, Repair, and Overhaul

Grevatt, "Japan looks to new defence policy to boost defence industry," *Jane's Defence Weekly*, October 30, 2012, p. 23; Indonesia. IHS Jane's Navigating the Emerging Markets (Surrey: IHS Jane's, 2012); Malaysia. IHS Jane's Navigating the Emerging Markets (Surrey: IHS Jane's, 2012); Republic of Singapore. IHS Jane's Navigating the Emerging Markets (Surrey: IHS Jane's, 2011); South Korea. IHS Jane's Navigating the Emerging Markets (Surrey: IHS Jane's, 2012); Vietnam. IHS Jane's Navigating the Emerging Markets (Surrey: IHS Jane's, 2012); Guy Anderson and Jon Grevatt, "Rich pickings. Emerging markets: Southeast Asia," *Jane's Defence Weekly*, September 19, 2012, pp.20~29; Guy Anderson, "A Changing Game Board: How Competition on the International Defence Market is Shifting" (Surrey: IHS Jane's, 2012); IISS, *The Military Balance 2012* (London: Routledge, 2012), pp.206~208.

(MRO), manufactures small arms and munitions, and is engaged in shipbuilding. For the future, Malaysia puts priority on developing C4ISR technologies and has an interest in unmanned aerial systems. Satellite services, information technology, and simulation systems are among the country's focus areas as well. However, as of recently Malaysia has pushed back the procurement of several key platforms such as the new Multi-Role Combat Aircraft. In contrast, the new Scorpene submarines have been deployed.

- **Singapore** certainly is the region's leader in terms of indigenous defense industrial capabilities. Existing capabilities span a broad spectrum ranging from naval, ground, and air systems (including MRO and engine technologies) to communication systems as well as surveillance, radar, and sensor systems. Unmanned systems round off the country's defense industrial capabilities. Among others, Singapore is investing in foreign systems, such as the KC-135 Tanker replacement, the F-35 fighter jet, and submarines.
- **South Korea** has a mature national defense industrial base that is active in the development of air, land, and sea systems as well as defense electronics with a focus on C4ISR and command and control systems. Despite the country's declared goal of defense-industrial self-reliance, South Korea is investing in new foreign build platforms, such as next-generation fighters and attack helicopters, mainly of U.S. origin.
- **Thailand** has established national capabilities in the fields of MRO for air and land systems and is engaged in naval construction. Developing missile systems using Chinese technologies is said to be among Thailand's future priorities together with C4ISR and unmanned systems.
- **Vietnam's** existing defense industrial capabilities are rudimentary in the fields of air and sea systems. The country's national defense industrial ambitions are limited. But Vietnam has embarked on serious

efforts to improve existing naval and air capabilities

Based on this brief overview, the following clusters could be considered for smart defense cooperation:

- When it comes to **propulsion systems**, Germany is literally the “powerhouse,” with diesel engine deliveries across the region. France and the United Kingdom also play a strong role, in particular in the field of aircraft engines. Energy efficiency is of paramount importance for armed forces in order to reduce the energy footprint and save money due to sky rocketing fuel prices. This could provide interesting opportunities to create MRO hubs, if not already offered by the respective companies. Research and development for energy efficiency could benefit from the fact that Asian countries also play a strong role in the automotive and shipbuilding industries. Smart cooperation in an Asia–Pacific efficient propulsion system cluster would provide attractive incentives for different public and private stakeholders.
- In the **missile segment** France plays a key role. Most of the missile systems delivered to Asia–Pacific customers are built by MBDA,⁵⁰ which is co-owned by EADS, BAE Systems, and Finmeccanica. Buyers’ attention for missile developments is likely to be driven by the use of missiles as effective A2AD tools, the problem of missile proliferation, and the need for missile defense in the region. Consolidating European interests in this field could thus leverage Europe’s supplying power vis-à-vis the United States, China, and Russia. If European nations could agree on jointly marketing key platforms (e.g., vessels, attack aircraft) needed for missile delivery, opportunities could even look better. In addition, missile defense could

50) Other main EU suppliers include Thales and Saab, for example.

also open doors for fruitful cooperation with the United States and even Russia.

- Unlike the missile market, the underwater market for **torpedoes** is more contested among European suppliers. Here Germany's Atlas Elektronik, DCNS from France, and Italy's WASS, a Finmeccanica subsidiary, are competing with each other. As will be discussed below, there are opportunities for cooperation in the underwater segment but most likely on a bilateral supplier-client basis. However, the situation could change, if European companies were to agree on more cooperation to address Asia-Pacific torpedo markets.
- Clustering opportunities could also exist in the **radar** market. Given the growing concern about A2AD, wide area sensors will be much needed. Table 4 makes it clear that France, the Netherlands, and Sweden have delivered different types of radars and electro-optical systems to Asia-Pacific customers. In most cases, the supplier is Thales or Saab. This opens the door for Asia-Pacific nations to think about joint MRO approaches and collaboration to advance future radar technology.
- **C4ISR** emerges as an area of collaboration only for the most advanced defense industrial nations in the Asia-Pacific, such as Singapore, South Korea, and Japan.⁵¹ This would fit well with the current European supplier profile in the radar market and with existing expertise for electro-optical components.

51) Many Asia-Pacific countries have an interest in procuring C4ISR assets, but only few have the necessary industrial capability to enter technology development and production projects. See also: Wendell Minnick, "In Asia, C4ISR Market is Growing," *Defense News*, November 12, 2012, pp.12~14. For a more general analysis, see: Michael C. Horowitz, "Information-Age Economics and the Future of the East Asian Security Environment", in Goldstein/Mansfield, eds., *The Nexus of Economics, Security, and International Relations in East Asia*, pp.211~235.

Table 4: Transfer of Weapon Systems from EU27 Suppliers to Selected ASEM Countries (2000~2011)

	IND	IDN	JPN	MYS	PHL	SGP	ROK	THA	VNM
Air Systems									
Airborne early warning & control aircraft								SWE	
Fighter ground attack aircraft	FRA UK	UK						SWE	CZE
Light transport aircraft	DEU								POL
Light aircraft		FRA						AUT	
Maritime patrol aircraft	DEU	FRA ESP					UK	DEU	POL
Trainer aircraft	POL	DEU			ITA				ROM
Trainer/combat aircraft	UK			ITA		ITA		DEU	CZE
Transport aircraft		ESP		DEU ESP FRA UK				SWE	
SIGINT aircraft							FRA		
ASW helicopter							UK		
Helicopter		FRA	UK	FRA UK	POL		FRA	UK	
Light helicopter	FRA	FRA DEU	DEU	FRA ITA		FRA	DEU	FRA	
UAV		FRA							
Naval Systems									
Frigate		NDL		DEU		FRA			
Offshore patrol vessel								UK	
Patrol craft		DEU							
Submarine	FRA			FRA ESP		SWE	DEU		
Support ship	DEU ITA								
Ground Vehicles/Ground Systems									
Armored bridge-laying system					POL				
Armored engineering vehicle					POL				
Armored recovery vehicle	POL				POL	DEU			
Armored personnel carrier		FRA							
Tank					POL	DEU			
Effectors and Subsystems									
Air defense system		POL							
Anti-tank missile	DEU FRA			FRA		FRA			
Armored vehicle turret		BEL							
Mortar			FRA	FRA					
Self-propelled multiple-rocket launcher		CZE							
Beyond-visual-range air-to-air missile	FRA								
Close-in weapons system							NDL		
Portable surface-to-air missile	FRA	FRA POL					FRA	FRA SWE	
Surface-to-air missile				UK		FRA	DEU FRA		
Anti-ship missile	FRA	FRA		FRA ITA UK			UK	SWE	

	IND	IDN	JPN	MYS	PHL	SGP	ROK	THA	VNM
AS torpedo						SWE			
ASW torpedo	ITA	ITA				ITA SWE			
AS/ASW torpedo	ITA			ITA		ITA	DEU		
Naval gun	ITA	ITA SWE	ITA	ITA SWE		ITA	ITA	ITA	
Self-propelled gun									FRA
Towed gun									ITA UK
Electro-optical search/fire control					NDL				DNK NDL
Radar/Sonar									
ASW sonar	FRA	FRA							DEU
Mine counter measure sonar			UK	FRA					UK
Air/sea search radar		NDL		DEU ITA				NDL	DNK
Air search radar	FRA ITA NDL	FRA		FRA		FRA SWE	NDL	ITA SWE	
Artillery locating radar				SWE		SWE	SWE		
Fire control radar	ITA	NDL		ITA UK			NDL SWE	ITA NDL SWE	
Maritime patrol aircraft radar		FRA	FRA	FRA					UK
Sea search radar	NDL						DNK		
Aircraft electro-optical system				FRA					
Propulsion Systems									
Air refuel system			UK	UK					
Air independent propulsion engine			SWE						
Diesel engine	FRA DEU	DEU DNK FRA	FRA	DEU		DEU	DEU FRA	DEU UK	DEU
Gas turbine			UK						
Turboshaft (engine)		FRA							
Turbofan			UK			DEU		SWE	
Turbojet				UK					

Country codes: BEL Belgium; CZE Czech Republic; DNK Denmark; DEU Germany; ESP Spain; FRA France; IDN Indonesia; IND India; ITA Italy; JPN Japan; MYS Malaysia; NDL Netherlands; PHL Philippines; POL Poland; ROK Republic of Korea; ROM Romania; SGP Singapore; SWE Sweden; THA Thailand; UK United Kingdom; VNM Vietnam

Source : http://armstrade.sipri.org/armstrade/page/trade_register.php (accessed October 18, 2012).

In addition to these bottom-up ideas for defense industrial clustering, additional top-down ideas are needed to advance smart defense cooperation. These top-down ideas should address the long-term security challenges discussed in the first section of this paper and strike a balance between security and prosperity interests. The key to achieve this goal is joint situational awareness and joint situational understanding.

1. Establish global commons-related joint situational awareness and joint situational understanding

The most serious strategic concern for the Asia-Pacific is an A2AD-based arms race that leads to tit-for-tat tactics in various policy fields. This will seriously undermine the freedom of the global commons. Given the overall lack of trust and confidence across the region, this is a probable threat scenario. Activities aimed at furthering joint situational awareness and joint situational understanding can help mitigate the respective risks.

Today's request for comprehensive security and defense solutions translates into the requirement for joint information and knowledge development and sharing between various public and private stakeholders. Progress in the field of common operational pictures (COP) epitomizes this trend. In many ways, the effectiveness of network-enabled forces nowadays depends on their ability to plug and operate on the basis of a joint COP.⁵² So far, most COPs focus on single domains. Given the multi-faceted A2AD threat to the freedom of the global commons, there is a need for a next generation COP.

A Global Commons COP (GC-COP) should bring together information from different domains to provide public and private stakeholders with a holistic view of various activities influencing the freedom of the global commons. In doing so, a GC-COP would enable stakeholders to understand the interplay between the different domains of the global commons. A GC-COP is also essential to evaluate how different decisions affect the relative position of each stakeholder in the global commons. This in turn can improve anticipatory capabilities with regard to these stakeholders' future

52) For more on this see: Ralph Thiele, "Smart Defense in the 21st Century," *The Korean Journal of Security Affairs*, Vol. 17, No. 1 (June 2012), pp.83~99, in particular pp.93~99.

action. In sum, Asia–Pacific countries should see the GC–COP concept as a logical continuation of the exchange of information agreed as part of ASEAN’s confidence building measures⁵³ and as a strategic lever that can be used to cooperate with international partners such as NATO and the EU.

2. Advance underwater situational awareness and situational understanding

Section one discussed various underwater activities that bear the potential for serious rifts between countries. Current underwater activities to exploit marine resources such as minerals at the seabed, fossil resources, and fish will continue to grow as resource demand is on the rise. In addition to these activities, several countries are beefing up underwater defense capabilities.⁵⁴ Given the lack of trusted information regarding these specific activities, there is a need for projects that advance joint underwater

53) “ADMM–Plus: Strategic Cooperation for Peace, Stability, and Development in the Region,” Chairman’s Statement for the First ASEAN Defence Ministers’ Meeting–Plus, Hanoi, October 12, 2010, para. 17, <http://www.asean.org/news/item/chairman-s-statement-of-the-first-asean-defence-ministers-meeting-plus-admm-plus-strategic-cooperation-for-peace-stability-and-development-in-the-region-ha-noi-12-october-2010> (accessed November 23, 2012). Among other things, Expert Working Groups address issues like counter–terrorism, maritime piracy, and peacekeeping. I thank Brigadier Jacques Lemay for bringing this to my attention.

54) For example, the United States is exploring the idea of an underwater shield network to protect naval ships. However, this would likely only be the first step in a more sophisticated underwater defense system. See: Michael Fabey, “U.S. Navy Seeks Undersea Aegis–like System,” *Aviation Week*, October 24, 2012, http://www.aviationweek.com/Article.aspx?id=/article-xml/asd_10_24_2012_p03-02-509975.xml (accessed November 1, 2012).

situational awareness and situational understanding.

It goes without saying that a common operational underwater picture that keeps track of different underwater activities would prove most beneficial in heavily contested areas, such as the Spratly Islands. Although one could consider launching a respective project under international auspices, the idea is unlikely to receive support from key regional actors. Therefore, nations could think about complementing existing common operational maritime pictures with a powerful underwater surveillance module. This would make particular sense in those countries that are home to the world's busiest container terminals, such as China, Hong Kong, Singapore, and South Korea. In addition to navies and coast guards, respective projects could also involve harbor operators, the maritime logistics industry, energy companies, deep-sea mining companies, and others.

From a technical perspective, the creation of wide area common operational underwater picture is tough, as it poses challenging requirements for sensors, above water and underwater communication, bandwidth, data fusion, and anomaly detection, to name just a few areas. Industry and academia should have an interest in such an initiative, as it will enable them to develop valuable dual-use technologies that are much sought after in many different markets. Several Asia-Pacific nations focus on C4ISR technologies and could form the nucleus of respective pooling and sharing projects.

3. Protect key underwater infrastructures

Pooling capabilities to improve the protection of key underwater infrastructures follows logically from a growing international interest in underwater assets. Direct attacks against critical underwater infrastructures

should be taken into account as a future threat scenario. These attacks would serve several purposes such as causing environmental damage, creating public outrage, and creating financial and reputational damages. One can speculate about the motives, resources, and expertise of possible perpetrators, but it seems quite obvious that protection against a comprehensive set of risks (e.g., natural hazards, technical vulnerabilities, use of weapons) should be taken seriously. As many underwater infrastructures would most likely affect the interests of several coastal parties, the need to manage the respective risks could create opportunities for cooperation.

A look at the current map of deep-sea communication cables, to single out a very specific underwater infrastructure (Figure 1), makes it amply clear that global communication traffic between East Asia, Southeast Asia, and the U.S. West coast depends on cables landing at a few hot spots.⁵⁵ There might be alternatives to these landing points, redundancy is certainly also available, but the fact remains that cables are vulnerable to harmful action against these landing points. As this issue is vital to the whole region, countries could consider pooling resources in tandem with cable operators to provide adequate protection measures for these critical assets.

55) For more on this, see: Ronald J. Rapp et. al., "India's Critical Role in the Resilience of the Global Undersea Communications Cable Infrastructure," *Strategic Analysis*, Vol. 36, No. 3 (May-June 2012), pp.375~383.

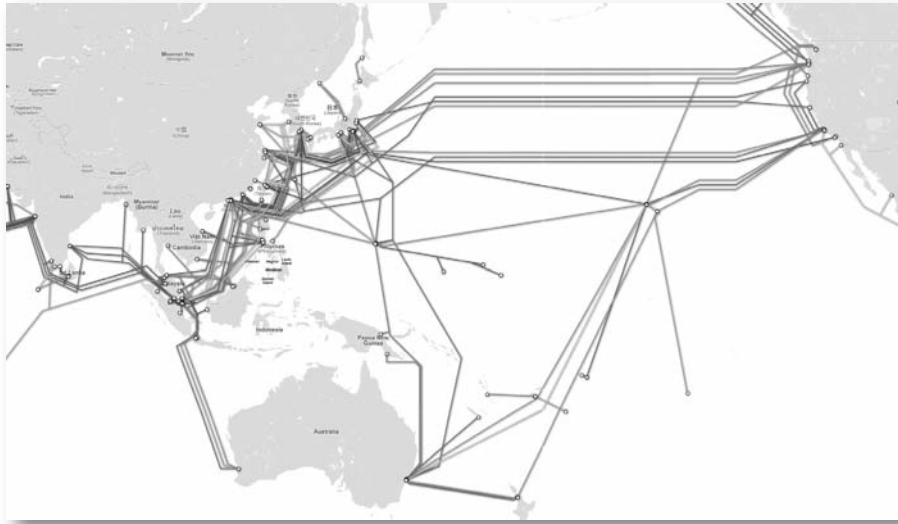


Figure 1: Selected Landing Points of Deep-Sea Communication Cables

Source: <http://www.submarinecablemap.com> (accessed October 18, 2012)

4. Improve the security of maritime trade

Maritime trade is key to the prosperity of the Asia-Pacific region. Risks posed by pirates and robberies have already prompted several countries to join forces and pool resources to address the respective consequences. Pooling and sharing between public and private stakeholders could also help address two issues of growing concern:

- **Maritime cyber risks:** Like many other critical infrastructures, maritimetransport depends on information and communicational technology (ICT). Without ICT harbors, automatic identification systems, navigation, logistics systems, and vessels do not operate. With the exception of dedicated naval communication systems,⁵⁶ maritime cyber

56) “China hackers enter Navy computers, plant bug to extract sensitive data,” *The Indian Express*, July 1, 2012, <http://www.indianexpress.com/news/china-hackers-enter-navy-computers-plant-bug-to-extract-sensitive-data/968897/0> (accessed October 18, 2012).

infrastructures have so far not been at the center of cyber villains' interest. This could rapidly change, however. In addition to the world's busiest container terminals, the Asia-Pacific is also home of PSA International, Hutchinson Port Holding, and Cosco, three of the world's biggest container port operators. Coordinated cyber attacks against these infrastructure operators would have rippling effects far beyond the region. The main challenge in address maritime cyber risks stems from the fact that the International Shipping and Port Security Code (ISPS Code) is focusing on physical rather than digital security risks. By taking up this concern, nations in the region could help advance global security for critical maritime infrastructures. They could use the global response center of the International Multilateral Partnership Against Cyber Threats (IMPACT)⁵⁷ located in Malaysia to set up global information exchanges for maritime cyber security-related incidents.

- **Stand-off cargo screening:** Breaches of international sanctions and the transfer of illicit goods are some of the most pressing security challenges directly affecting maritime trade. Given high maritime transport volumes, cargo screening at points of embarkation and disembarkation runs into practical problems. For this reason, detection should be pushed from harbors to the open sea while ships are approaching harbors. Investing in stand-off technologies for cargo screening at sea would render harbor operations more efficient and could help identify illicit goods early enough to intervene in an environment that is less fragile than busy harbors. As we have seen, several Asia-Pacific countries are investing in C4SIR as well as air- and space-based detection technologies. Together these countries could form the nucleus of a stand-off cargo screening cluster. The resulting

57) <http://impact-alliance.org/home/index.html> (accessed October 18, 2012).

capability would depend not only on sensors and platforms, which help field the respective sensors. Advanced analytics for change detection and pattern recognition would be required as well. Finally, seamless exchange of information between cargo operators and public authorities is needed to accomplish this task, thus prompting a need for concepts and technologies to support public-private information exchanges.

5. Prepare for the opening of Arctic sea routes

The opening up of the North Sea Passage comes with risks and opportunities for the Asia-Pacific region. Already today, several nations are preparing to seize the opportunity and claim their interest in the High North. Despite the obvious rivalry this might cause, two issues could drive countries towards smart solutions:

- **Icebreakers:** Even the most optimistic scenarios do not expect the Northern Sea route to be open all year round. There continues to be a need for assets to keep routes open. Today, Russia maintains the biggest fleet of nuclear icebreakers.⁵⁸ Given average construction time of eight to 10 years and investments costs of more than \$1 billion for the most powerful nuclear icebreakers, these platforms seem perfect for pooling initiatives.⁵⁹ South Korea, Japan, and China are the world's

58) Baltic Icebreaker Management, *The World Icebreaker and Icebreaking Supply Vessel Fleet* (Helsinki: Baltic Icebreaking Management, 2008).

59) Charles K. Ebinger and Evie Zambetakis, "The geopolitics of Arctic melt," *International Affairs*, Vol. 85, No. 6 (November 2009), p.1220; Natalya Kovalenko, "Russia to build new nuclear icebreaker," *The Voice of Russia*, July 4, 2012, http://english.ruvr.ru/2012_07_04/Russia-to-build-new-nuclear-icebreaker/ (accessed October 18, 2012).

leading shipbuilders.⁶⁰ Unfortunately, the current political climate is likely to prevent cooperation. But together with partners from the EU27 and/or the United States, each of them could be interested in exploring the possibility of a joint investment pool to build nuclear icebreakers. Building on the idea of NATO's C-17 Strategic Airlift pool, a nuclear icebreaker flotilla would offer services to all partners investing in the pool and could even serve clients outside the pool on a "power by the hour" model, for example.

- **Electronics in the Arctic:** The Arctic is a harsh environment. Any asset operated there must meet very challenging requirements. This is particularly true for electronics, which are at the heart of modern defense equipment. Some of the most sophisticated sensors, electronics, and communication systems might thus not properly work in this environment. In addition, energy management under Arctic conditions causes extrachallenges. Together, these aspects could create incentives for tailored product developments to satisfy the needs of this operating environment. Asia-Pacific countries with leading defense electronic capabilities such as Japan, Singapore, and South

60) In June 2009, the Republic of Korea launched the first icebreaking research vessel, which was built by Hanjin Heavy Industries. See: http://www.hanjinsc.com/eng/pr/notice/notice_view.aspx?noticeID=128&SearchField=&SearchWord= (accessed December 2, 2012). Japan's Maritime Self-Defense Forces also operate icebreakers, mostly for research purposes. These platforms are built by United Shipping Corporation. See: http://www.u-zosen.co.jp/en_u-zosen/gaiyou.html (accessed December 2, 2012). The Chinese icebreaker Snow Dragon passed the Arctic Ocean from Asia along the coast of Russia to Iceland, where it arrived in mid-August 2012. See: Jon Viglundson and Alister Doyle, "Chinese icebreaker crosses Arctic Ocean. Thaw could open region to oil exploration, shipping," *Reuters*, August 18, 2012, <http://www.vancouversun.com/technology/Chinese+icebreaker+crosses+Arctic+Ocean/7110681/story.html> (accessed October 18, 2012).

Korea might have an interest in exploring this opportunity. They could pool research and development activities in cooperation with U.S., European, or Russian partners.

V Conclusion

This paper has argued that pooling and sharing defense capabilities is about tying nations into joint collaborative endeavors. Financial pressure is a motive for pooling and sharing in order to share the burden of providing adequate capabilities. More importantly, pooling and sharing can help making sure that nations that play a critical role for the stability of a region become and remain engaged to help stabilize it. This should be the primary rationale for considering pooling and sharing in the Asia-Pacific region. By following this line of argumentation, Asia-Pacific nations could succeed to lock in the United States as the region's ultimate balancer. This, in turn, could serve as a useful wake up call for Europe. If Europe wants to remain relevant as a transatlantic partner, the U.S. pivot to Asia must prompt the EU27 to reconsider their defense and security posture in the Asia-Pacific region. Pooling and sharing with Asia-Pacific partners might be the only way for Europe to engage in the region. As a consequence, pooling and sharing could turn out most beneficial from an Asia-Pacific perspective, as it helps bring in new partners that have an interest in the long-term stability and prosperity of the region.

Implementing this bold vision will require each of the three partners to think beyond current levels and frameworks of cooperation: Asian-Pacific countries struggle with regional antagonisms and thus have a long way to

go to nurture mutual trust and confidence. Bilateral cooperation with the U.S. and European partners could help overcome some of today's problems. As was suggested above, there are real opportunities for smart defense initiatives. Mutual trade relations have built strong bonds among them. Pooling and sharing in defense and security should not be allowed to distort these relations, as they serve as the foundation of regional progress. However, this is anything but easy, as most Asian-Pacific countries depend on U.S. and/or European partners for defense supplies. By considering pooling and sharing, Asia-Pacific countries will therefore require strategic caution.

The EU27 will face the biggest challenge. So far, the EU's strategic thinking has focused on Europe and its near abroad. Deducting strategic implications from the fact that the Asia-Pacific region is vital for the EU's long-term economic well-being is not easy. In addition, EU member states are cash strapped. However, if EU members were serious about pooling and sharing with Asia-Pacific partners, they could make a virtue out of the current situation: EU/NATO experience in terms of the necessary defense institutional framework as well as certain assets could be shared in return for political and financial support by Asia-Pacific partners for joint initiatives. In addition, the EU could also tap into existing science and technology funds to co-finance respective projects. Overall, EU member states will need to come to terms with competing export visions for national defense suppliers. Without agreeing on at least some strategic guidelines to jointly access Asia-Pacific markets, companies might end up in fierce competition and thus render the value of pooling and sharing nil and void. In addition, EU members will also have to examine whether the U.S. pivot to Asia is concurrent with Europe's strategic interests there and consider appropriate action in case of diverging ambitions.

Although Washington might seem to enjoy the most comfortable position

in this “smart triangle,” the United States will also have to solve tricky questions. Pooling and sharing might close ranks with existing allies in the region and form new collaboration patterns. But the United States will always want to assess the impact of specific cooperation projects on the overall power distribution with China,⁶¹ India, and also Russia. In so doing, Washington should avoid the impression that closer cooperation via pooling and sharing is directed against single countries in the region. As a consequence, the United States will have to think about an overall framework that could accommodate the interests of all stakeholders in the Asia–Pacific.

61) For a critical assessment of the current U.S. strategy vis-à-vis the Asia–Pacific region, see for example: Lanxin Xiang, “China and the ‘Pivot,’” *Survival*, Vol. 54, No. 5 (October–November 2012), pp.113~128; Robert S. Ross, “The Problem With the Pivot,” *Foreign Affairs*, Vol. 91, No. 6 (November–December 2012), pp. 58~69. Among others, Xiang argues that “from Beijing’s perspective, Washington’s strategy towards Asia has most of the key features of a cold-war strategy” (p.117). Similarly, Ross believes that “the new U.S. policy unnecessarily compounds Beijing’s insecurities and will only feed China’s aggressiveness” (p.72).

Appendix A: Defense Imports 2005~2011 by Selected Countries and EU Member States

Importers	Suppliers																	Total								
	AUS	AUT	BEL	BRA	CND	CZE	DNK	ESP	FRA	FIN	DEU	ISR	ITA	NDL	NOR	POR	RSA		RUS	SGP	SVK	SWE	UKR	UK	USA	TRK
AUT											843	36														895
BEL								45		55	9	66	271			46								27		550
BUL			314					94			4	42											14			468
CYP								20			15											5				140
CZE		21		8			52	75		5	35	392					203		14			3	60			782
DEU		3								47	1	42	466										175			1'084
DNK				4				215		1'188	65	214											52			566
EST					15			10	18	2	3												54			134
FIN				6			39	83		66	44	70	11	7		35							27			713
FRA		108	3				8		18	30	17	76	30	4									86			386
GRE				48	20		1'027		2'091	8	154	162					63					150	1'458			5'303
HUN									5	5	38												83			499
IRL										4	31			4		2							6			57
ITA	3							40		767	39	42	30		22								309	511		1'743
LTU							24			15					2								73	25		201
LUX										12																14
LVA										5		3	88				4							27		140
MLT												18												8		26
NDL	18					2		101	12	217	119	3		33									11	302		1'119
POL				14			91		139	63	61	220	10	12										1'841		2'565
POR	61			24			195		24	550	33	190	503										36	489		2'105
ROU				10			1	18		168	95	73	199										220	184		976
SVK						3					2						1	10								19
SVN		8						26	16					2			25							2		84
SWE				70			5	28		91	14	32		5			31						14	179		469
UK	5	30		138			5	323		104	47	60	464	2										1'819		3'164
Total	87	170	317	48	294	18	36	386	2'105	232	6'323	590	1'460	2'262	96	46	87	446	29	14	1'905	407	1'037	7'819	2	26'286
in %	0%	1%	1%	0%	1%	0%	0%	1%	8%	1%	24%	2%	6%	9%	0%	0%	0%	2%	0%	7%	2%	4%	4%	30%		
Intra-EU		170	317			18	36	386	2'105	232	6'323		1'460	2'262		46				14	1'905		1'037	7'819		16'371
US																								7'819		7'819
Others	87			48	294						590			96		87	446	29				10		2		2'094

Source : SIPRI Arms Transfer Database, Importer/Exporter TIV Tables, <http://armstrade.sipri.org/armstrade/page/values.php> (accessed October 16, 2012).

편집위원

위원장	소장	연제욱
위원	준장	이상철
	서기관	백경희
	사무관	이진희
	사무관	최영선
	사무관	채보정
	중령	박정재
	주무관	조준형
	주무관	이경아
	주무관	인진희
	중위	임승택
간사	주무관	김원기

원고모집

- 분야 : 군비통제와 관련된 논문, 평론, 자료
- 대상 : 제한 없음
- 매수 : A4용지 20~30매 내외
- 보내실 곳 : 140-701 서울시 용산구 이태원로 22(용산동3가 1번지)
국방부 정책기획관실 「한반도 군비통제」 편집담당
- 전화번호 : 02-748-6247

▶ 채택된 원고에 대해서는 소정의 원고료를 지급함.

※ 본 자료는 국방부 홈페이지에도 게재되어 있습니다.

한반도 군비통제

군비통제연구 제52집 2012. 12

발행 국방부 정책기획관실
인쇄 국군인쇄창(12128926)

2012년 12월 28일 인쇄
2012년 12월 31일 발행



Ministry of National Defense

www.mnd.go.kr