Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.6, Dec. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.6.1263

국방 사이버 방호체계 구축 생태계 취약점 분석 및 개선방안

백 재 종,[1†‡] 문 병 무[2]
[1]대한민국 해군, [2]숭실대학교

Cyber Defense Analysis and Improvement of Military ecosystem with Information Security Industry

Jaejong Baek,[1†‡] Byoung-Moo Moon[2]
[1]Republic of Korea Navy, [2]Soongsil University

요 약

상용제품에 종속적인 국방 사이버 방호체계 생태계는 APT(Advanced Persistent Threat) 등 지능화된 최근 사이버 공격양상에 더욱 취약할 수 있다. 일반무기체계는 대부분 특정 방위산업체가 양산한 관급제품으로 원천기술 등에 대한 보호가 가능하지만 사이버 방호체계는 대부분 상용제품으로 군을 공격하지 않고 산업체 공격을 통해 군 공격이 직·간접적으로 가능하다. 본 논문에서는 국방 사이버 방호체계를 구축해나가는 생태계에 있어서 적 공격의 가상 시나리오를 분석해보고, 이에 대한 취약성 및 위협성을 평가 및 검증하여 안전한 국방 사이버 방호체계 생태계 구축을 위한 기술적, 정책적 방안을 제시한다.

ABSTRACT

Since the cyber defense has been dependent on commercial products and protection systems, in aspect of the recent trends, our cyber defence ecosystem can be more vulnerable. In case of general defense weapon companies, they have to be observed by the government such as certain proprietary technologies and products for the protection from the enemy. On the contrary, most cyber weapon companies have not been managed like that. For this reason, cyber attack can reach to the inside of our military through the security hole of commercial products. In this paper, we enhanced a military cyber protection ecosystems out of enemy attacks and analyze the hypothetical scenarios to evaluate and verify the vulnerability, and finally more securable ecosystem of military protection system is presented politically and technically.

Keywords: Cyber warfare, Information security, Information assurance, hacking

I. 연구 배경 및 목적

비대칭 전력으로 평가받고 있는 사이버 공격은 사이버 공간의 국경선이 명확하지 않아 공격 대상을 개인과 기업에서 국가범위로 확장되고 있으며 북한의 지속적인 사이버 위협도 증가 되고 있다[1]. 최초의 산업제어시스템을 공격한 Stuxnet, 특정 목적으로 지속 잠복 공격하는 APT 등의 새로운 공격기법은 상용제품에 종속적인 국방 사이버 방호체계 생태계에 더욱 위협적이다. 군의 일반무기체계는 대부분 특정 방위산업체가 양산한 관급제품으로 원천기술 등에 대한 보호가 가능하다. 그러나 사이버 무기(방호)체계는 대부분

접수일(2014년 9월1일), 수정일(1차: 2014년 10월 29일, 2차: 2014년 11월 24일), 게재확정일(2014년 11월 25일)
† 주저자, jjb27@naver.com
‡ 교신저자, jjb27@naver.com(Corresponding author)

상용제품으로 구축되어 있어 군을 직접 공격하지 않고도 산업체 공격을 통해 군에 피해를 입힐 수 있는 가능성이 있다. 이처럼 군의 새로운 사이버 취약점을 발굴하고 대비하기 위해서는 사이버 공간을 벗어나 물리적 공간까지 고려해야 한다. 또한 현재까지 추진해온 군의 사이버 방호체계 구축 생태계를 되돌아보아 검토되지 않았던 취약점들을 식별하고 분석하여 선제적으로 대비하는 것이 필요하다. 따라서 본 논문은 이와 관련된 적 공격의 가상 시나리오를 분석하고 취약성을 평가하여 안전한 국방 사이버 방호체계 생태계 구축을 위한 기술적, 정책적 방안을 제시한다. 본 논문의 구성은 다음과 같다. 2장에서는 상용제품에 종속적인 국방 사이버 방호체계 생태계를 분석 하고, 물리적/가상 공간이 혼재되어 있는 최근 사이버 공격 양상에 대한 취약점을 식별한다. 3장에서는 국방 사이버 방호체계를 구축 생태계에 있어서 적 공격의 가상 시나리오를 분석한다. 또한 공격 대응시간에 영향을 주는 요소를 식별할 수 있도록 모델링 및 시뮬레이션을 통해 검증한다. 4장에서는 도출된 취약점에 대한 개선 방안을 정책적으로 제시한다. 끝으로 5장에서는 논문 내용을 요약 및 정리 한다.

II. 사이버 방호체계 구축 생태계 분석

2.1 국방 사이버 방호체계 구축 실태

2.1.1 도입 및 구축 패러다임

국방 사이버방호체계는 국방정보화업무훈령상 국방정보시스템 기반체계로 분류되어 있다. 군내 도입방식은 일반 컴퓨터 하드웨어 및 소프트웨어와 동일하다. 도입 주관기관은 전군을 지원하는 공통체계의 경우 사이버사령부, 각 군 고유 정보보호체계는 각 군별로 일괄 도입을 추진하고 있다. 정보보호시스템은 관련법령(전자정부법 제56조, 시행령 69조)에 따라 국가 사이버안전센터(국가보안 기술연구소 위임)에서 1998년 2월부터 시행하는 보안적합성 검증(공통평가기준, CC: Common Criteria 등급)을 통과한 제품(침입차단시스템 등 26종, 국가사이버 안전센터 '13.3월 기준)을 도입 조건으로 하고 있다. 암호모듈도 별도로 검증제도를 두어 암호모듈의 안전성과 구현 적합성을 검증하고 있다. 이러한 CC 인증의 문제점은 심사 중점이 제품 개발 과정에 있기 때문에 제품을 제작하는 회사의 인력자원이나 회사 간 합병, 인수 이력 등에 대한 내용은 심사기준에 반영되는지 불투명 하다는 것이다. 따라서 인증 심사 기준 중 재인증 요청 시 회사 간 인수합병 여부 및 인력 등에 대해 철저한 검증이 될 수 있도록 강화할 필요가 있다. 이러한 맥락에서 물리적 무기체계와 사이버 무기체계의 차이를 보다 명확하게 식별하기 위해 특징을 비교한 내용은 표 1과 같다.

방위사업법 35조에 따라 방위사업체로 지정이 되면, 시설기준과 보안요건에 대한 주기적인 점검을 받아야 된다. 또한 인수합병에 따른 경영지배권의 변화 발생 시 관련서류를 제출하여 장관승인을 득해야 한다. 반면 사이버 무기는 주요 방위산업체 지정에 미포함되어 있기 때문에 업체 인력, 경영지배권의 변화에 대한 인지 및 통제에 취약할 수밖에 없다. 이처럼 무기체계는 대부분 관급제품으로 양산 배치함에 따른 원천기술에 대한 보호가 가능하다. 그러나 사이버무기체계는 대부분 상용제품으로 쉽게 취득 가능하며, 역공학 등을 통하여 취약점을 식별하여 군을 직접 공격하지 않고 산업체 공격을 통해 군에 간접적으로 침투할 수 있는 가능성이 상존한다.

Table 1. Comparison physical vs. cyber warfare system

Item	Physical	Cyber
Manu-facture	Defense contractor (management by Defense business law)	Private companies
Verificati-on M&A	Need to admit by the commerce minister	Unnecessary
Cost, prolifera-tion	High cost and time to spread	Low and easy to spread
Mainten-ance	Periodic inspection in accordance with the laws and regulations	No inspection
Original technology	Protection in accordance with the relevant laws	No protection

2.1.2 유지보수 업체 관리 실태

현재의 군 유지보수 방안은 SLA(Service Level Agreement)방식으로 적정 유지보수 대가를 지불하는데 초점을 두고 있다. 업체의 재무성이나 경력에 따른 판단으로 선정된 업체는 지정된 요건만 만족되면 인력을 변경하여 추진할 수 있다. 따라서 유지보수 계약 기간 중 군 감독자는 업체 간의 하청관계를 면밀히

확인 및 통제가 어려울 수 있다. 또는 업체가 인력을 임의 변경 시, 군 내부망 접근 등 악의적 행위의 가능성을 배제할 수 없다. 따라서 유지보수 업체에 대한 종합적인 관리/협조체계가 느슨해짐에 따른 틈새는 언제나 적으로부터 좋은 공격 시발점이 될 수 있다.

III. 사이버 공격 시나리오 분석

3.1 공격 시나리오 도출

본 장에서는 2장에서 분석된 문제점을 토대로 사이버 공격 시나리오를 도출하고 분석 한다. 향후 사이버 공격 양상은 더 이상 사이버 공간으로만 구성되지 않고 물리적 공격이 혼재되어 노출된 보안 틈을 통해 감행되어 진다. 따라서 예상되는 물리적인 공격 요소를 먼저 식별한 후 사이버 공격 요소와 조합하여 공격 시나리오를 도출 한다. 첫 번째 가상 사이버 공격 시나리오는 군의 신종악성코드 대응시간을 지연시키는 공격과, 두 번째 시나리오는 상용(COTS: Commercial Off-the-self)/관용(GOTS: Government Off-the-shelf) 제품 구성 비율에 따른 대응지연 공격 시나리오를 도출한다.

• 시나리오 A. 신종악성코드 대응 지연 공격

그림 1은 신종악성코드 발생 시 백신업체까지 전달되는 흐름과 공격 가능한 영역을 나타낸다. 공격 지점으로 각 영역을 ①, ②, ③, ④ 지점으로 구분하였다. 각 공격 지점에서는 표 2와 같이 가능한 공격자 및 가능한 사이버 공격 시나리오를 도출 할 수 있다. 이처럼 각 영역에 있어서 공격자에 따른 공격 가능한 시나리오는 다양하게 예상된다.

• 시나리오 B. 상용/관용제품 구성비율에 따른 대응지연 공격

사이버 방호체계를 상용 및 관용제품으로 구성할 때 이에 따른 위험도(risk)를 판단하는 것은 사이버 방호체계를 구축하는데 정책적으로 도움이 된다. 정성적인 평가와 예측은 상대적 기준의 모호성으로 객

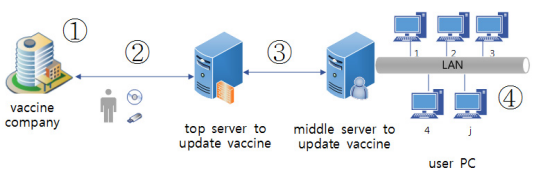

Fig. 1. Vaccine Update Process and attackable points

Table 2. Attack scenarios by attackable position

Position	Attacker	Attackable scenarios
①	• Visitors • Partners's staffs • Acquisition / merger company employees • Employee of outsourcing company	• Bombing, firing, blocking vaccine suppliers or maintenances
②		• Man-in-the-middle attack - faking, interrupting vaccine patch
③ ④	• Service staff • Military insider	• Disguised employment - accessing by lawful means - hiding backdoors

관성을 보장하기에는 부적절 하다. 따라서 두 번째 시나리오는 상용/관용제품 구성비율과 유지보수 능력에 따라 종합적인 위험도를 정량화하여 위험도가 높은 방어체계를 무력화 시키는 공격이다. 먼저 공격대상의 취약도를 판단하기 위해 표 3은 한 단위부대의 사이버 방호체계의 복구 능력 및 취약도를 정량화 하였다. 일반적으로 Risk를 계산하기 위해서는 예방, 탐지, 대응능력 별 다양한 요소 들이 고려되어야 한다. 그러나 본 논문에서는 상용제품에 종속적인 국방 사이버방호체계 구조 특성을 기반으로 대응지연시간에 초점을 둔 공격 시나리오이기 때문에 복구능력이 대응시간에 가장 큰 영향을 미치므로 복구능력을 중심으로 수식을 정의했다. 복구능력을 구성하는 것은 상용/관용 제품의 유지보수 능력과, 기타 유지보수 능력의 평균값으로 정의하였다.

Table 3. Defense capability and Vulnerability

	Defense system	COTS	GOTS	Maint-enance	Recovery	Vuln-erability
V_1	Network	×	○	○	0.66	0.34
V_2	Server	○	○	○	1	0
V_3	Personal computer	○	×	×	0.33	0.67
V_4	Privacy	○	×	○	0.66	0.34

• Recovery = Σ(COTS' IF + GOTS' IF + Maintenance's IF)/n
• IF = if recovery capability exist 1, else 0
• Vulnerability(V) = 1 - Recovery
• Recovery 0.58 / Vulnerability 0.42
• n = Number of factors

Table 4. Attack profile and assessment

	Attack types	Position	Weight (delay hour)
T_1	Key employees abducted	③,④	30
T_2	Supplier facilities attacks (destruction)	④	20
T_3	Transfer means attack	③	10
T_4	Switched communication medium	③	10
T_5	Disguised employment attacks	①,②	30

취약도는 복구능력에 반비례하기 때문에 "1-복구능력"을 취약도로 나타내었다. 각 유지보수 능력은 Kang[2]과 같이 전문가에 의한 설문/평가에 따라 평가가 가능하나 본 논문에서는 연구의 범위를 벗어난다고 판단하여 복구능력 유무에 따라 0과 1로 가정 하였다. 표 3의 결과, 공격자는 우선적으로 취약도가 가장 높은 지점 V_3 를 공격 대상으로 선택할 것이다. 그 다음 순서는 어떤 방법으로 공격할 것인가를 판단하는 것이다. 이를 위해 표 4와 같은 공격 프로파일을 적용하여 보다 완성도 높은 공격시나리오를 작성할 수 있다. 프로파일에 정의되는 공격내용은 군의 대응시간을 지연시키기 위한 물리적인 공격만을 기술하였다. 공격위치는 그림 1과 같은 군부대/업체 간의 구성을 기반으로 할 때 각 지점이다. 각 공격에 대한 가중치(weight)는 피해를 입었을 때 예상되는 지연시간(hour)이며 공격 피해 정도에 따라 다르므로 본 논문에서는 임의 값으로 가정하였다.

Table 5. Total risk value

	Vulner-ability	Threat(n=5)	Total Risk
1	V1	$(\sum_{i=1}^{n} T_i)/n$	6.8
2	V2	$(\sum_{i=1}^{n} T_i)/n$	0
3	V3	$(\sum_{i=1}^{n} T_i)/n$	13.4
4	V4	$(\sum_{i=1}^{n} T_i)/n$	6.8
Total			27

추후 전문가 그룹의 설문조사 또는 실제 경험한 데이터의 통계 등을 적용하여 정확도를 높일 수 있다. 이처럼 공격과 방어에 대한 프로파일을 정의하여 다양한 사이버 공격 시나리오를 도출 할 수 있다. 각 경우의 수에 대한 공격/방어력을 표현하여 취약한 우선순위대로 개선방안을 강구하는데 사용될 수 있다. 이는 각 구성요인의 비율과 대응지연시간과의 관계를 연관시켜 대응시간 최소화를 위한 체계 구성방안을 사전에 정책적으로 선정하는데 사용될 수 있다.

종합 위험도 = 취약도(V) x 위협도(A) x 가치도 (1)

식 1은 기업의 노동 가치를 시간과 함께 계산한 값을 취약도에 따른 손실도, 즉 위험도로 표현한다[3]. 이 식을 이용하여 시나리오 B에서 가정한 공격에 대한 종합 위협도는 다음 표 5와 같으며 표 3의 취약도를 기준으로 표 4의 위협도를 연관 적용, 평균값을 산출하였다. 가치도는 자산 평가에 따라 변동적이므로 1로 고정하였다. 결과적으로 취약도 V_3, 즉 PC 방어체계가 가장 위협도가 높은 것으로 평가된다. 그 이유로는 복구능력이 취약한 상용제품 비율이 상대적으로 높다는 것을 알 수 있다.

3.2 상용/관용 제품 구성비율의 영향성 검증

3.1에서 도출한 사이버 공격 시나리오에서 상용/관용제품의 구성 비율이 웜의 감염(확산)/방역 비율에 미치는 영향을 분석하기 위해 시뮬레이션을 통하여 검증한다. 이를 위해 JDK 기반의 SSFNet (Scalable Simulation Framework) 2.0 네트워크 시뮬레이터(API, engine)를 활용한다.

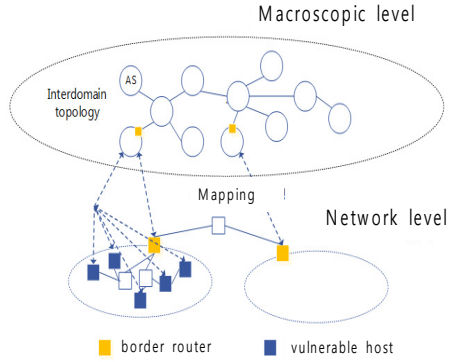

Fig. 2 Simulation model

```
worm_model [
   Epidemic [
   s_0      359999,     i_0      1, beta   1.235e-9]...]
Net [ id 0
  AS_num 557
     router [ id 0
     interface [ id 0 _extends .dictionary.100Mb ]]

  host [ id 1
  interface [ id 0 _extends.100Mb ]]
  link [ attach 0(1) attach 1(0) delay 0.003 ]...]

    Net [ id 1
      AS_num 1351
      router [ id 0
      interface [ id 0 _extends .dictionary.100Mb ]]...
```

Fig. 3. DML scripts for simulations

SSFNet은 호스트와 네트워크 토플러지 및 프로토콜(IP 레이어 이상)을 DML(Domain Modeling Language)로 비교적 쉽고 상세하게 표현할 수 있는 장점이 있다[4]. 본 실험에서는 SSFNet이 기본 제공하고 있는 Worm Attack 샘플소스코드 중 대응시간에 영향을 주는 파라미터를 수정하여 수행한다. 시뮬레이션 모델은 그림 2 Liljenstam[5]의 감염 모델을 활용한다. 그림 3은 웜 확산 모델을 구성하는 네트워크 및 호스트(단말기) 등을 정의하는 스크립트이며 파라미터 의미와 초기 값은 표 6과 같다. 다음은 시뮬레이션을 위한 가정 사항이다.

1) 각 네트워크에 연결된 호스트는 웜에 취약하다.
2) 관용제품 구성비율 : 70%, 상용제품 : 30%
3) 관용제품 구성비율 : 30%, 상용제품 : 70%
4) 감염률, 방역률, 웜 트랙픽 모델 [6] : Code Red v2

시뮬레이션 결과, 그림 4는 네트워크 구성이 상용제품으로만 구성된 경우 웜 확산 및 방역도를 나타내고 있다. 웜 공격 10시간 후 최대 확산(약 28만대) 되고 이후 방역조치가 이루어져 감소되고 있음을 나타내고 있다. 그림 5는 상용제품으로만 구성된 경우, 관용/상용 비율을 각각 7:3, 3:7 비율로 구성한 세 가지 경우의 시뮬레이션 결과를 나타낸다. 그림 4, 5의 의미는 웜 공격 10시간 이후 상용제품 구성 비율이 높은 네트워크는 약 20만대, 관용제품 구성 비율이 높은 네트워크는 약 13만대까지 확산되고 이후 방역조치로 감소됨 을 보이고 있다. 결과적으로 관용제품의 구성 비율이 높을수록 웜 공격 피해율과 복구율에 유리하다는 것을 알 수 있고, 이를 근거로 적절한 대응 허용 시간을 파악하여 정책적으로 관용/상용제품의 구성 비율에 적용할 수 있다.

Table 6. Simulation parameter initial value

Parameter	Description(intial value)
N	number of host = 360,000
s_0	# of host = N-1
i_0	# of infected = 1
beta	infection ration=1.6/3600)/N · Core Red worm(reference [6])
AS_num	# of COTS network = 557 # of GOTS network = 1351 · defending on ration of COTS/GOTS
bite rate	100 Mbps, 1 Gbps
delay	0.003 sec

3.3 공격 대응시간 산출 모델

시뮬레이션은 실세계를 정확하게 모델링 했는지에 따라 결과가 달라지며 복잡하고 다양한 사이버 공격 상황을 분석하는 데에는 한계가 있다. 이를 보완하기 위하여 특정 사이버 공격에 대한 군의 행동, 즉 방어체계를 관찰하고 이를 분석하는 보완 사항이 필요하다. 3.2절의 시뮬레이션 결과 10시간 이후 방역조치가 이루어진 것을 알 수 있다. 이 시간을 공격대응시간 R(Response time)로 정의하여 각 요소간 관계를 파

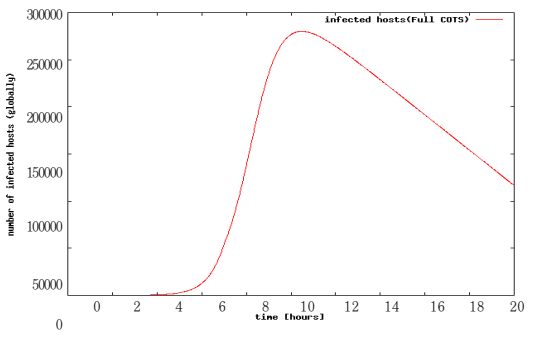

Fig. 4. Infection ratio with Full COTS

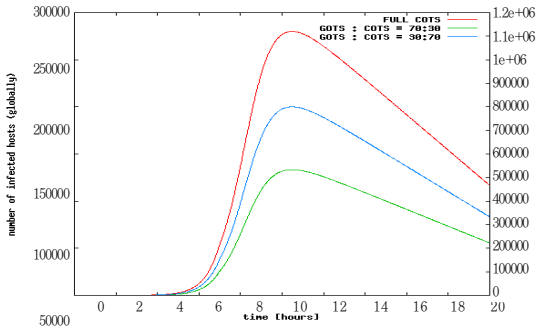

Fig. 5. Infection ratio with COTS and GOTS

Table 7. Factors for parameters

	Factors
T_{pass}	Transmission methods (human, vehicle), media (CD, USB), line(VPN)
$T_{analysis}$	Malware obfuscation algorithms, packer, anti-reversing applied degree
T_{patch}	Infection methods, infection, degree of infection
$T_{update\ i}$	Military personnel / maintenance personnel response time, power-based systems, such as protection type
$T_{update\ j}$	

악하기 위한 수식을 도출 및 정의한다. 시나리오 A에 대해 최종 사용자 PC에 업체로부터 백신 패치를 업데이트 하는데 소요되는 시간 R은 다음과 식 2와 같다.

$$R = (2T_{pass} + T_{analysis} + T_{patch}) + \max(T_{update\ i}) + \max(T_{update\ j}) \quad (2)$$

각 구간에서 소요되는 시간들은 T_{pass}, $T_{analysis}$, T_{patch}, $T_{update\ i}$, $T_{update\ j}$ 로 구성하였으며 $T_{update\ i}$, $T_{update\ j}$ 는 동시에 업데이트 되므로 최대 소요시간 값으로 표현하였다. 각 시간변수에 영향을 주는 요소는 다음 표 8과 같다. 이러한 영향 요소는 보호대상 정보자산을 모델링 할 때 분석 변수로 사용될 수 있다. 예를 들어 10시간이 소요되는 대응시간에 가장 큰 지연을 초래한 구간이 어디인지, 단축할 수 있는 방안은 무엇인지 분석을 통해 감염의 확산을 최소화 할 수 있다.

Table 8. Parameters for equation (2)

	Description(unit, h: hour)
T_{pass}	Time to pass vaccine or patches(h)
$T_{analysis}$	Time to analyze malware(h)
T_{patch}	Time to make vaccine(h)
$T_{update\ i}$	Time to update from top server to middle server(h)
$T_{update\ j}$	Time to update from middle server to user (h)
i	# of middle server(EA)
j	# of user PC(EA)

IV. 국방 사이버방호체계 생태계 개선 방안

4.1 사이버 정보보호체계 구축시 기술 이전 추진

사이버 무기체계는 외부 민간업체의 기술에만 의존하였을 경우 복잡한 변수로 인해 적시에 대응하기에는 제한사항이 있다. 정보보호 제품 도입 시 단순 구매가 아닌 무기체계와 같이 절충교역을 통해 기술이전 방식으로 도입된다면 군내 자체 기술 축적으로 인한 인력 유지로, 민간 업체 의존도를 낮출 수 있는 방안이 될 것이다. 이를 위한 조직, 제도 및 법령(국방정보화업무 훈령 등)의 정비가 병행되어져야 한다.

4.2 역공학 방지 코딩기술 도입 및 백신체계 개선

적은 군 내부망에 대한 끊임없는 공격 시도를 구상하고 이행하고 있을 것이다. 예를 들면 군에서 사용되는 내부 응용체계들의 취약점을 이용하여 침투할 수 있다. 또한 보안코딩이 미흡한 군 자체개발 응용체계에 대한 공격 감행도 가능할 수 있다. 이에 대한 대응책으로 역공학 방지를 위한 보안코딩 기술을 확대 적용하여 언어별, 플랫폼 OS 별 원천적인 공격을 차단시키도록 해야 한다. 인터넷과 물리적으로 분리된 군 내부망은 민간 인터넷에서는 이미 면역되어 있는 악성코드에 쉽게 무너질 수도 있다. 따라서 군 내부망에 접속 활용되는 PC의 실행중인 프로세스 레벨로 정형화된 DB를 구성하여, 비정상 프로세스를 탐지하도록 백신체계를 개선하는 것도 신종악성코드를 탐지해내는 개선된 방법이 될 수 있다.

4.3 투명한 유지보수 업체 관리 강화

신종 악성코드 등에 따른 해킹사고 발생 시 군은 신속하게 유지보수업체에 악성코드 샘플 전달해야한다. 또한 유지보수 업체도 군에 방역 백신이나 패치 업데이트를 긴급히 수행해야 한다. 이러한 군과 유지보수 업체간 이루어지는 유지보수 과정은 적에게 노출되기 쉬운 취약점이다. 즉, 적에게 전달과정을 지연시키는 공격을 받았을 때 군의 피해는 급속도록 확산되는 구조로 구축되어 있다. 따라서 유지보수 업체에 대한 경계 방호시설 확충, 샘플과 백신패치 전달과정에서의 무결성을 보장할 수 있는 체계를 구축해야 한다. 또한 유지보수 업체의 하청관계를 면밀히 감독하여 인원, 장비, 기술 유효성 등이 철저히 통제되어야 한다.

4.4 악성코드 대응능력 강화

먼저 군과 백신 제작업체 간 백신패치 전달 절차가 물리적공간과 사이버공간상 균형적으로 강화되어야 한다. 현재 인편으로 전달시 전달 매체(탈취, 위

변조를 대비한 파일 암호화, packing 등), 운송인원, 교통수단, 경로 등 사전계획이 수립되어 있는지 확인해야 한다. 그리고 다각적인 긴급 상황에 대응할 수 있도록 관련 인원, 도구, 시설 등의 훈련이 필요하다. 또한, 백신개발업체의 재해복구시스템 구축으로 적의 물리적인 공격에 의해 대응/복구 자원이 소산할 것을 대비하여야 한다. 핵심 백신업체에 대한 예비 개발센터를 군 영내 등 경계방호 설정 구역 내 설립하는 것도 방안이다. 각 종 상황에 따른 핵심 백신 개발인원에 대한 경호 및 후송 대책 강구하여 훈련/숙달이 필요한 부분이다.

V. 결 론

최근 북한은 정치적 상황을 고려하여 사이버 공격 또는 테러를 비대칭 전력으로 적절히 활용하고 있다. 이는 전략적으로 미사일을 활용하여 중요시설을 타격한 것보다 사이버 공격을 활용하여 우리에게 심리적/물리적 타격을 줄 수 있음을 시사한다. 본 논문에서는 이처럼 사이버 무기를 무기체계로 인식함에도 불구하고 물리적인 무기체계와는 다르게 소홀이 관리되고 있음을 지적하였다. 또한 군의 정보보호체계를 구축하는 생태계에 취약점이 있음을 확인하였고 이에 대한 대안을 기술적 및 정책적인 측면에서 제시하였다. 현재의 국방 정보자원 환경은 상용제품에 편중되어 있고, ICT 외부 인력에 의한 위탁관리 환경은 사이버 공격에 취약한 환경으로 판단되었다. 따라서 상용제품/관용제품 구성비를 적절히 조정하고, 외부 업체를 방위산업체와 유사하게 관리/통제하여 안정적인 국방 정보자원 환경에 부합하는 사이버 방호체계 구축 생태계를 제시하였다. 또한 이를 검증하기 위해 공격대응시간에 영향을 주는 복구능력 등의 요소를 식별하고 모델을 가정하여 각 요소별로 대응시간에 미치는 영향을 정량화 하였다.

References

[1] KISA, White paper on National Information Security, JinhanM&B, pp. 30-31, Apr. 2014.

[2] JungMin Kang et al, "A Study on National Cyber Capability Assessment Methodology," KIISC, 22(5), pp. 1039-1055, Oct. 2012.

[3] Winterfeld et al, The basics of cyber warfare : Understanding the fundamentals of Cyber warfare in theory and practice, Syngress, pp 24-25, Oct. 2013.

[4] http://ssfnet.org/homePage.html

[5] Michael Liljenstam et al, "A Mixed Abstraction Level Simulation Model of Large-Scale Internet Worm Infestations," IEEE/ACM MASCOTS, pp. 109-116, Oct. 2002.

[6] Adrian Shehu et al, "A Cyber Attack Scenario Using SSFNet," the 14th International Conference on Network-Based Information Systems, pp. 690-693, Sept. 2011.

〈저 자 소 개〉

백 재 종 (Jaejong Baek) 종신회원
1996년 2월: 한밭대학교 전자계산학과 학사
2001년 2월: 연세대학교 컴퓨터과학과 석사
2011년 8월: 연세대학교 컴퓨터과학과 박사
〈관심분야〉 사이버전쟁, 역공학, 이동통신 보안

문 병 무 (Byoung-moo Moon) 학생회원
1991년 2월: 경남대학교 전자계산학과 학사
1997년 2월: 부산대학교 산업대학원 전산학전공 석사
2013년 3월~현재: 숭실대학교 IT정책경영학과 박사과정 재학
〈관심분야〉 정보보호, 데이터모델링, 정보시스템 감리