情報保護學會論文誌
第 22 卷 第 5 號, 2012. 10

국가 사이버 역량 평가 방법론 연구

강 정 민,[1†] 황 현 욱,[1] 이 종 문,[1] 윤 영 태,[1] 배 병 철,[1] 정 순 영[2‡]
[1]ETRI 부설연구소, [2]고려대학교

A Study on National Cyber Capability Assessment Methodology

JungMin Kang,[1†] HyunUk Hwang,[1] JongMoon Lee,[1] YoungTae Yun,[1]
ByungChul Bae,[1] SoonYoung Jung[2‡]
[1]The Attached Institute of ETRI, [2]Korea University

요 약

세계 각국이 경쟁적으로 사이버 역량 강화를 위하여 다각적인 노력을 경주하고 있는 분위기에 따라 우리나라도 실질적인 국가 사이버 역량 제고의 필요성이 제기되고 있다. 하지만 한국은 사이버 역량 강화의 지표를 제시할 사이버 역량 평가 방법론이 존재하지 않아 실질적인 국가 사이버 역량 수준을 판단하기가 어려운 실정이다. 본 논문은 국가 사이버 역량 강화를 위한 정책 수립에 활용하기 위하여 체계적으로 분석·접근할 수 있는 국가 사이버 역량 평가 방법론을 개발하고 주요 5개국(미국·중국·일본·러시아·한국)의 사이버 역량을 평가하였다. 평가 방법론은 공개된 자료를 기반으로 기반 역량·공격 역량·방어 역량 세 가지 분야의 평가 항목에 따라 절대 평가 또는 상대 평가를 수행하여 평가 대상국별 역량 점수를 정량화함으로서 이해가 쉽도록 하였다. 종합 결과는 미국, 중국, 한국, 러시아, 일본 순으로 평가 되었으며, 평가 결과를 분석한 결과 한국의 사이버 역량 제고를 위하여 기반 역량 분야의 예산·인력에 대한 지속적인 투자, 공격 역량 수준 제고를 위한 전략 마련 및 방어 역량 분야의 패치 보급률 및 보안 관제 수준 제고가 필요함을 알 수 있었다.

ABSTRACT

It is required for us to enhance the national cyber capability as the worldwide countries have been doing effort to strengthen their cyber capabilities. However, we are encountering the difficulty in estimating national cyber capability due to the absence of any cyber capability assessment methodology. This paper presents the national cyber capability assessment methodology which is used for settle up national cyber policy. We also introduce the result of five major nations(US, China, Japan, Russia, Korea)' cyber capability assessment using the proposed methodology. The methodology is developed using open data and includes three areas; base capability, attack capability and defense capability. The assessment result shows the in the order of US, China, Korea, Russia, Japan. As the analysis of that result, in order to enhance the our cyber capability, we recommend that first, cyber budget and human resources for the base capability should be more invested, second, the strategy for attack capability enhancement is strongly required and lastly, the patch ratio and security monitoring level should be upgraded.

Keywords: Cyber Capability, Base, Defense, Attack

접수일(2012년 3월 22일), 수정일(2012년 10월 8일),
게재확정일(2012년 10월 9일)
† 주저자, jmkang@ensec.re.kr
‡ 교신저자, jsy@korea.ac.kr

I. 서 론

세계 강국들은 육·해·공·우주에 이어 제5의 전장으로 꼽히는 사이버 공간에서 사이버 전쟁 준비에 박차를 가하고 있으며, 특히 사이버 강대국으로 알려진 미국과 중국은 사이버 공격을 둘러싼 국가 간 신경전이 날로 거세지고 있는 실정이다 [1] . 이에 따라 국가 사이버 역량 강화의 필요성이 강조되고 있지만 [2] , 역량 강화의 지표를 제시할 사이버 역량 평가 방법론이 존재하지 않아 실질적인 국가 사이버 역량 수준을 판단하기가 어렵다. 학자 또는 특정 개인의 정성적인 사이버 역량 평가는 역량 강화의 필요성을 주장할 수는 있지만 국가 차원의 총체적인 사이버 역량을 점검하기에는 부족할 수밖에 없다 [3] . 세계 최초로 미국은 사이버 역량 평가 방법론을 개발하여 세계 국가들에 대한 평가를 수행함으로서 사이버 강대국다운 면모를 보여주고 있으면서도 평가 방법론은 공개하지 않고 있다. 본 논문은 국가 사이버 역량 강화를 위한 정책 수립에 활용하기 위하여 체계적으로 분석·접근할 수 있는 사이버 역량 평가 방법론을 개발하고 주요 5개국(미국·중국·일본·러시아·한국)의 사이버 역량을 평가·분석한다. 본 논문의 구성은 다음과 같다. II장에서는 미국의 사이버 역량 평가 연구를 살펴보고, III장에서는 공개 자료 기반의 사이버 역량 평가 방법론 개발 내용을, Ⅳ장에서 주요 5개국에 대한 사이버 역량 평가 결과를 설명한다. 마지막으로 Ⅴ장에서 결론을 맺는다.

II. 관련 연구

2.1 Technolytics, 군 사이버 역량 평가(2009년)

Technolytics는 2009년 사이버 무기 및 첩보 활동을 하는 160여개 국가의 군 사이버 역량을 아래 세 가지 분야별로 평가하고 측정 점수 합의 평균으로 종합 역량 등급을 산정하였다 [4] .

- 사이버 역량 목적(Cyber Capabilities Intent): 목적 달성을 위한 목표와 (심리) 상태 (aim and state of mind for a purpose)
- 사이버 공격 역량(Offensive Cyber Capabilities): 전시 특수 목적을 달성하기 위한 능력(군 조직, 기술 우위, 준비도, 지속성)
- 사이버 정보수집 등급(Cyber Intelligence Rating): 새로운 사이버 영역에서의 정보 수집 적응력

〔표 1〕 Technolytics 군 사이버 역량 평가(5점 만점)

국가	역량목적	공격역량	정보수집	역량등급
중국	4.2	3.8	4.0	4.0
미국	4.2	3.8	4.0	4.0
러시아	4.3	3.5	3.5	3.7
인도	4.0	3.5	3.5	3.7
이란	4.1	3.4	3.4	3.6
북한	4.2	3.4	3.3	3.6
일본	3.9	3.3	3.5	3.6
이스라엘	4.0	3.8	3.0	3.6
한국	3.5	3.0	3.2	3.2
파키스탄	3.9	2.7	2.6	3.1

〔표 2〕 Technolytics 군 사이버 공격 역량 평가(5점 만점)

국가	공격 경험	공격역량 등급	정보수집 경험	역량 등급
중국	4.2	3.5	4.2	4.0
미국	4.2	3.6	3.8	3.9
러시아	4.4	3.0	3.2	3.5
인도	3.2	3.5	3.0	3.2
이란	3.4	3.4	3.0	3.3
북한	3.1	3.0	3.0	3.0
일본	3.0	3.3	3.5	3.3
이스라엘	3.8	3.8	3.8	3.8
한국	3.0	3.0	3.1	3.0
파키스탄	3.0	2.9	2.8	2.9

160여개 국가 중 상위 10개국의 평가 결과는 〔표 1〕과 같으며 평가 활용 자료 및 평가 방법론은 공개하지 않고 있다. 단, 중국 사이버 군사력 [5] , 러시아 사이버 군사력 [6] , 이란 사이버 군사력 자료 [7] 이 평가에 활용 된 것으로 추정된다.

2.2 Technolytics, 군 사이버 공격 역량 평가(2009년)

공개된 사이버 공격 사례를 바탕으로 군 사이버 공격 역량을 사이버 공격 경험(Cyber Attack[1] Experience), 공격 역량 등급(Attack Vector Capabilities Rating), 사이버 정보수집 경험(Cyber Intelligence Experience) 분야별로 평가하고 측정 점수 합의 평균으로 종합 역량 등급을 산정하였다. 이란, 이스라엘의 경우 사이버 군 역량 순위가 낮지만 사이버 군 공격 역량 순위는 높은 것을 확인할 수 있

1) Cyber Attack Vector: 공격자가 악의적인 행위를 하기 위하여 컴퓨터, 네트워크, 서버 또는 다른 전자 장치에 접근(접속)할 수 있는 경로 또는 수단

다[표 2].

2.3 Richard A. Clarke, 사이버 역량 평가(2010년)

Richard는 공격(Offense: 타 국가를 공격할 수 있는 능력), 방어(Defense: 공격에 대한 저지 및 완화 능력), 의존(Dependence: 국가기반시설이 네트워크에 연결된 정도, 전산화가 덜 될수록 높음) 세 가지 범주에 대해 저자의 주관적인 판단에 의해 점수를 부여하고 각 분야의 점수를 총합하여 평가를 수행하였다 [8] . Richard는 중국의 높은 방어 능력은 유사시 불필요한 네트워크를 단절시키는 계획 및 능력을 보유하였기 때문이며, 반면 미국은 네트워크가 개인 소유로 운영되어 국가가 단절시킬 계획 또는 능력이 없다고 판단하고 있다. 북한은 중국 보다 쉽고 효과적으로 사이버 공간 연결을 제한 할 수 있을 뿐만 아니라 사이버 공간에 연결된 시스템이 거의 없어서 방어 및 의존 점수가 높다. 저자는 미국 입장에서 사이버전 격차(Cyberwar Gap[2])를 해소하는 방법에 대해 공격 능력 향상은 사이버전 격차를 줄일 수 없으며 또한 네트워크에 대한 의존도를 줄이는 것도 불가하여, 사이버전 격차를 줄이고 사이버 역량을 강화하는 유일한 방법은 방어 능력을 향상 시키는 것이라고 주장한다 [8] .

정량적으로 국가 사이버 역량 평가를 수행한 최초의 미국은 방법론 및 평가 활용 자료를 공개하지 않고 결과만을 공개하고 있다. 이는 사이버 강대국 위상을 계속 유지하고 자국의 사이버 안보 정책을 수립하기 위한 것으로 풀이된다. 우리나라도 사이버 역량 측정 및 평가를 통해 객관적이고 정량적인 자료를 토대로 국가 사이버 안보 정책이 수립 되어야 할 것이며, 이를 위한 사이버 역량 평가 방법론 연구가 필요하다 하겠다.

[표 3] Richard A. Clarke 사이버 역량 평가

국가	공격	의존	방어	총합
미국	8	2	1	11
러시아	7	5	4	16
중국	5	4	6	15
이란	4	5	3	12
북한	2	9	7	18

2) 사이버전쟁 격차(Cyberwar Gap): 사이버전력이 높은 국가가 낮은 국가를 공격하여 심각한 피해를 입히는 반면, 대응 공격에 대한 내성이 강하여 피해가 작음

[그림 1] 사이버 역량 평가 분야

III. 사이버 역량 평가 방법론 개발

사이버 역량은 사이버 공간에서 타 국가를 상대로 공격 및 방어를 수행할 수 있는 평·위기 시 관리 능력을 의미한다. 본 논문에서 국가 사이버 역량은 공개된 자료를 기반으로 기반 역량·공격 역량·방어 역량 세 가지 분야[그림 1]의 평가 항목에 따라 절대 평가 또는 상대 평가를 수행하여 평가 대상국별 역량 점수(10점 만점) 및 순위를 산정하였다. 이를 위해 본 장에서는 대분류(평가 분야), 중분류 및 평가 항목을 도출하고 현실적인 평가 가능여부를 검토하여 평가 항목을 선정하는 절차를 소개하고, 기반, 공격, 방어 역량의 평가 방법을 제안한다.

3.1 평가 항목 선정

3.1.1 단계 1: 대분류 도출

국력은 크게 경성 국력(Hard Power)과 연성 국력(Soft Power)로 나뉜다. 경성 국력의 요소는 학자들마다 다소 상이하지만 일반적으로 영토, 자원, 인구는 필수 요소로 인식되고 있다. 한편 연성 국력의 요소는 물리적으로 정량화하기 어려운 군사력, 외교력, 정치력, 경제력 등이 있다. 현대전을 치루기 위한 군사력은 핵·미사일과 재래식 전력 등 양적으로 측정 가능한 무기체계도 다양한 차별성을 보이고 있는 한편, 부대의 사기 및 지휘관의 자질 등 질적인 차이를 보이는 복잡한 요인들을 포함하고 있어 단순한 계산에 의해 측정하기 어렵다 [9] . 따라서 국력 요소와 사이버 역량 요소를 비교해 봤을 때, 경성 국력은 사이버의 기반 역

[표 4] 국력과 사이버 역량

국력	국력 요소	사이버 역량 요소	사이버 역량
경성 국력	영토	네트워크·시스템	기반 역량
	자원	예산·IT	
	인구	인력·조직	
연성 국력	군사력(무기)	사이버 무기	공격 역량 방어 역량

〔표 5〕 기반 역량 중분류 및 평가 항목

대분류	중분류	평가항목	설명(선정이유/의미)
기반	영토 (인프라)	네트워크 수준	- 사이버 영토를 구성하는 중요한 물리적인 구성요소 - 사이버의 가장 기본적인 인프라 시설
		시스템 수준	
	자원 (예산)	IT 예산 규모	- 사이버 경제력을 나타내고 있는 국가 예산 - 사이버 공격과 방어 무기 및 기술개발 등에 직접 영향
		정보보호 예산 규모	
	인구 (조직)	사이버전사 규모	- 사이버 공격과 방어를 직접 수행할 수 있는 인력 - 사이버 공격과 방어를 위해 편성된 필수 인력
		보충역 규모 (보안업체, IT관련학과, 해커커뮤니티 등)	- 사이버 공격과 방어를 수행하거나 기술개발에 활용할 수 있는 대체 인력 및 조직 - 사이버 위기시 활용될 수 있는 중요 요소(보안업체, IT관련학과, 해커 등)
		컨트롤타워 유무	- 사이버 공격과 방어 행위를 직접 지휘·감독하는 조직 - 사이버 공격과 방어에 대한 종합적인 판단을 수행할 수 있는 조직
	기타	외교적 노력	- 사이버에서 발생되는 상황에 대해 국제 협력 - 사이버 위기에 대한 국제공조 및 협력을 통해 자국의 입장을 대변
		훈련 규모	- 사이버 공격과 방어 행위를 수행하기 위한 인력과 조직에 대한 훈련 - 사이버 위기에 대해 조직적으로 신속하게 대응할 수 있게 하는 중요 요소

량으로, 군사력 핵심인 무기 중심의 연성 국력은 사이버상의 공격과 방어 역량으로 분류하였다〔표 4〕.

3.1.2 단계 2: 중분류 및 평가항목 선정

가. 기반 역량 중분류 및 평가 항목: 본 연구팀은 전통적인 국력의 필수 요소인 영토, 자원, 인구를 사이버상의 개념으로 분석(매핑)하여 아래와 같이 중분류 및 평가항목을 도출 하였다〔표 5〕.

- 영토: 사이버상의 영토는 물리적으로 한정된 공간은 아니지만, 사이버 공간을 형성하기 위한 네트워크, 시스템이 기반시설에 해당됨
- 자원: 자원은 천연자원 등과 같이 국력에서 경제력 등으로 설명되며, 사이버 역량을 확보하기 위한 경제력으로 예산에 해당됨
- 인구: 인구는 국가를 구성하는 가장 중요한 구성요소이며, 사이버 역량에서도 가장 중요한 요소로서 인력의 규모와 조직이 이에 해당됨

〔표 6〕 공격 역량 중분류 및 평가 항목

대분류	중분류	평가항목	설명(선정이유/의미)
공격	정보수집	디지털 스누핑 수준 (Digital Snooping)	- 무선랜 등에서 패스워드나 통신자료를 중간에서 가로채기 위해 네트워크를 감시 - 첩보 수집 능력에 직결
		사회공학기법 (APT) 수준	- 공격대상을 찾기 위해 거점확보 등 취약시스템 정보 수집 - 특정 공격목표를 대상으로 지속적으로 다양한 위협을 생산하는 APT 공격 증가
		트로이목마 수준	- 원격 정보탈취용 악성코드 - 개인정보 및 조직의 중요정보를 절취하는 사례 증가
	침투	취약점 악용 수준	- 시스템 취약점을 발굴・관리・악용하는 기술 - 표적시스템 내에서 은밀한 공격 수행을 위한 필수기술
		웜바이러스 수준	- 스스로를 복제하여 다른 소프트웨어를 감염, 전파, 확산시키는 악성코드 - 무차별 표적 또는 특정 표적을 대상으로 침투하는 악성코드의 실체
		보안시스템 우회 수준	- 코드 난독화, 가상화 등을 이용해 보안시스템을 우회 - 백신 무력화 및 공격 코드 분석을 어렵게 하는 악성코드의 필수 기술
	파괴/ 무력화	DDoS 수준	- 시스템을 마비시키기 위하여 메시지나 트래픽을 폭주시켜 과부하 일으킴 - 빈번하게 발생하는 사이버 공격의 대표적인 형태
		시스템 파괴 수준	- 운영 체제 파괴, 자료 삭제 및 HW 무력화 기술 - 적 교란 및 시스템 운영을 저지하는 핵심 기술
		EMP 수준	- 전자적 방법이나 폭발을 일으켜 강력한 전자파를 발생시키는 장치 - IT장치의 오동작을 유발하는 물리적 신호를 이용한 공격

〔표 7〕 방어 역량 중분류 및 평가 항목

대분류	중분류	평가항목	설명(선정이유/의미)
방어	예방	소프트웨어 보안 인증 수준	- 소프트웨어 보안 취약점을 사전에 검증하는 예방 행위 - 소프트웨어의 취약점을 사전에 예방
		보안서버 보급률	- 인터넷상에서 전송되는 자료를 암호화하여 송수신 - 트래픽 암호화를 통해 디지털 스누핑과 같은 공격을 예방
		패치 보급률 (MS 패치)	- 운영체제나 응용 프로그램에 내재된 보안 취약점 보완 - 취약점을 이용한 공격을 방지하기 위한 필수 기술
	탐지	침입탐지시스템 수준	- 비정상적인 사용, 오용, 남용 등을 실시간으로 탐지 - 네트워크에 접근하는 침해 행위를 탐지하는 필수 기술
		보안 관제 수준	- 각종 침입에 대하여 중앙 관제 센터에서 실시간으로 감시 및 분석, 대응 활동 - 침해 행위를 판별하기 위한 종합 컨트롤 타워 역할
		백신 수준	- 악성코드를 탐지하고 손상된 파일을 치료 - 악성코드를 탐지해서 치료하는 필수 시스템 보안기술
	대응	CERT 활동	- 침해사고 대응을 위한 공식적인 비상 대응팀 - 침해 사고에 대한 예방, 탐지 후 대응 분석을 수행하는 기본적인 조직
		포렌식 전문가	- 디지털 증거를 수집, 보존, 분석하는 활동 - 침해 사고에 대한 증거를 관리하고 행위를 분석
		악성코드 분석 수준	- 감염된 시스템에 존재하는 바이너리 코드를 분석 - 사이버 공격의 원인, 증상을 파악하기 위해 악의적인 행위를 분석하는 필수 기술

- 기타: 과거 전통적인 요소들뿐만 아니라 현대에는 외교, 사이버 훈련 등의 요소들이 국가 사이버 역량에 중요한 요소로 인식되어 지고 있음

나. 공격 역량 중분류 및 평가 항목: 사이버 공격 무기는 임무·기능에 따라 정보 수집, 침투, 파괴·무력화로 분류하며, 각 분야별 평가 항목들은 아래 표와 같으며 현존하는 공격 사례들을 모두 설명할 수 있다〔표 6〕.

다. 방어 역량 중분류 및 평가 항목: 사이버 역량 측정에서 방어의 개념은 국가 차원에서 민・관・군이 평상시 정보통신망을 안전하게 관리하도록 하는 사이버 위협 예방에서부터 탐지, 그리고 복구 대응까지의 종합적인 보안 체계를 의미, NCSC 국가 사이버안전 업무 및 국가 사이버안보 마스터플랜의 내용과 같이 예방・탐지・대응 분야로 분류될 수 있다〔표 7〕.

3.1.3 단계 3: 평가항목 검토

자료 수집 등의 현실적인 평가 가능성을 검토 후 최종 평가항목을 도출하였다〔표 8〕.

3.2 사이버 역량 평가 방법론

3.2.1 기반 역량 평가 방법

기반 역량 평가는 신뢰할 만한 공개 자료를 기반으로 평가 항목별 〔표 9〕의 방법을 따른다. 평가에 활용되는 자료는 기본적으로 신뢰 기관의 자료를 수집하였으며, 수집이 어려운 부분은 언론 보도 자료를 기반으로 하였다. 본 연구는 평가 방법론을 개발하는 것을 목표로 하는 것이며 연구팀의 자료 수집 능력 내에서 언론 자료까지를 신뢰 자료로 간주(가정)하였다. 신뢰 자료 수집은 지속적으로 여러 경로를 거쳐 지속적으로 보완되어야 할 것이다.

3.2.2 공격 역량 평가 방법

자료 수집의 어려움으로 인해 언론기사 등 공개 자료 및 전문가 집단의 상호 의견 교환에 의해 평가 항목 별 전문가 평가 후 최고점과 최저점을 제외한 평균을 계산하여 평가 한다〔표 10〕.

3.2.3 방어 역량 평가 방법

방어 역량 평가는 신뢰할 만한 공개 자료를 기반으로 평가 항목별 〔표 11〕의 방법을 따른다.

〔표 8〕 평가항목 검토

대분류	중분류	평가항목	이상적인 평가	현실적인 평가
기반	영토 (인프라)	네트워크 수준	- 네트워크 투자규모 - 네트워크 대역폭 - 인터넷 연결 개수 - 인터넷 이용자수	- 네트워크 준비지수
		시스템 수준	- 전체시스템 수 - 보안서버 수 - 인터넷 PC 수	- 디지털 경제지수
	자원 (예산)	IT 예산 규모	- 국가 전체 IT 예산	- 공개된 국가 IT 예산
		정보보호 예산규모	- IT 예산중 정보보호 예산	- 공개된 정보보호 예산
	인구 (조직)	사이버전사 규모	- 사이버 공격·방어에 참여하는 인력 수	- 공개된 국가·국방 조직(사이버사령부 등) 인력 수
		보충역 규모	- 국가기관이 사이버 공격·방어에 동원할 수 있는 인력 수	- 정보보안업체 인력 수 - 대학 IT관련학과 인력 수 - 해커커뮤티티 수
		컨트롤타워 유무	- 국가 차원의 사이버 안보를 총괄하는 조직 및 규모	- 대통령실 사이버안보 조직 유무 - 사이버사령부 조직 유무
	기타	외교적 노력	- 사이버 공격 및 방어관련 업무협조가 가능한 국가의 수	- 국제협력기구 참여여부(UN GGE, OECD, 런던회의 등의 참여 및 역할)
		훈련 규모	- 국가차원 훈련과 전문조직의 훈련의 범위, 횟수, 강도, 실제성	- 사이버 대응훈련 규모
공격	정보수집	디지털 스누핑 수준	- 네트워크 감청 및 암호화 정보 해독기술 현 수준	- 네트워크 감청 및 해독 관련 공개 자료 분석을 통한 수준 평가
		사회공학기법 (APT) 수준	- 목표 시스템에 대한 정보 수집 능력 - APT공격에 활용되는 다양한 위협 및 기법	- APT 공격 관련 공개 자료 분석을 통한 수준 평가
		트로이목마 수준	- 정보탈취 기술 수준 - 탈취 정보 전송 기술	- 정보절취 공개사례 분석을 통한 수준 평가
	침투	취약점 악용 수준	- 취약점 퍼징 기술 - 취약점 악용 쉘코드 및 익스플로잇 제작 기술 수준	- 취약점 DB 보유 수준 평가
		웜바이러스 수준	- 악성코드 유포 기술 수준 - 네트워크를 통한 확산 기술 수준 - 다양한 플랫폼 적용 기술 수준	- 윈도우용 악성코드 유포 및 확산 기술 수준 평가
		보안시스템 우회 수준	- IDS, 웹방화벽 등 네트워크 보안시스템 우회 기술 수준 - 백신 등 시스템 보안솔루션우회기술 수준	- 보안시스템 우회 사례 분석 및 수준 평가 - 악성코드 난독화 등 분석 내용 참고
	파괴/ 무력화	DDoS 수준	- 좀비 PC 확보 수준 - 대역폭 소진, 호스트 자원 소진 등 다양한 기술 수준	- DDoS 공격 사례를 통한 수준 평가
		시스템 파괴 수준	- 운영체제 등 SW 파괴 기술 수준 - 바이오스, HDD 등 HW 파괴 기술 수준	- 시스템 파괴 사례 분석을 통한 수준 평가
		EMP 수준	- EMP 제작 기술 수준	- EMP 사용 사례를 통한 수준 평가
방어	예방	소프트웨어 보안 인증 수준	- 소프트웨어 무결성 체계 수립 여부 - 소프트웨어 취약점 검증 기술 수준	- CCRA 참여국 여부 및 수준 평가
		보안서버 보급률	- 보안서버 보급 대수 - 보안서버 보급률	- 보안서버 기관 보급률
		패치 보급률 (MS 패치)	- 보안패치 적용 비율 - 보안패치 소프트웨어 보급률 - 보안패치 체계 수립 여부	- MS 보안패치 소프트웨어 적용 비율
	탐지	침입탐지 시스템 수준	- 침입탐지시스템 보급 대수 - 침입탐지시스템 보급률 - 침입탐지시스템 기술 수준	- 국제공통평가기준(CC) 인증 활용
		보안 관제 수준	- 관제 기관 수 - 관제 기관 비율	- 국가별 관제규모 및 현황
		백신 수준	- 백신의 기술 수준 - 백신 회사 보유 현황	- VB 평가 활용
	대응	CERT 활동	- CERT 운영 기관 수 - 전체 기관 대비 CERT 운영 기관 비율 - 국제 CERT 기관 가입 여부	- FIRST 가입 수
		포렌식 전문가	- 포렌식 기술적 수준 - 포렌식 전문가 자격증 보유 현황 - 포렌식 랩 구축 기관 수	- 포렌식 전문가 자격증 수
		악성코드 분석 수준	- 악성코드 분석기술 수준 - 악성코드 샘플보유 현황 - 악성코드 분석 전문가 보유 현황	- 악성코드 분석 기술 수준 평가

〔표 9〕 기반 역량 평가 방법

평가 항목	내용	자료 평가 방법
네트워크 수준	WEF 네트워크 준비지수	- WEF, The Global Information Technology Report 2010-1011 [10] ・WEF(세계경제 포럼)는 세계 128개 주요국의 정보통신기술 설비 등 주요 인프라, 정보통신기술 사용률 등을 종합적으로 파악해 발표
		- Network Readiness Index 준용
시스템 수준	EIU 디지털 경제지수	- EIU Digital Economy Rankings 2010 Beyond e-readiness [11] ・2000년부터 IBM이 국제적인 경제분석기관(EIU)에 의뢰해 70개 국가별 IT 인프라 품질, 소비자·기업·정부의 ICT를 평가
		- EIU 디지털 경제지수 준용
IT 예산 규모	각 국의 IT 예산	- 〔미〕 예산관리국의 IT 예산보고서(http://www.whitehouse.gov/omb/budget) - 〔중〕 전국인민대표회의예산보고서(http://www.npc.gov.cn) - 〔일, 러〕 한국무역투자진흥공사(KOTRA)(http://www.globalwindows.org) - 〔한〕 기획재정부
		- 각국에서 발표하는 IT 예산 준용 〔이하 LH 계산법〕 - Min, Max 값 제외한 값들의 평균 및 등급범위(평균/3) 계산 - L = 평균 - (등급범위/2), H = 평균 + (등급범위/2) - S: (H + 등급범위) 이상 - A: H ~ (H + 등급범위) - B: L ~ H - C: (L - 등급범위) ~ L - D: (L - 등급범위) 이하
정보보호 예산 규모	각 국의 정보보호 예산	- 〔미〕 예산관리국의 IT 예산보고서(http://www.whitehouse.gov/omb/budget) - 〔중〕 공업정보화부(http://www.miit.gov.cn) - 〔일〕 총무성(http://www.soumu.go.jp) - 〔러〕 정보통신산업진흥원(http://www.itfind.or.kr) - 〔한〕 기획재정부
		- 각국에서 발표하는 정보보호 예산 준용 - LH 계산법
사이버 전사 규모	사이버 전사 수	- 〔미〕 美 '사이버 전투군' 5만여 명 배치('10.05.24, 조선일보) - 〔중〕 "사이버전만큼은 미국에 안 밀린다" 중국, 후진타오 지시 - 〔일〕 N/A - 〔러〕 미래기획 작년자료 - 〔한〕 사이버사령부 독립...인력 2배확대('11.04.19, 한국일보)
		- 언론을 통해 발표되는 사이버전사 수 - LH 계산법
보충력 규모	보충력 수	- 〔미〕 한겨레, 미국사이버사령부 전문병력만 5000명('10.02.21, 한겨레) - 〔중〕 '제3차 세계대전' 사이버전쟁 시작됐다('09.06.16, 주간조선) - 〔일〕 N/A - 〔러〕 N/A - 〔한〕 지식정보보안분야 인력현황(KISA 보고서)
		- 언론을 통해 발표되는 보충력(해커) 수 - LH 계산법
컨트롤타워 유무	대통령실의 사이버안보 조직, 국방사이버사령부 조직유무	- 〔미〕 오바마 정부의 정보보호전략('09.09.06, 디지털타임즈), 미 사이버사령부 창설('09.06.24 한겨레) - 〔중〕 중국 인민해방군 사이버 사령부 창설('10.07.22, 경향신문) - 〔일〕 〔7.7대란〕 국가별 사이버부대는('09.07.10, 아시아경제) - 〔러〕 〔7.7대란〕 국가별 사이버부대는('09.07.10, 아시아경제) - 〔한〕 대통령 직속 사이버보안기관 필요('11.07.12, 디지털타임스), 軍사이버사령부 11일 창설('10.01.08, 조선일보)
		- 컨트롤타워는 대통령실의 사이버안보 조직과 국방 사이버사령부 조직의 유무 - S: 2개 존재, B: 1개 존재, D: 부재
외교적 노력	국제회의 활동	- UN GGE, OECD, 런던회의 참여여부 ・OECD(경제협력개발기구) 정보보호 분과는 정보통신분야 최고 의결기구인 정보통신위원회와 연계해 개최되며 2008년 서울대회에서는 47개국 장관들이 참석, 국가정보보호 지수 개발 추진
		- S: 3개회의 모두 참여 - A: 2개(UN GGE, 런던회의) 참여 - B: 2개(OECD, UN GGE 또는 런던회의) 참여 - C: 1개 참여 - D: 참여 없음
훈련 규모	사이버 훈련 규모	- 〔미〕 美, 사이버공격 대응 훈련..新전략 첫 시험대('10.09.28, 조선일보) - 〔중〕 CNSecurity 중국기술수준파악 보고서(정보제공서비스) - 〔일〕 美 국토안보부 '사이버 훈련'에 日 첫 참가('10.10.04, 세계일보) - 〔러〕 N/A - 〔한〕 정부, 사이버 위기대응 통합훈련실시('11.11.04, 연합뉴스)
		- S: 국제적인 훈련 실시 - A: 범국가 차원의 훈련 실시 - B: 일부기관이 참여하는 훈련 실시 - C: 타국 훈련에 참가 - D: 훈련 부재

〔표 10〕 공격 역량 평가 방법

평가항목	내용	자료
		평가방법
디지털 스누핑 수준	디지털 스누핑 현황 및 전문가 의견	- 〔미〕 구글 '스트리트뷰' 결국 불법 판결…국내는?('11.07.02, 지디넷코리아) - 〔중〕 中 휴대전화 도청 바이러스 급증..1천 3백만대 감염돼('11.09.10, 민중의 소리) - 〔일〕 N/A - 〔러〕 김영진 외 3명, 국가 전산망 보안관제 업무의 효율적 수행방안에 관한 연구(정보보호학회 논문지) - 〔한〕 N/A
		- 자료를 기반으로 한 전문가 판단
사회공학기법 (APT) 수준	APT 공격 현황 및 전문가 의견	- 〔미〕 스턱스넷과 유사한 새 악성코드 발견('11.10.19, 동아일보) - 〔중〕 CNSecurity 중국기술수준파악 보고서(정보제공서비스) 등 - 〔일〕 N/A - 〔러〕 N/A - 〔한〕 N/A
		- 자료를 기반으로 한 전문가 판단
트로이목마 수준	정보유출형 악성코드 현황 및 전문가 의견	- 〔미〕 N/A - 〔중〕 CNSecurity 중국기술수준파악 보고서(정보제공서비스) 등 - 〔일〕 N/A - 〔러〕 중국·러시아 미국 내 사이버 공격 벌여('11.11.04, 프레시안) - 〔한〕 N/A
		- 자료를 기반으로 한 전문가 판단
취약점 악용 수준	취약점 악용 현황 및 전문가 의견	- 〔미〕 National Vulnerability Database, http://nvd.nist.gov/home.cfm - 〔중〕 CNSecurity 중국기술수준파악 보고서(정보제공서비스) 등 - 〔일〕 N/A - 〔러〕 Russia 익스플로잇 코드 모음 사이트, http://www.opennet.ru - 〔한〕 인터넷 스톰센터, http://nchovy.kr
		- 자료를 기반으로 한 전문가 판단
웜바이러스 수준	웜바이러스 현황 및 전문가 의견	- 〔미〕 씨만텍분석보고서, "Stuxnet 웜 분석 자료" - 〔중〕 CNSecurity 중국기술수준파악 보고서(정보제공서비스) 등 - 〔일〕 N/A - 〔러〕· SEO Sploit Kt, 러시아에서 제작된 웹익스플로잇 툴킷 (http://blog.ahnlab.com/asec/366) ·다양한 Exploit Pack(Mpack, BleedingLife, Black hole exploit pack 등) 제작 (http://coderant.egloos.com/5428735) ·Gleg 사의 SCADA 익스플로잇 도구 배포 및 업그레이드 - 〔한〕 N/A
		- 자료를 기반으로 한 전문가 판단
보안시스템 우회 수준	보안시스템 우회 현황 및 전문가 의견	- 〔미〕 씨만텍분석보고서, "Stuxnet 웜 분석 자료" - 〔중〕 CNSecurity 중국기술수준파악 보고서(정보제공서비스) 등 - 〔일〕 N/A - 〔러〕 QR 코드로 감염되는 안드로이드 악성코드 발견('11.10.12, 데일리시큐리티) - 〔한〕 N/A
		- 자료를 기반으로 한 전문가 판단
DDoS 수준	DDoS 현황 및 전문가 의견	- 〔미〕 팔레스타인 해킹공격 당해…미국이 배후?('11.11.02, 지디넷코리아) - 〔중〕 CNSecurity 중국기술수준파악 보고서(정보제공서비스) 등 - 〔일〕 일본발 DDoS 공격, 국내 전산망 뒤흔들다('08.12.18, 전자신문) - 〔러〕 미 주요기관, 중·러시아 해커들에 당하기도('09.07.08, 조선일보) - 〔한〕 N/A
		- 자료를 기반으로 한 전문가 판단
시스템 파괴 수준	시스템 파괴 현황 및 전문가 의견	- 〔미〕 ·소련 70년만에 붕괴 왜? 미국의 트로이 목마 바이러스 때문('10.03.21, 일간스포츠) ·핵시설 공격 파괴 악성코드 제작, "美·이", 이란 핵시설 Stuxnet 공격('11.01.16, 연합뉴스) - 〔중〕 사이버스파이, 미 주요 인프라 해킹('09.04.09, 보안뉴스) - 〔일〕 N/A - 〔러〕 사이버스파이, 미 주요 인프라 해킹('09.04.09, 보안뉴스) - 〔한〕 N/A
		- 자료를 기반으로 한 전문가 판단
EMP 수준	EMP 현황 및 전문가 의견	- 〔미〕 軍 전자기기 무력화 EMP탄 전력화 수준('11.03.07, 조선일보) 손영동, iWar P174~175 - 〔중〕 美 군사개입 막아라, 中 EMP탄 개발중('11.07.23, 세계일보) - 〔일〕 N/A - 〔러〕 충청도 상공에 터트리면 대한민국 OFF('11.05.08, 중앙선데이) 미 전자기파 폭탄에 무방비('08.07.24, 동아일보) - 〔한〕 충청도 상공에 터트리면 대한민국 OFF('11.05.08, 중앙선데이) EMP탄 기술 국내 첫 개발('09.07.07, 문화일보)
		- 자료를 기반으로 한 전문가 판단

〔표 11〕 방어 역량 평가 방법

평가항목	내용	자료 평가방법
소프트웨어 보안 인증 수준	CCRA 참여국 여부	- http://www.commmoncriteriaportal.org/ccra/members ・CCRA는 공통평가기준 기반의 상호인정협정을 의미하며 사실상 국제규범으로 자리 잡고 있으며, 2011년 현재 26개국이 참여하여 하고 있음
		- CCRA 참여: S, 미참 B
보안서버 보급률	인구 백만 명당 보안서버 대수	- WEF, The Global Information Technology Report 2010-1011
		- Secure Internet Servers/million pop 항목 점수 준용 - LH 계산법
패치 보급률 (MS 패치)	감염률 통계 활용	- Microsoft Security Intelligence Report Volume 11 in the first half of 2011(http://www.mirosoft.com/sir) ・전 세계적으로 가장 범용적 운영체제인 MS의 윈도우 기반 감염률을 기준으로 패치 보급률을 계산
		- (100 - 감염률) / 10
침입탐지시스템 수준	국제공통평가기준 (CC) 인증 활용	- http://www.commmoncriteriaportal.org/products ・CC는 국제공통평가 기준으로 정보보호제품 평가에 국제 기준으로 자리 잡음 ・EAL 기준은 가장 높은 등급인 EAL7에서 가장 하위 등급인 EAL1로 분류되어 있으며, 국가별 인증 최고 등급은 EAL4 이하만을 상호인정하기로 합의된 상태로 상호인정의 최고 등급인 EAL4가 기준이 되었음
		- 인증제품 有: 6, 無: 4 - 인증제품 5개 이상: +2 - EAL4 이상: +2
보안관제 수준	국가별 보안관제 현황 분석	- 김영진 외 3명, 국가 전산망 보안관제 업무의 효율적 수행방안에 관한 연구(정보보호학회논문지) - 이연수 외 3명, 주요국의 사이버안전관련 법・조직체계 비교 및 발전방안 연구(국가정보연구)
		- 국가 단위 관제 有: 6, 無: 4 - 차세대 기술 개발: +2 - 네트워크 통제 원활: +2
백신 수준	Virus Bulletin 평가 결과 활용	- http://www.virusbtn.com/vb100/archieve/test?id=160 ・Virus Bulletin은 매년 개최되는 최대 규모의 백신 컨퍼런스로서 1년에 상시 백신 평가를 수행하고 있음 ・RAP는 백신의 최신 악성코드 진단율을 의미
		- RAP(Reactive and Proactive) 점수 / 10
CERT 활동	각 국가의 FIRST 가입 단체수	- http://www.first.org/members/teams ・FIRST는 국제침해사고대응팀 협의체로서 국제적 침해사고대응기관 간 정보공유 및 협력기구임
		- LH 계산법
포렌식 전문가	EnCE 포렌식 자격증 국가별 인원수	- EnCE Referral(http://www.guidancesoftware.com/EnCE-Referral.htm) ・전세계 포렌식 도구의 Defactor 표준으로 자리잡은 Encase의 자격검증테스트로서 포렌식 전문가의 기본적인 자격증
		- LH 계산법
악성코드 분석 수준	분석 보고서 수준	- 〔미〕 시만텍, TELUS, VB, 맥아피, 트렌드마이크로 분석 보고서 등 - 〔중〕 지앙민(JiangMin) 분석 보고서 등 - 〔일〕 FFR(Yarai 백신) 분석 보고서 등 - 〔러〕 카스퍼스키 분석 보고서 등 - 〔한〕 안랩, 이스트소프트, 하우리 악성코드 분석 보고서 등
		- 자료를 기반으로 한 전문가 판단: S, A, B, C, D

IV. 주요국 사이버 역량 평가

본 장은 주요 5개국(미국, 중국, 일본, 러시아, 한국)의 사이버 현황을 조사하고 III장의 역량 평가 방법을 이용하여 각 국가의 사이버 역량을 평가하였으며, 평가 결과에 대한 분석 내용을 소개한다.

4.1 주요국 현황

〔표 12〕 미국 사이버 현황

대분류	중분류	평가항목	현황
기반	영토 (인프라)	네트워크 수준	- 5.33(5위)
		시스템 수준	- 8.41(1위)
	자원 (예산)	IT 예산 규모	- 3천3백조원(3조3천억 달러)
		정보보호 예산 규모	- 7조3천억(73억 달러)
	인구	사이버전사 규모	- 5만명
		보충력 규모	- 8만8000명
		컨트롤타워 유무	- 사이버안보 조정관직을 신설하여 콘트롤타워 역할 수행 - 미국 국방부가 별도로 운영해온 조직을 통합 전략사령부(STRATCOM)산하에 사이버 사령부 신설
	기타	외교적 노력	- UN GGE, OECD, 런던회의에 참석
		훈련 규모	- 격년으로 국가차원의 사이버보안 훈련인 CyberStorm 실시, 2010년 9월에 실시되는 CyberStorm III에는 미국 내 11개 주정부, 12개국 60개 사기업 참여
공격	정보수집	디지털 스누핑 수준	- 에슐론(Echelon), 구글 등 디지털 도감청 수행 추정
		사회공학기법 (APT) 수준	- Stuxnet, Duqu 개발 추정
		트로이목마 수준	- N/A
	침투	취약점악용 수준	- CVE, SecurityFocus 등 세계적인 취약점 DB 운영
		웜바이러스 수준	- Stuxnet에 포함된 취약점 이용 기술, 확산 기술 및 SCADA 장치에 취약점 적용 기술
		보안시스템 우회 수준	- Stuxnet에 포함된 보안 제품 우회 기술(메모리 인젝션, 루트킷 기술 등)
	파괴/ 무력화	DDoS 수준	- 팔레스타인 인터넷 서비스 마비의 배후로 미국, 이스라엘 지목
		시스템 파괴 수준	- 구 소련의 천연가스 파이프 자동제어 시스템 파괴
		EMP 수준	- 피해반경이 6.8km에 이르는 EMP탄 개발 중
방어	예방	소프트웨어 보안 인증 수준	- CCRA 참여 有
		보안서버 보급률	- 1234.1(Secure Internet Servers/million 점수)
		패치 보급률 (MS 패치)	- Infection Rate : 1분기(5.6), 2분기(5.6)
	탐지	침입탐지시스템 수준	- 인증제품 有, 인증제품 5개 이상, EAL4 이상
		보안관제 수준	- 국가 단위 관제 有 - 차세대 기술 Einstein 개발
		백신 수준	- RAP: 84.3
	대응	CERT 활동	- 59개 기관
		포렌식 전문가	- 1,200명
		악성코드 분석 수준	- 시만텍, TELUS, VB, 맥아피, 트렌드마이크로 유료 보고서

〔표 13〕 중국 사이버 현황

대분류	중분류	평가항목	현황
기반	영토 (인프라)	네트워크 수준	- 4.35(36위)
		시스템 수준	- 4.28(56위)
	자원 (예산)	IT 예산 규모	- 4조 6천억
		정보보호 예산 규모	- 2조 1천억
	인구	사이버전사 규모	- 5만명
		보충력 규모	- 100만명
		컨트롤타워 유무	- 국가의 사이버보안 업무는 국무원 중심으로 수행 - 군사업무는 인민해방군 총참모부 직속의 '인터넷 기초총부'라는 사이버사령부 창설
	기타	외교적 노력	- UN GGE, OECD, 런던회의에 참석
		훈련 규모	- 사이버 남군(30여명) 공격과 사이버 홍군 방어 훈련
공격	정보수집	디지털 스누핑 수준	- 정부 주도의 광범위한 도감청 수행 가능 추정
		사회공학기법 (APT) 수준	- 오로라 작전: 구글 해킹사건에 중국정부기관 개입 - 네이트 해킹: 3,500만명 개인정보유출 피해발생
		트로이목마 수준	- Rejoice, Gh0st, 회색비둘기 등의 기능: 키로깅, 음성녹음, Cam 녹화, 터미널원격제어, 시스템관리, AV제품 우회 등
	침투	취약점 악용 수준	- http://sebug.net ・SecurityFocus DB 및 자체 DB 보유 ・2011년 11월 현재 19,440여개 공개 - http://WooYun.org ・중국내 103개 대형 사이트 취약점 공개 ・2011년 11월 현재 2,254개 공개 - 기타 개인 블로그 및 사이트에 공개
		웜바이러스 수준	- 향피우는 팬더(2006년): 수만 대 컴퓨터 감염
		보안시스템 우회 수준	- 보안 시스템 우회 기술 공개, 블랙마켓 거래 - 패킹 전문 업자 활동
	파괴/ 무력화	DDoS 수준	- Netbot, 강시 도깨비 등 많은 유료/무료 도구 존재 - 청부형 DDoS 공격 증가
		시스템 파괴 수준	- 美 전기시설망 시스템 파괴 프로그램 설치
		EMP 수준	- 대만과의 분쟁 발생 시 미국 개입을 막기 위해 전자기파 탄두 개발 중 - 중국은 미국에 대한 군사기술 열세를 뒤집기 위해 추진한 일명 '자객의 검' 프로그램을 통해 EMP탄을 제작(30~40Km의 낮은 고도에서 동작)
방어	예방	소프트웨어 보안 인증 수준	- CCRA 참여 無
		보안서버 보급률	- 1.2(Secure Internet Servers/million 점수)
		패치 보급률 (MS 패치)	- Infection Rate : 1분기(2.4), 2분기(2.3)
	탐지	침입탐지시스템 수준	- 인증제품 無
		보안관제 수준	- 국가 단위 관제 有, 네트워크 통제 용이
		백신 수준	- RAP: 41.7
	대응	CERT 활동	- 4개 기관(CMCERT/CC, CNCERT/CC, HKCERT, Huawei NSIRT)
		포렌식 전문가	- 15명
		악성코드 분석 수준	- 커뮤니티 등에서 악성코드 분석 활발

〔표 14〕 일본 사이버 현황

대분류	중분류	평가항목	현황
기반	영토 (인프라)	네트워크 수준	- 4.95(19위)
		시스템 수준	- 7.85(16위)
	자원 (예산)	IT 예산 규모	- 3조 6천억 원
		정보보호 예산 규모	- 860억 원
	인구	사이버전사 규모	- N/A
		보충력 규모	- N/A
		컨트롤타워 유무	- 컨트롤 타워 부재 - 내각관방 중심으로 정보보안 업무 수행 - 정보보안을 강화하기 위하여 육상, 해상, 공중에 분리되어 있던 부대를 통합하고 사이버부대 설립
	기타	외교적 노력	- OECD, 런던회의에 참석
		훈련 규모	- 미국 사이버스톰 훈련에 2010년부터 참가
공격	정보수집	디지털 스누핑 수준	- N/A
		사회공학기법 (APT) 수준	- N/A
		트로이목마 수준	- N/A
	침투	취약점 악용 수준	- idefense 취약점 정보 확보 추정
		웜바이러스 수준	- N/A
		보안시스템 우회 수준	- N/A
	파괴/ 무력화	DDoS 수준	- 사용자 PC에 동시접속 프로그램 설치
		시스템 파괴 수준	- N/A
		EMP 수준	- N/A
방어	예방	소프트웨어 보안 인증 수준	- CCRA 참여 有
		보안서버 보급률	- 519.6(Secure Internet Servers/million 점수)
		패치 보급률 (MS 패치)	- Infection Rate : 1분기(2.7), 2분기(2.1)
	탐지	침입탐지시스템 수준	- 인증제품 無
		보안관제 수준	- 국가 단위 관제 有
		백신 수준	- N/A
	대응	CERT 활동	- 17개 기관
		포렌식 전문가	- 5명
		악성코드 분석 수준	- FFR(http://www.fourteenforty.jp) 분석

〔표 15〕 러시아 사이버 현황

대분류	중분류	평가항목	현황
기반	영토 (인프라)	네트워크 수준	- 3.69(77위)
		시스템 수준	- 3.97(59위)
	자원 (예산)	IT 예산 규모	- 1조 3천억(13억 달러)
		정보보호 예산 규모	- 1천억(약 2억 달러(비국방 과학기술 지원 예산))
	인구	사이버전사 규모	- 7,700명
		보충력 규모	- N/A
		컨트롤타워 유무	- 컨트롤 타워 부재 - 연방보안국(FSB : Federal Security Service of the Russian Federation)을 중심으로 수행
	기타	외교적 노력	- UN GGE, OECD, 런던회의에 참석
		훈련 규모	- N/A
공격	정보수집	디지털 스누핑 수준	- SORM 이용 통신정보 도감청 가능
		사회공학기법 (APT) 수준	- N/A
		트로이목마 수준	- 제우스(Zeus) 이용 고객계좌 탈취, 온라인뱅킹 사기
	침투	취약점 악용 수준	- 러시아 익스플로잇 모음 사이트 http://www.opennet.ru
		웜바이러스 수준	- Gleg사는 SCADA 익스플로잇 도구도 출시
		보안시스템 우회 수준	- 안드로이드 악성코드에 난독화 적용
	파괴/ 무력화	DDoS 수준	- 키르기스스탄, 에스토니아, 그루지아 등 DDoS 공격
		시스템 파괴 수준	- 美 전기시설망 시스템 파괴 프로그램 설치
		EMP 수준	- 러시아 슈퍼EMP 설계 - 러시아 과학자들 북 EMP 개발 도움
방어	예방	소프트웨어 보안 인증 수준	- CCRA 참여 無
		보안서버 보급률	- 10.5(Secure Internet Servers/million 점수)
		패치 보급률 (MS 패치)	- Infection Rate: 1분기(6.7), 2분기(6.0)
	탐지	침입탐지시스템 수준	- 인증제품 無
		보안관제 수준	- 국가 단위 관제 有 - 네트워크 통제 용이
		백신 수준	- RAP: 88.9
	대응	CERT 활동	- 1개 기관
		포렌식 전문가	- 0명
		악성코드 분석 수준	- 카스퍼스키 분석

〔표 16〕 한국 사이버 현황

대분류	중분류	평가항목	현황
기반	영토 (인프라)	네트워크 수준	- 5.19(10위)
		시스템 수준	- 7.94(13위)
	자원 (예산)	IT 예산 규모	- 3조 2천668억
		정보보호 예산 규모	- 2천633억
	인구	사이버전사 규모	- 1000여명
		보충력 규모	- 14,000명
		컨트롤타워 유무	- 사이버사령부는 국방 사이버 지휘통제를 중심으로 사이버공간에서의 군사작전 임무 수행
	기타	외교적 노력	- UN GGE, OECD, 런던회의에 참석
		훈련 규모	- 매년 을지연습기간에 범정부 차원의 사이버위기대응 훈련 실시
공격	정보수집	디지털 스누핑 수준	- N/A
		사회공학기법 (APT) 수준	- N/A
		트로이목마 수준	- N/A
	침투	취약점 악용 수준	- N/A
		웜바이러스 수준	- N/A
		보안시스템 우회 수준	- N/A
	파괴/ 무력화	DDoS 수준	- N/A
		시스템 파괴 수준	- N/A
		EMP 수준	- '09년 EMP 방호시스템 설치 계획 발표, 진전 없음 - ADD는 100m내 모든 첨단무기 무력화시킬 수 있는 초보 단계 EMP탄 성능 실험에 성공, 2014년까지 1Km 이내에 영향 끼치는 EMP탄 개발 예정
방어	예방	소프트웨어 보안 인증	- CCRA 참여 有
		보안서버 보급률	- 926.7(Secure Internet Servers/million 점수)
		패치 보급률 (MS 패치)	- CCM : 1분기(30.1), 2분기(19.8)
	탐지	침입탐지시스템 수준	- 인증제품 有 - EAL4 이상
		보안관제 수준	- 국가단위 관제 有
		백신 수준	- RAP: 81.9
	대응	CERT 활동	- 7개 기관
		포렌식 전문가	- 57명
		악성코드 분석 수준	- 안랩, 이스트소프트, 하우리 악성코드 분석

4.2 사이버 역량 평가

4.2.1 평가 결과

〔그림 2〕는 주요 5개국에 대한 사이버 역량 평가 결과를 보여준다. 공격 역량 평가는 전문가 7명(정보보안 분야 경력 10년 이상, 자체 전문가 평가위원회 구성)이 평가를 실시하였으며, 평가 항목별 최고/최저 점수를 제외한 나머지 5명의 평가 결과 합의 평균으로 평가하였다.

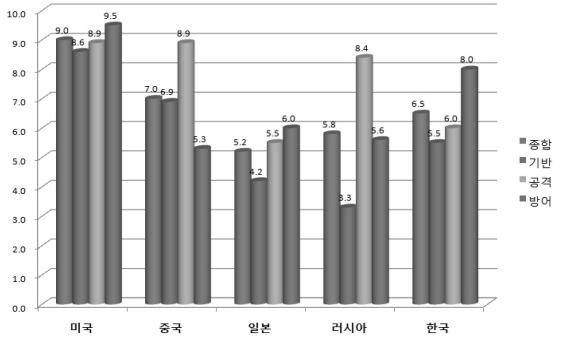
4.2.2 한국의 사이버 역량 제고를 위한 제언

〔그림 3〕은 5개국에 대한 사이버 역량 평가 순위를 나타낸다. 평가 결과를 분석한 결과 한국의 사이버 역량 제고를 위해 다음과 같이 세 가지를 제안한다.

첫째, 기반 역량 분야의 예산·인력에 대한 지속적인 투자가 필요하다. 한국은 기반 역량 분야에서 네트워크 수준 및 시스템 수준에서 선진화된 기반을 구축했음에도 불구하고, 정보보호 예산과 인력의 절대 규모 수준에서 미국·중국을 넘어서기는 어려우나 지속적인

사이버 역량 평가 시스템(CCSS v1.0)												
대분류	중분류	평가항목	평가					점수				
			미국	중국	일본	러시아	한국	미국	중국	일본	러시아	한국
기반역량	영토(인프라)	네트워크 수준	5.3	4.3	4.9	3.6	5.1	5.3	4.3	4.9	3.6	5.1
		시스템 수준	8.4	4.2	7.8	3.9	7.9	8.4	4.2	7.8	3.9	7.9
		영토(사이버 인프라) 역량						6.9	4.3	6.4	3.8	6.5
	자원(예산)	IT 예산 규모	S	A	B	D	B	10.0	8.0	6.0	2.0	6.0
		정보보호 예산 규모	S	S	D	D	D	10.0	10.0	2.0	2.0	2.0
		자원(예산) 역량						10.0	9.0	4.0	2.0	4.0
	인구(조직)	사이버전사 규모	S	S	D	D	D	10.0	10.0	2.0	2.0	2.0
		보충력 규모	S	S	D	D	D	10.0	10.0	2.0	2.0	2.0
		컨트롤타워 유무	S	B	D	D	B	10.0	6.0	2.0	2.0	6.0
		인구(조직) 역량						7.5	6.5	1.5	1.5	2.5
	기타	외교적 노력	S	S	B	S	S	10.0	10.0	6.0	10.0	10.0
		훈련 규모	S	B	C	D	A	10.0	6.0	4.0	2.0	8.0
		기타 역량						10.0	8.0	5.0	6.0	9.0
기반 역량								8.6	6.9	4.2	3.3	5.5
공격역량	정보수집	디지털 스누핑 수준	9.1	8.6	5.6	7.2	6.0	9.1	8.6	5.6	7.2	6.0
		사회공학기법(APT) 수준	8.9	9.0	5.0	8.0	6.7	8.9	9.0	5.0	8.0	6.7
		트로이목마 수준	8.7	9.2	5.4	8.5	6.1	8.7	9.2	5.4	8.5	6.1
		정보수집 역량						8.9	8.9	5.3	7.9	6.3
	침투	취약점 악용 수준	9.0	9.2	6.0	8.5	5.9	9.0	9.2	6.0	8.5	5.9
		웜바이러스 수준	8.8	9.0	4.8	9.0	5.9	8.8	9.0	4.8	9.0	5.9
		보안시스템 우회 수준	8.7	8.9	4.6	8.7	5.8	8.7	8.9	4.6	8.7	5.8
		침투 역량						8.8	9.0	5.1	8.7	5.9
	파괴/무력화	DDoS 수준	8.9	9.0	6.2	8.9	6.9	8.9	9.0	6.2	8.9	6.9
		시스템 파괴 수준	8.8	8.4	4.6	8.2	5.6	8.8	8.4	4.6	8.2	5.6
		EMP 수준	9.1	8.4	7.2	8.8	5.2	9.1	8.4	7.2	8.8	5.2
		파괴/무력화 역량						8.9	8.6	6.0	8.6	5.9
공격 역량								8.9	8.9	5.5	8.4	6.0
방어역량	예방	소프트웨어 보안 인증 수준	S	B	S	B	S	10.0	6.0	10.0	6.0	10.0
		보안서버 보급률	S	D	B	D	S	10.0	2.0	6.0	2.0	10.0
		패치 보급률(MS 패치)	9.4	9.7	9.7	9.3	7.5	9.4	9.7	9.7	9.3	7.5
		예방 역량						9.8	5.9	8.6	5.8	9.2
	탐지	침입탐지시스템 수준	10.0	4.0	4.0	4.0	8.0	10.0	4.0	4.0	4.0	8.0
		보안 관제 수준	8.0	8.0	6.0	8.0	6.0	8.0	8.0	6.0	8.0	6.0
		백신 수준	8.4	4.1	0.0	8.8	8.1	8.4	4.1	0.0	8.8	8.1
		탐지 역량						8.8	5.4	3.3	6.9	7.4
	대응	CERT 활동(FIRST 가입수)	S	D	S	D	C	10.0	2.0	10.0	2.0	4.0
		포렌식 전문가	S	C	D	D	S	10.0	4.0	2.0	2.0	10.0
		악성코드 분석 수준	S	A	B	A	A	10.0	8.0	6.0	8.0	8.0
		대응 역량						10.0	4.7	6.0	4.0	7.3
방어 역량								9.5	5.3	6.0	5.6	8.0
총점(10점 만점 기준)								9.0	7.0	5.2	5.8	6.5
순위								1	2	5	4	3

〔그림 2〕 사이버 역량 평가 결과



〔그림 3〕 사이버 역량 평가 순위

투자가 필요하다고 판단된다.

둘째, 공격 역량 수준 제고를 위한 전략 마련이 시급하다. 공격에 무게 중심을 둔 강대국 수준에 비해 한국은 방어에 치중을 하여 공격 역량이 낮은 실정이다. 군사력, 경제력, 기술력 측면에서 강대국인 미국은 기반, 공격, 방어 분야에서 모두 강한 사이버 역량을 보여준다. 한편, 미국과의 대립각을 세우고 있는 중국·러시아는 방어 역량은 약하지만 공격 역량에서 미국과 비슷한 수준을 보이고 있다. 이는 사이버 분쟁·전쟁에 있어서 비대칭 전력으로써 방어 보다는 공격에 무게 중심을 두고 있는 전략의 결과로 판단되며, 또한, 사이버 공격에 대한 대응 수단으로써 수동적 방어 보다는 선제적 공격 전략을 택한 미국을 견제하는 것으로도 해석된다.

셋째, 방어 역량 분야의 패치 보급률 및 보안 관제 수준 제고가 필요하다. 주변국의 사이버 공격에 빈번하게 노출된 우리나라의 방어 역량은 그동안 많은 발전이 있어 왔지만, 패치 보급률과 보안 관제 수준 제고는 풀어야 할 숙제이다.

V. 결 론

사이버공격을 둘러싼 국가 간 신경전이 거세짐에 따라 사이버 역량 강화의 필요성이 제기되고 있는 실정이다. 자신과 상대방의 상황에 대하여 잘 알고 있으면 백번 싸워도 위태로울 것이 없다는 지피지기 백전불태라는 말처럼 국가 사이버 공간을 수호하기 위해서는 주변국들의 사이버 역량을 평가·분석하는 것이 필수라고 할 수 있다. 본 논문에서는 사이버 역량 평가 방법론을 개발하고 동 방법론을 이용하여 주요 5개국(미국·중국·일본·러시아·한국)의 사이버 역량을 평가하였다. 사이버 역량 평가는 공개된 자료를 기반으로 기반·공격·방어 역량 분야의 평가항목에 따라 절대 평가 또는 상대 평가를 수행하였다. 미국, 중국에 이어 3위를 차지한 우리나라는 기반 역량 분야의 예산·인력에 대한 지속적인 투자와 방어 역량 분야의 패치 보급률 및 보안 관제 수준 제고가 필요하다고 분석되었다. 특히 우리나라는 외부로부터 공격을 많이 받는 경향이 있어서 방어 역량은 높게 측정 되었으나, 공격 역량이 부족하다고 평가되었다. 세계 각국이 사이버무기 개발 경쟁에 돌입한 시기에 우리나라도 방어 역량 뿐만 아니라 공격 역량을 강화하기 위한 전략 마련이 시급하다.

참고문헌

〔1〕 보안닷컴, "미 vs 중, 사이버 전쟁 신경전 고조," http://www.boannews.com, 2011.08.
〔2〕 디지털타임스, "사이버안보, 실질적 역량 확대해야," http://www.dt.co.kr, 2011.08.
〔3〕 대한뉴스, "북한의 사이버 역량 미 CIA 능가," http://www.dhns.kr, 2011.06.
〔4〕 Technolytics, "Cyber Commander's eHandbook version 2.0," Technolytics, 2011.
〔5〕 Defense Tech, "China's Cyber Forces," http://defensetech.org/2008/05/08/chinas-cyber-forces, 2008.05.
〔6〕 Defense Tech, "Russia's Cyber Forces," http://defensetech.org/2008/05/27/russias-cyber-forces, 2008.05.
〔7〕 Defense Tech, "Iranian Cyber Warfare Threat Assessment," http://defensetech.org/2008/09/23/iranian-cyber-warfare-threat-assessment, 2008.09.
〔8〕 Richard A. Clarke, "Cyber War: The Next Threat to National Security and What to Do About It," Copyrighted Material, 2010.
〔9〕 전현준, 김국신, 정영태, 최수영, 김진환, "북한의 국력 평가연구," 통일연구원, 2009.
〔10〕 WEF, "The Global Information Technology Report 2010-2011," 2011.
〔11〕 Economist Intelligence Unit, "Digital economy ranking 2010 Beyond e-readiness," IBM, 2010.

〈著者紹介〉

사 진

강 정 민 (JungMin Kang) 정회원
2002년 2월: 광주과학기술원(GIST) 정보통신공학과 석사
2002년 3월~2003년 5월: 삼성 SDS
2011년 2월: 고려대학교 컴퓨터교육학과 박사 수료
2003년 6월~현재: ETRI 부설연구소
〈관심분야〉 보안 OS, 모바일컴퓨팅, 사이버전

사 진

황 현 욱 (HyrnUk Hwang) 정회원
2000년 2월: 조선대학교 정보통신공학과 졸업
2002년 2월: 조선대학교 전자공학과 석사
2004년 8월: 전남대학교 정보보호협동과정 박사
2004년 9월~현재: ETRI 부설연구소
〈관심분야〉 정보보호, 전자공학, 통신공학

사 진

이 종 문 (JongMoon Lee) 정회원
1998년 2월: 강원대학교 수학과 졸업
2000년 8월: 강원대학교 컴퓨터과학과 석사
2000년 8월~2004년 4월: ㈜시그엔
2004년 8월~현재: ETRI 부설연구소
〈관심분야〉 정보보호, 보안관제, 네트워크보안

사 진

윤 영 태 (YoungTae Yun) 정회원
1995년 2월: 충남대학교 컴퓨터과학과 졸업
1999년 2월: 충남대학교 컴퓨터과학과 석사
2006년 8월: 충남대학교 컴퓨터과학과 박사
2000년 1월~현재: ETRI 부설연구소
〈관심분야〉 정보보호, 네트워크

사 진

배 병 철 (ByungChul Bae) 정회원
1994년 2월: 홍익대학교 컴퓨터공학과 졸업
1996년 2월: 홍익대학교 일반대학원 전자계산학과 석사
2007년 3월: 충남대학교 대학원 컴퓨터공학과 박사 수료
1996년 1월~1999년 1월: 국방정보체계연구소 연구원
1999년 1월~2000년 1월: 국방과학연구소 연구원
2000년 2월~현재: ETRI 부설연구소
〈관심분야〉 정보보호, 사이버 보안관제, 네트워크 및 분산시스템 보안

정 순 영 (SoonYoung Jung) 정회원
1990년 2월: 고려대학교 전산과학과 졸업
1992년 2월: 고려대학교 전산과학과 석사
1997년 2월: 고려대학교 전산과학과 박사
1997년~2000년: (주)ECO 연구개발실장
2000년~현재: 고려대학교 컴퓨터교육학과 교수
〈관심분야〉 데이터베이스, 모바일컴퓨팅, 지식기반시스템