SUN TZU, THE ART OF CYBER WAR

Bedirhan YILDIZ, Ozan MURAT, Mertcan KARAYILAN, Bahar TİMAÇ,
Çağrı DOĞU, Hüseyin YAĞCI,
Çağatay YÜCEL, Ahmet KOLTUKSUZ
Cyber Space Security Lab.
Yaşar University
Department of Computer Engineering

Aim

The battlefield strategies & methodologies defined by Sun Tzu in his celebrated field manual known as “The Art of War” have been mapped to the cyber space as it is the newly added dimension to the conventional warfare.

Definitions

Entropy is a unit of uncertainty of environment. It may thus be regarded as the amount of unknown information.

Shannon defined the entropy for the discrete systems as

$$H = -\sum_{p_i} \log_b pi$$

(Shannon, 1948)

Moreover, this definition, in another sense, may also be a metric for the information, such that “a measure of information in a distribution” (Shannon,1948).

Cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems.

The Cyber Arsenal

The amount of yearly produced data now exceeds Zettabytes (Csc, 2016). That huge amount of data gets to be processed it now presents itself as information which is the biggest asset in any cyberwarfare. Naturally this conversion of data into the information requires an equally powerful information processing hardware and software. This whole data/information producing, processing, storing and communicating over yet another medium known as the internet is collectively forms the digital arsenal of the cyber battlefield.

References

Shannon, C. E. (1948). The mathematical theory of communication. 1963. *MD Computing Computers in Medical Practice*, *14*(4), 306–317. http://doi.org/10.1145/584091.584093

Csc (2016). Big Data Universe Beginning To Explode, «http://www.csc.com/insights/flxwd/78931-big_data_universe_beginning_to_explode», 2016, Last Accessed: June 17th ,2016

Graphic Design by Murat ÖDEMİŞ

Mapping

Sun Tzu, The Art of War	Sun Tzu, The Art of CYBER War
The Army on the March	
“When an invading force crosses a river in its onward march, do not advance to meet it in mid - stream. It will be best to let half the army get across, and then deliver your attack.”	In this part, the concept of army is related with transferred data between actors. In this perspective, this data can be a part of an exploit code or an APT attack which tries to securely connect with control center in command & control state
Laying Plans	
“Now the general who wins a battle makes many calculations in his temple ere the battle is fought. The general who loses a battle makes but few calculations beforehand. Thus do many calculations lead to victory, and few calculations to defeat: how much more no calculation at all! It is by attention to this point that I can foresee who is likely to win or lose.”	In cyberspace, information can be modified by adversaries to deceive the actors. Adversaries uses OSINT and reconnaissance techniques to gather and manipulate information for their benefits.
Attack by Stratagem	
“Hence to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting.”	The main purpose of the kinetic war is to overcome the enemy’s resistance. On the other hand, the main purpose of cyber wars is the decreasing information processing capabilities of the enemy actors. Advance persistent threat (APT) is one of the useful tools in cyberspace for such an aim. APT clearly matches with Sun Tzu’s description of “**attack by stratagem**”.
Waging War	
“Hence a wise general makes a point foraging on the enemy. One cartload of the enemy's provisions is equivalent to twenty of one's own, and likewise a single PICUL of his provender is equivalent to twenty from one's own store”	Information stealing and cyber espionage can be considered as one of the powerful attacks in the cyber domain. As one’s knowledge against enemies increases, the more likely one is close to overcome enemies.
Use of Energy	
“In battle, there are not more than two methods of attack - the direct and the indirect; yet these two in combination give rise to an endless series of maneuvers.”	In cyberspace, the processing power is not only enough to have a powerful position on cyberwarfare for actors. Their aim should be paying the minimum cost to achieve their objective. They need to come up with several tactics and strategies because of variety in the cyber space. They should carefully select the best strategy for each situation.
Maneuvering an Army	
Changing the location of the fighters in three dimensions.	In cyberspace, the maneuvering of an actor is not a physical movement. Anonymity techniques and networks such as TOR network or VPNs can be considered as maneuvering and changing location.
Attack by fire	
“There are five ways of attacking with fire. The first is to burn soldiers in their camp, second is to burn stores, the third is to burn baggage trains, the fourth is to burn arsenals and magazines and the fifth is to hurl dropping fire amongst the enemy.”	The information processing was comprised of different processing units. Some of these units have more importance than others for information processing. Today’s cyber world, these units called as a critical infrastructure. Actor’s major information processing depends of reliable functioning of critical infrastructure.
Tactical Dispositions	
“Measurement owes its existence to Earth; Estimation of quantity to Measurement; Calculation to Estimation of quantity; Balancing of chances to Calculation; and Victory to Balancing of chances.”	One significant measurement system for cyber warfare is the very definition of **the entropy** as given in the previous chapter. Entropy can be utilized to calculate the chances of being under attack or chances as system is open to attack. Entropic analysis of unicity distance for a secure communication can lead to cryptanalysis of a system. Deep package inspection is also done on bits thus entropy calculation again might reveal the chances of being under attack or being vulnerable. Victory is dependent on balancing all of these chances as stated by Tzu, therefore the anectode applies.
Weak Points and Strong	
“The spot where we intend to fight must not be made known; for then the enemy will have to prepare against a possible attack at several different points”	Cyber attacks are to be made in the domain which takes place with a powerful interactions which can be controlled quickly and of which allows you to instantly be successful. An unexpected move, a surprise attack, is accomplished using the open source information. Whilst being incredibly powerful to conduct a surprise attack, it is as important as being ready for one.
Use of Spies	
“A major military operation is a severe drain on the nation, and may be kept up for years in the struggle for one day's victory. So to fail to know the conditions of opponents because of reluctance to give rewards for intelligence is extremely inhumane, uncharacteristic of a true military leader, uncharacteristic of an assistant of the government, uncharacteristic of a victorious chief.”	Use of spies in modern cyber warfare has transformed into the cyber world as utilization of Trojan and other types of Trap Door software. Considering a cyber war, it would be an uncharacteristic act of a nation to not to know of the cyber traces and network traffic of critical infrastructures and enemy units.