Cyber Attack Timing

Ferhat Çalışkan, and Yavuz İduğ

***Abstract*—Cyber attacks range in magnitude from large scale attacks to more targeted small attacks. Ill-timed and ill-planned sequence of large scale cyber attacks may weaken the power of the ones next to it. Small scale targeted cyber attacks will mostly have one shot opportunity because of the countermeasures taken by the defender soon after the attack. In this case acceleration trend of the progress of targeted development project will be the determinant factor to decide when to launch cyber attack. This work examines the timing factors in large scale cyber attacks and targeted small scale cyber attacks**

***Index Terms*—Cyber Attack Planning, Timing, Cyber Defense.**

I. INTRODUCTION

CYBER attacks range in magnitude from large scale attacks to more targeted small attacks. The first type of attacks targets whole infrastructure of a country such as the case of an Eastern Europe country in 2007. This cyber attacks resulted in paralyzing the ability of the state to govern [1]. Not only the government agencies but also the national media was affected severely [2]. The second types of attacks are more targeted and have a goal of disrupting progress of a project. This may be a high-tech military technology development project or other balance tipping capabilities such as uranium enrichment. Stuxnet is the most known example of these targeted cyber attacks. Although no government has taken credit for this attack, officials acknowledged the effect of Stuxnet on nuclear site in Natanz [3]. In terms of timing of the attacks, large scale attacks and targeted small attacks provides the cyber attack planners with different and crucial considerations.

II. DETERMINANT TIME FACTORS IN CYBER ATTACKS

A. Purpose of the Study

Cyber warfare studies mostly deals with the defense side of the cyber space. But a better understanding of the cyber attack planning factors will also contribute to cyber defense with the help of increased deterrence by means of enhanced offensive capability. This deterrence can only be reached by detecting security gaps in the networks or systems of the opponent. Gathered intelligence about the gaps will constitute the cyber build-up against a given opponent. This build-up should be kept until the appropriate time comes to launch attack. In this paper time factor in cyber attacks will be examined by differentiating between large scale cyber attacks and small scale targeted cyber attacks.

B. Large Scale Cyber Attacks

Compared with the attack, defense in cyber warfare is more difficult, expensive and needs more effort. The more network operations becomes complex the more they become vulnerable to cyber attacks. This trend always works to the advantage of the cyber attacker rather than the defender [4]. Therefore attacker should gather information about the security gaps in its opponents' networks and critical infrastructures. Then this gathered information should be kept in a vulnerability log of that opponent. This vulnerability log is the cyber version of conventional military build-up. The real advantage lies in the vulnerabilities that are not known by the attacker but not detected by the defender. In Art of War, Sun Tzu puts emphasis on this issue and states that: "We should hide the point where we want to attack the opponent. In this case the opponent will have to consider lots of probabilities at the same time. This will prevent it from massing its power to a point [5]."

Importance of determining time of attack comes to fore at this point. Because ill-timed and ill-planned sequence of cyber attacks will deprive the attacker of the benefits the cyber build-up offers. But only by means of properly determining time and sequence of attacks, this benefit can be transformed to a successful cyber attack.

Between 27 April and 18 May 2007, a series of cyber attacks hit the Eastern Europe country's ministries, banks and other institutions. First wave of attacks started on 27 April and hit the web sites related with the government, on 4 May more organized second wave included botnets and roughly one million computers were used. Third wave of attacks was the most powerful one with a size roughly 2,5 times the bandwidth capacity of country. But because of the countermeasures taken by the officials, when the third wave started on 9 May it did not bear the desired end. It caused a huge damage but this was short of shutting down the entire internet in country [6]. First and second wave of attacks became a warning for the officials in defending country and they raced with time to take countermeasures. Time interval between waves of attacks was enough wide for the defending country to detect security gaps and find solutions.

The response time and countermeasure capability of the defender is the key planning factors for the cyber attack planners. Figure 1 explains the side effects of sequential

Ferhat Çalışkan, War Colleges Command, Army War College, Dept. of Combat Tactics, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Turkey, e-mail: fcaliskan10@gmail.com

Yavuz İduğ, War Colleges Command, Army War College, Dept. of Combat Tactics, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Turkey, e-mail: yavuzidug@gmail.com.

cyber attacks. The key point here is the time interval between waves and the response time of the defender. Response time is a factor of speed of bureaucracy in a given country. If the cyber attack planners do not integrate the time planning vis-à-vis countermeasure response time, each waves of attacks will weaken the power of the subsequent cyber attacks. This will also harm the cyber buildup of the attacker, which will end up with weakened cyber deterrence.

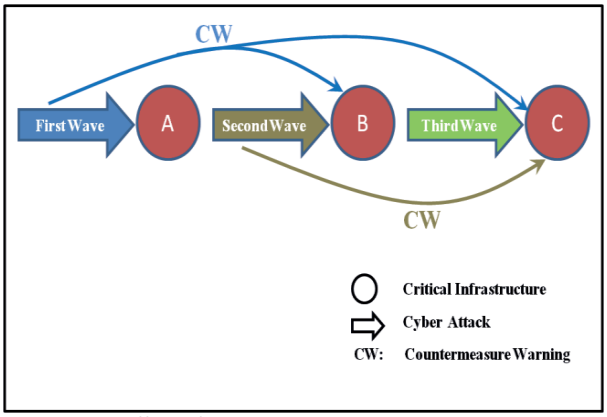
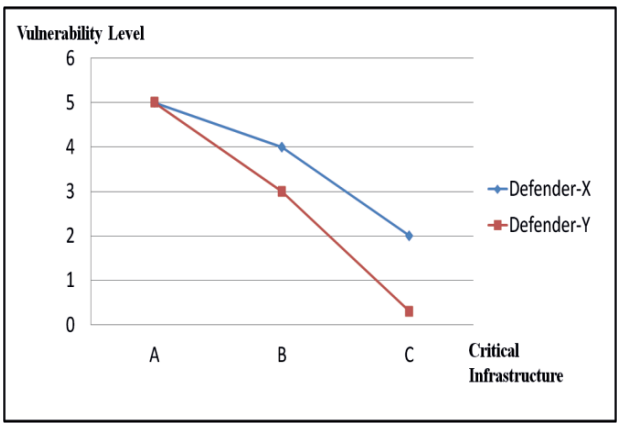


Figure 1. Side Effects of Sequential Cyber Attacks

Vulnerability level of the defender to cyber attacks will depend on the capabilities of the cyber experts working for the defending country. As illustrated in Graph 1, vulnerability level of the critical infrastructures A, B and C, will decrease to the extent of the capabilities of the cyber experts working for X or Y. Cyber expert working for Y are more adaptive than cyber expert working for X to improvising countermeasures. Therefore each wave of attacks to the critical infrastructures A, B and C results in different size of damage in Y and X.



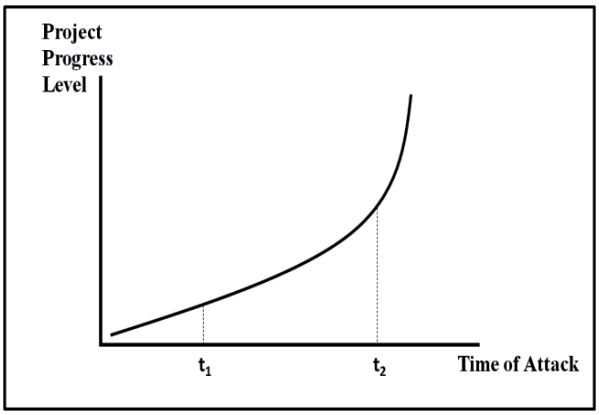
Graph 1. Countermeasure Capability

C. Small Scale Cyber Attacks

Stuxnet attack targeted the frequency-converters that control the speed of centrifuge motors. After Stuxnet reached the centrifuges in Natanz, it stayed inert and one month later it started to change spin frequency from 1410 Hz to 2 Hz. This sudden change caused the physical damage to the centrifuges. This cyber attack certainly caused a drop in the numbers of the machines in the facility. But the timing of the attack was not quite good to get the most of the security gap detected by the attackers. Defending country took necessary measures and closed the security gap, which made the subsequent attacks much more difficult to infiltrate. If the attack was made when the engineers reached the weapons grade level the time provided by the delay in the uranium enrichment would be more valuable [7].

Targeted small scale cyber attacks differ from large scale attack in the conditions that are advantageous for the defender. Since a given infrastructure or a development project will probably have less security gap than whole country network, the attackers will have one shot opportunity to reach the desired end. In short we cannot mention about subsequent waves of cyber attacks which we see in large scale attacks. Therefore vulnerability log of the targeted project is more important than that of large scale attacks and there is no place for wasting. The detected security gap must be kept until suitable time comes to launch cyber attack.

If the aim of the cyber attacks to retard the progress of the project, cyber attack planners must consider the acceleration trends in the progress of the project and then determine the time of attack. In short, acceleration trend of the targeted project and the time of the attack are two crucial factors that lead to success or failure. As seen in Graph 2, acceleration of the Project Progress Level on t_2 more than that of on t_1. Time gained in an attack staged on t_2 will be more valuable than the one staged on t_1. Therefore best time for cyber attack is t_2. If not kept for the suitable time, the security gap will be closed after an attack on t_1.



Graph 2. Timing in Small Scale Cyber Attacks

III. Conclusion

Cyber attacks are different from the conventional ones in their side effects on the subsequent attacks. Ill-timed and ill-planned sequence of large scale cyber attacks may weaken the power of the ones next to it. The determinant timing factors in large scale cyber attacks are the response time of the defender and the interval between the waves of attacks. In small scale targeted cyber attacks there will be one shot opportunity because of the countermeasures taken by the defender soon after the attack. In this case acceleration trend of the progress of targeted development project will be the determinant factor to decide when to attack. The period when the project's progress gains acceleration will be the best time to launch cyber attack.

ACKNOWLEDGMENT

We thank to War Colleges Command, Army War College, Dept. of Combat Tactic staff officers for their valuable contribution.

REFERENCES

[1] E. T. Jensen, "Cyber Warfare and Precautions Against the Effects of Attacks," *Texas Law Review*, Vol. 88, pp.1533-1569.
[2] S. Mansfield-Devine, "Estonia: What Doesn't Kill You Makes You Stronger," *Network Security*, July 2012, p.13.
[3] I. Barzashka, "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on The Iranian Enrichment Praogramme," *The Rusi Journal*, April/May 2013, 158:2, p.48.
[4] R.A. Miller, D.T. Kuehl, and I. Lachow, "Cyber War: Issues in Attack and Defense," *JFQ*, Issue 61, 2d quarter 2011, pp.18-23.
[5] Sun Tzu, *Savaş Sanatı*, Trans.. Adil Demir, Kastaş Yayınevi, 2012, p. 58
[6] S. Mansfield-Devine, "Estonia: What Doesn't Kill You Makes You Stronger," *Network Security*, July 2012, p.14.
[7] I. Barzashka, "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on The Iranian Enrichment Programme," *The Rusi Journal*, April/May 2013, 158:2, p.54.

Ferhat Çalışkan received his B.S.degree in System Engineering from Turkish Military Academy in 2003. He was accepted in the Naval Postgraduate School (NPS) in California, and received M.A. degree in Security Studies-Middle East in 2011. He currently continues his study at the Turkish Army War College. He is interested in international relations, Middle East, game theory, cyber attack planning.

Yavuz İduğ received his B.S.degree in International Relations and Leadership&Management from the United States Military Academy at West Point in 2003. He received his MBA in Financial Management from the Naval Postgraduate School in California. He currently continues his study at the Turkish Army War College. He is interested in international relations, leadership & management studies and cyber attack planning.