공격 원점지 타격을 위한 사이버 킬체인 전략

유재원* · 박대우*

*호서대학교 벤처대학원

Cyber kill chain strategy for hitting attacker origin

Jae-won Yoo* · Dea-woo Park**

*Hoseo Graduate School of Venture

E-mail : peace.yoo@gmail.com

요 약

현대 ICT 기술의 발달은, 국가와 사회에 인프라를 이용하여 사이버 세계를 구성하고 있다. 사이버 세계에서는 국경이 없다. 세계 각국들은 자국의 이익을 목적으로, 사이버 공격을 수행하고 있다. 사이버 공격을 방어하기 위해서는 사이버 킬체인 전략이 필요하다. 사이버 공격을 방어하거나, 공격책임을 판단하기 위해서는, 공격 원점지의 파악이 중요하다. 공격 원점지에 대한 타격을 하기 위해서는, 전략적인 사이버 킬체인이 필요하다. 본 논문에서는 공격 원점지를 분석하는 연구를 한다. 그리고 공격 원점지 타격을 위한 사이버 킬체인을 분석한다. 공격 원점지 타격을 위한 효율적이고 맞춤형 사이버 킬체인 전략을 연구한다. 사이버 킬체인 전략은 비대칭 전력으로, 핵과 미사일의 위력을 대치할 수 있는 실용적인 전략이 될 것이다.

ABSTRACT

The development of modern ICT technology constitutes cyber world by using infrastructure in country and society. There is no border in cyber world. Countries around the world are carrying out cyber attacks for their own benefit. A cyber killer strategy is needed to defend cyber attacks. In order to defend the cyber attack or to determine the responsibility of attack, it is important to grasp the attacker origin point. Strategic cyber kill chains are needed to strike against the attacker origin. In this paper, we study the analysis of attacker origin. And analyze the cyber kill chain for attacker origin point strike. Study the efficient and customized cyber kill chain strategy for attacking the origin point. The cyber kill chain strategy will be a practical strategy to replace the power of nuclear and missiles with asymmetric power.

키워드

사이버 공격(cyber attack), 사이버 킬체인(cyber kill chain), 사이버보안(cybersecurity), 공격 원점(attacker origin)

Ⅰ. 서 론

2017년 9월 13일 북한은 국제사회의 경고에도 불구 6차 핵실험을 실시하였다. 이후에도 미사일 발사시험을 하여 국제사회의 불안을 유발시키고 있다.

북한은 00년대 이후부터 한미 동맹 전력 대비 재래식전력 열세를 극복하고 위해 노력을 하여왔다. 비대칭 전력 일환으로 핵WMD 및 사이버 전력을 지속 증강하고 있다.

핵 WMD 전력에 대응하기 위하여 한국형 3축 체계를 구축하여 대응하고 있다. 핵 WMD을 사용하기 전에 식별해서 선제적 타격을 의미하는 Kill Chain, 핵 WMD 전력이 투사시 피해최소화

를 위한 한국형 미사일방어체계(KAMD), 핵 WMD 피해 발생이후 공격지휘세력에 대한 대량응징보복작전(KMPR)으로 개념이 마련되고 실현이 되고 있는 실정이다.

본 논문에서는 사이버 공격에 대비하기 위한 식별하고 사전 공격을 무력화시키는 사이버 Kill Chain구축 전략에 대해 알아보고자 한다.

II. Kill chain관련 연구 동향

2.1 Kill Chain 개념

킬체인은 미군이 1991년 걸프전 이후 중동지역에서 전쟁을 수행하면서 적 미사일이나 지도부 및 테러요원과 같은 기민하게 움직이는 시한성 표적에 대한 효과적인 타격방법을 모색하는 과정에서 등장한 개념 미군의 역동적인 표적처리절차(Dynamic Targeting Step)'에 대한 별칭이다[1]. 즉, 사전 식별되고 움직이지 않는 대상이 아니라 갑자기 나타나는 위협에 대해 긴급표적처리절차이다.

미군의 긴급표적처리절차는 그림 1과 같이 나타내고 있다[2].

그림 1. 미군의 Kill chain 개념

그림 1에서 나와 있듯이 6단계로 절차를 볼 수 있다. 1단계는 위협에 대한 전장을 식별하는 과정(Find)이며 2단계는 위협요소가 식별되면 해당전장에 대해 집중적인 관찰을 통해 피아식별 과정(Fix)과정, 3단계는 지속적인 감시를 통해 최신화된 타겟 정보를 유지하고(Track), 4단계는 해당 타겟에 대해 적절한 전력을 결정하는 과정(Target), 5단계는 결정된 전력으로 타겟을 제거(Engage)하며, 6단계로 피해평가(Assess)를 실시하게 된다.

2.2 한국형 Kill Chain 개념

한국형 Kill Chain은 북한 미사일에 대비하기 위해 미공군 Kill Chain 운용 개념과 유사하며 4단계로 간략화[3]되어 있다.

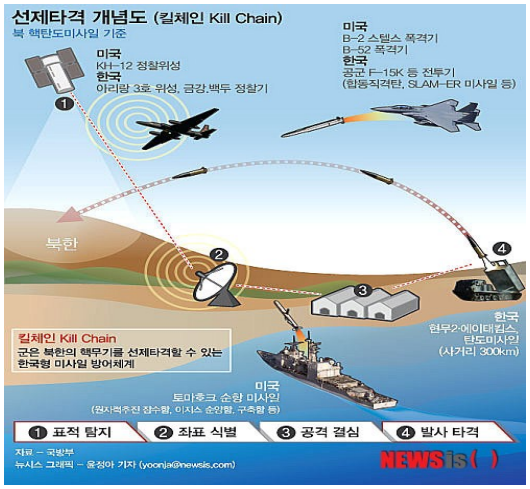

그림 2. 한국군 Kill chain 개념
* 출처: 윤정아, "선제타격 개념도 (킬체인 Kill Chain)," 뉴시스 , 2013. 2. 13.

한국형 킬체인이란 북한이 핵.미사일로 한국을 타격할 가능성이 커질 경우, 한국은 이런 징후를 조기에 포착하여 선제공격을 실시하여 제거하는 개념이다.

2.3. Kill Chain 구현요구 사항

Kill Chain 전략은 구현되기 위해서는 감시체계, 결심체계인 C4I체계, 그리고 타격/요격체계가 필요하다. 추가적으로 각 체계를 유기적으로 연동되는 체계, 즉 System of System이 필요하다고 알려져 있다.

전략은 목표와 수단, 운영개념이 구성되며 Kill Chain은 공세적 방위전략으로 침략임박시 행해지는 선제타격, 혹은 미래위협을 사전에 제거하는 예방전쟁이 대표적인 예이다.

억제전략은 능력(Capability), 의사소통(Communication), 신뢰성(Credibility) 등 3C를 만족시켜야 성공이 가능하다.[3]

2.4. 사이버 Kill Chain 개념 등장

사이버 Kill Chain의 개념을 사용한 것은 록히드마틴사[4,6]에서 최초 도입한 이후 베다시스사[5,6] 등에서 개념을 발전시키고 있다.

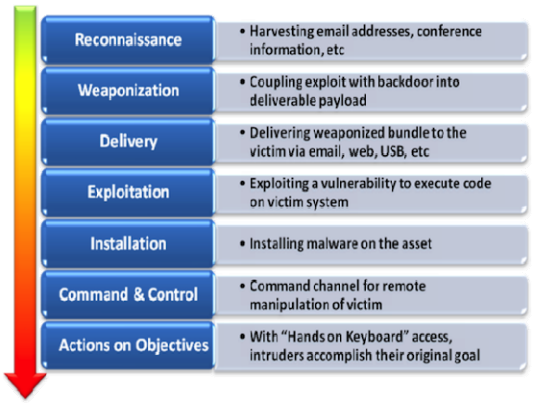

그림 3. Lockheed Martin사 Kill Chain 모델

대표적인 록히드마틴사 사이버 Kill Chain 모델을 살펴보면 그림 3과 같다.

록히드마틴사는 그림 3과 같이 APT 공격형태를 기반으로 Kill Chain 모델을 제시하였다. 정보를 통합하는 정찰(Re- connaisance)단계부터 목표물 조종(Ac tions on Objectives)까지 7단계를 거치게 되어 있다. 록히드마틴산의 Kill Chain 모델은 단계별 공격 단계를 차단에 중점을 두고 있다.

그림 4. Verdasys사 Kill Chain 모델

또한, Verdasys사의 Kill Chain 모델은 [그림 4]과 같다. 방어(Protect), 탐지(Detect), 조사(Investigate), 억제(Contain)의 4단계 대응 절차에 초점이 맞추어져 있다.

2.5. 사이버 Kill Chain의 한계[7]

록히드마틴社 및 베다시스社의 Kill Chain모델을 살펴보면 이동단계(Delivery) 이후 탐지시 이미 적이 네트워크 내부로 침입이 진행된 상태로 대부분의 방어체계는 통과하여 방어자에게 수세적 대응만 할 수 있도록 강요한다.

또한, 원점 타격을 위한 대응방법은 제시하지 못하고 있다. 따라서 공세적 대응을 위한 사이버 Kill Chain 전략이 필요한 실정이다.

III. 사이버 Kill chain 구축 방안

3.1 기존 Kill Chain 모델의 한계 및 의미

기존 록히드마틴社와 베다시스社에서 제안한 Kill Chain은 현실세계의 Kill Chain과 개념부터 차이를 보인다.

현실세계 Kill Chain은 선제적 억제개념이 반영되어 있어 공격자가 공격시도 자체를 못 하게 하는 전략이라며, 제시된 사이버 Kill Chain은 공격자 입장에서 침투단계를 모델화시켰으며 침투단계를 단절시켜서 Kill Chain을 무력화시키는데 중점을 두고 있다.

반면, 기존 사이버 Kill Chain 모델연구는 우리가 제시하는 구축 모델에서 필요한 기술요소들을 무엇인지 제시해주고 있다.

3.2 제안하는 사이버 킬체인 구현 요소

사이버 Kill Chain 체계도 현실세계의 Kill Chain과 동일하게 감시정찰-결심-타격체계와 연동체계가 필요로 한다.

3.3 사이버 킬체인 감시정찰 체계 제안

감시 체계로는 침입탐지체계(IDS), 침입방지체계(IPS), 통합보안관제체계(ESM) 등 우리 네트워크에 대한 정보제품만이 아니라 봇(Bot), Off-line 정보 등을 통해 공격자의 네트워크 혹은 체계를 감시할 수 있는 수단이 있어야 한다.

3.4 사이버 킬체인 결심체계 제안

결심 체계로는 각종 로그파일, 침입시도 패턴 등을 감시체계를 통해 입수된 정보를 가지고 선제적 타격여부를 판단할 수 있는 체계로 구축되어야 한다. 사이버상의 공격은 인공지능 결심체계로 구축시 공격자의 행동에 대해 Kill Chain 가동 이후 과학적 공격근거를 제시할 수 있기 때문에 타격 이후 국제 사회지지를 이끌어 낼 수 있다.

3.5 사이버 킬체인 타격체계 제안

타격 수단은 온라인과 오프라인으로 구분되며 오프라인 타격은 실환경의 물리력과 결합되어야 한다.

3.6 사이버 킬체인 연동체계 제안

감시-결심-타격 체계가 별개가 아닌 유기적으로 작동하기 위해서는 체계가 연동이 가장 중요하다고 볼 수 있다.

유사시 사이버 킬체인 작동을 위해서는 TCP/IP 방식 등 기존 프로토콜이 아닌 중앙통제적인 프로토콜이 필요할 것이다. 즉, 기존 공개망을 독립된 전용통제망으로 전환시켜야 한다.

별도 프로토콜은 피아를 식별하는 용도와 독립 전용통제망을 위해 사용되며 공격의도를 가진 패킷을 역추적(Fingerprint/Backtrack) 기능도 있어야 한다.

Ⅳ. 결 론

사이버 킬체인은 공격 의도를 가진 대상에 대해 선제타격을 통해 우리의 망을 안전하게 지키는 데 목적이 있다.

사이버 킬체인을 구현하기 위한 기술들은 지속해서 개발 중이라 볼 수 있다. 또한, 각 기술을 활용간 발생할 수 있는 법적 문제도 해결해야 될 부분이라고 생각된다.

참고문헌

[1] Lo, Edward H.S. and T. Andrew Au. "Improving the Kill Chain for Prosecution of TimeSensitive Targets." edited by Alisson V. Brito. in Dynamic Modeling. (2010), p. 95.

[2] 양욱, "북한의 비대칭 위협을 제거한다: Kill-Chain," http://navercast.naver.com/contents.nhn?rid=107&contents_id=31409 (2013. 11. 15).

[3] 김열수, "킬체인(Kill-Chain)과 한국형 미사일 방어체제(KAMD): 실현가능성을 중심으로" 新亞細亞 20권 4호 (2013년, 겨울) p.112~p.136

[4] Lockheed-Martin Corporation-Hutchins, Cloppert, and Amin-Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains-2011.

[5]http://www2.verdasys.com/verdasys-cyber-threat‐whitepaper-PR.

[6] 김광제 외, 사이버킬체인에 기반한 사이버 방어체계 발전방안, AJMAHS Vol. 7, No.1. 2017. 1, p.277 ~ p.285.

[7] 김영환 외, 공세적 통합사이버작전을 위한 사이버사이버 킬체인 전략, 보안공학연구논문지 Vol.13, No.5. 2016.10, p.325 ~ p.340.

[8] 유재원, 박대우, "해상에서 실시간 TCP 링크관절 보안통신 연구, 정보통신학회 춘계학술대회, Vol.18, N0.1. p.250~p253.