Clausewitzian Cyber Strategy

Michael Ecke Tufts University
Michael.Ecke@tufts.edu

December 13, 2018

Abstract

The strategies used in traditional warfare have been defined and expanded upon for centuries. These methods pertain exclusively to traditional warfare, by traditional means. The strategies discussed beginning with Clausewitz writing in the 18th century, have thus far been able to adapt to new technologies in warfare, as each step forward in technological advancement was not a difference in kind but a difference in degree. However with the development of cyber systems and a means to attack and defend those systems, cyber warfare has created a realm in which there is truly a difference in kind. In light of this fact a new strategy needs to be developed and expanded upon for how such technologies should be used and applied in the service to a nation state. This paper seeks to define the role that cyber warfare should and it most likely to take place in war between nations, and then secondly to define a strategy for cyber warfare built on the principles of past military theory. We will then apply this strategy to the newly defined cyber strategy as defined in a 2018 document signed by President Trump.

I. Introduction

Modern nations must be prepared for conflict in the traditional sense but now increasingly, must also be prepared for conflict in the digital or cyber realm. They therefore must answer the difficult question of what cyber methods should be used and when, in an effort to best serve their nation. Here they face a conundrum, as the strategic resources available to them do not immediately apply to the new realm of cyber warfare. There therefore exists a need for the definition of a new strategy that will allow nations to best secure their interests.

The Cyber strategy of today is not too dissimilar from that of feudal lords throughout medieval Europe. The more advanced the attacks became, the higher and more structurally complex castle walls were built. This strategy was effective until cannons used in the siege of Constantinople in 1453 rendered them useless[1]. Similarly in the cyber realm we have reached a point where higher walls will not be sufficient to defend a nation, what is needed is an entirely new strategy to account for the changing defensive landscape.

This paper will primarily be concerned with how modern nations can best defend themselves from attack, but as we will see attack and defense go hand in hand. We will set forth the argument that what is a new strategy in which proactive and preemptive measures are taken in order to prevent potential attacks. This argument stems from several basic premises, the first being that our systems as currently constructed are indefensible, secondly that there exists a fundamental asymmetry in cyber warfare that favors the attacker in almost all circumstances, and that the rate of cyber conflicts is certain to increase without the presence of a capable defense. The strategy will be primarily derived from an application of the classic strategic work "On War" by Carl Von Clausewitz.

II. Defining Terms

We first must begin with a definition of both war and cyber war. According to Clausewitz war is the extension of politics carried out by

[1] Crowley

other means. This entails forcing the opponent to do your will, despite them refusing to comply [2]. It follows logically that such a pursuit requires the use of force, at first to compel the opponent to do your will and then on the part of the defender to prevent you from doing so.

Cyber warfare can be defined as the intention to harm an oppositionâĂŹs software with the ultimate aim of compelling them to do your will. This can include viruses or worms with the intent of destroying software, denial of service attacks, or hacking to obtain critical data from an institution. Immediately we see that the definition of war is not congruent with what cyber war is or can be. The cyber realm does not onto itself have the ability to exert force on an opposition. Meaning that no person has ever been murdered or can be murdered by a computer virus directly. Therefore whatever force cyber means exert can only come indirectly from a secondary source. For example, causing a Russian pipeline to explode as was rumored to have happened in 1982[3]. The supposed software used to stage the attack did not itself explode, but caused the pipeline to explode. This fact necessarily means that the role that cyber can play in war is a limited one, and one that must be focused mainly on sabotage, subversion and intelligence gathering.

Subversion and intelligence gathering are inherently non violent, and while sabotage can be violent the violence most often focused on physical equipment, not on people. Despite their lack of violence cyber means can still be incredibly useful when trying to bring harm to the opposition. For this reason cyber security and a strategy for that security should be of the utmost importance to modern nation states.

III. Premises

i. Indefensible

The network systems of nation states, as currently constructed, are by their very nature unable to be defended. General Alexander director of the National Security Agency was recently quoted as saying "We know where we are today is indefensible"[4]. The reason for this is that our network systems are incredibly large and complex, and within that size and complexity hackers are able to take advantage of every error that exists within the system. For instance consider Windows XP, which contains an estimated 50 million lines of code. An operating system of that size cannot be secure, by virtue of the statistical probability that there exists some exploitable error within the code. Now extrapolating this idea to millions of devices from computers, to industrial control systems, to cell phones we can begin to see the scope of the problem. There are too many devices, running too many systems, for a nation to adequately defend them all[5]. This means that attempting to defend an entire system from attack is a futile effort that when taken in isolation will only allow for more breaches to take place.

ii. Asymmetric Attack and Defense

In traditional battle Clausewitz believed that the defense had the advantage stating âĂIJDefense is the stronger form of warâĂİ[6]. He characterized the defensive position as one of âĂIJAwaiting the blowâĂİ and believed that the purpose of defense was preservation. In cyber war defense occupies the same role, that of preservation, but it cannot be said that it is the stronger position. In fact we will demonstrate that it is by far the weaker position. Not only are the costs associated with a lost cyber attack close to zero, the attacker has the added advantage of only needing to strike a broad target effectively only once.

Clausewitz believed that defense was the stronger position in large part because of the defenses that could be built, to inflict harm on the oncoming attackers. The defenders then had an opportunity to inflict damage on the attackers. There does not exist any analogous

[2] Clausewitz pg. 83
[3] Rid
[4] Schactman
[5] Assante
[6] Clausewitz pg. 427

action in the cyber realm. The defending party does not have any opportunity to equivalently harm the attackers, they are forced entirely into acting for their own preservation.

The attacker in the cyber realm also has the benefit of having their attacks cause disproportionate damage to the defender. That is one small alteration in code, can create potentially gigantic consequences to a nation. This is not the case in traditional warfare where a large attack is required to achieve a large result.

There are several minimal consequences that the attacker should be concerned with should their attack fail. One of which, the possibility of exposing more advanced technology to your opponent is somewhat unique to the cyber realm, the other being the possibility of retribution is not. We will examine both of these in greater detail.

The possibility of the opposition obtaining more advanced technology is not one that should be quickly discounted. By examining past attacks between nation we can understand that in practice, this is not as large of a concern as was previously thought. For the moment we can break attacks into two categories, generic and non-generic.

Generic attacks include all of the well known and often used attacks such as DDOS, SQL injection, and cross-site scripting[7]. The technical elements of these attacks are well known to the public and their usage could not possibly result in any information gain on the part of the attacked. It should be noted that while widely known, the attacks are still effective. For example it is believed that Russia was able to deny service to EstoniaâĂŹs national network by launching the largest DDOS attack in history, by using a botnet consisting of 85,000 computers[8].

Let us now examine non-generic attacks. These attacks use technical methods that are not widely known to the public, and can be in development for years before they are put into place. Such attacks will contain technical elements that the attacker would not want to disclose to the opposition. However reverse engineering code that advanced can be a lengthy and difficult process. More importantly though, such advanced attacks are incredibly narrow in scope and may not be of any practical use to the opposition. For example consider the Stuxnet attack of 2010. It is estimated that it took a team of ten programmers 2-3 years to construct the virus. The virus was primarily looking for âĂIJeight or ten arrays of 168 frequency converters eachâĂİ, clearly it was incredibly narrow in scope aimed at obfuscating the Iranian nuclear program[9]. Therefore while the Iranians were undoubtedly able to gain some technical information by examining the program, that information must be in a limited context. Just as importantly the launcher of the attack has forewarning that the information will be obtained by the opposition, and consequently has the opportunity to limit their own exposure to such an attack.

If the attacker responds with a cyber attack of their own, it is unlikely that the failed attack increased their ability to strike the attacker. Meaning that the party that had initially been attacked is not now in a stronger attacking position. This differs fundamentally from traditional warfare, where a failed attack can result in the destruction of the attacking force, there is no corresponding element of cyber warfare. The initial attacker is unlikely to be occupying a worse strategic position in terms of their defensive or offensive capabilities.

Secondly the attacker must be concerned with the likelihood of a retaliatory traditional attack. This is unlikely, primarily because such an attack would represent an escalation of force from non-lethal to lethal means. Meaning that the party that launched a physical attack would risk starting a full blown physical conflict.

The end result of these factors is that deterrence as it is traditionally understood does not exist in the cyber realm to the same degree that it does in the traditional one[10].No nation can adequately increase the costs of an attack so great as to deter an opponent from launching

[7]Melnick
[8]Rid pg. 40
[9]Fruhlinger
[10]Clayton

a cyber attack at them, nor can they rely solely on defensive measures as they are technically inadequate[11].

IV. One Consequence - More Cyber-Attacks

Clausewitz explains the suspension of military action as being caused directly by the advantage of the defensive position over the offensive one.That is because as he says âĂIJIt is virtually unknown for the weaker party to attack the stronger party and stay on the defensiveâĂİ. This is due to the fact that in his view defense occuppies the stronger position already, and can immediately take advantage of their position. As we have seen above the defense does not hold any advantage in the cyber-sphere[12]. Therefore by analyzing the converse of ClausewitzâĂŹs implication, it seems likely that cyber attacks will become increasingly common between adversarial parties.

This is a further detriment to the defensive position. The defender needs time to patch exploitable issues in their software, and additional time to update software over a large network. Both of these activities will often take far longer than it will take for an opponent to exploit the issues. It seems as though the defense will be in the reactionary position of responding to attacks, with no ability to catch-up to the latest attack.

V. Defining the Strategy

The most fundamental set forth set forth by Clausewitz is that the goal of war is to "Render the enemy powerless". War he argues is similar to a duel between two persons, the goal of each person is disarm the other, which is to eliminate the possibility of the opposition causing harm to oneself[13]. The application of this principle to the cyber realm is seamless, if a party is trying to win a cyber conflict they must fundamentally harm the software of the opposition to eliminate their opportunity and ability to attack.

Today nation states should adopt a policy of frequent preemptive strikes to disarm the opposition before the opponent has the ability to harm them[14]. Such attacks should focus primarily on the destruction of the opponents software but may also take the form of denial of service attacks which also limit the oppositions ability to fight back. The technical methods of such attacks are unimportant, they can be as sophisticated or as unsophisticated as necessary to disarm the adversary. Such a strategy takes advantage of the fundamental imbalance that exists between the attack and defense positions. The reasons that such preemptive attacks must be frequent, is because of the increasing rate of attacks that will occur. This strategy most closely aligns itself with the fundamental object of war as described by Clausewitz. Additionally as discussed previously launching even failed preemptive attacks have very low costs associated with them.

VI. Analysis of 2018 Document

In September of 2018 the White House released a memo outlining the long term cyber strategy of the United States. We will analyze this strategy in accordance with the strategy that we have just defined. The presidents strategy consists of four pillars defined as follows.

- The protection and security of critical infrastructure
- Promoting and fostering a healthy cybersecurity economy
- Preserving peace through strength
- Advance American influence abroad

Of these four pillars the first and third are of particular interest. The first pillar contains an outline of a plan to secure federal infrastructure. While certainly necessary securing all federal infrastructure is truly a herculean task that may require years to complete if it is able to be completed at all.

[11] Weichart
[12] Clausewitz pg. 430
[13] Clausewitz pg. 85
[14] Schlein

The third pillar, while only consisting of very little text contains one encouraging point, "Build a cyber deterrence initiative"[15]. While deterrence would certainly be valuable as we have seen it is difficult to establish. The document goes on to explain that this deterrence should be established by using a variety of tactics including sanctions and "public statements". While these may be effective, they are only reactionary measures. That is they can only take place after the extremely difficult question of attribution has been settled, in this respect the tactic is extremely limited.

VII. Conclusion

The strategy that has been defined is congruent with previous strategic thinking, and complies with our current knowledge of the incentives that are at play in the cyber realm for nation states. If two nations are at odds with one another, it is the one that has initiated the attack that can be sure that they are the one standing on the higher ground, and the one who will be more likely to win a given encounter.

References

[1] Carl Von Clausewitz *On War*. Everyman's Library, New York, New York, 1993.

[2] Thomas Rid *Cyber War Will Not Take Place*. Oxford University Press, New York, New York, 2017.

[3] Roger Crowley *1453: The Holy War for Constantinople and the Clash of Islam and the West* . Hachette, New York, New York, 2006.

[4] Melnick:Top Ten Most Common Types of Cyber Attacks, https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

[5] Assante:America's Critical Infrastructure is Vulnerable to Cyber Attacks, https://www.forbes.com/sites/realspin/2014/11/11/americas-critical-infrastructure-is-vulnerable-

[6] Clayton:Cybersecurity: How Preemptive Cyberwar is Entering the Nation's Arsenal https://www.csmonitor.com/USA/Military/2013/0204/Cybe

[7] Fruhlinger:What is Stuxnet, who created it and how does it work?, https://www.csoonline.com/article/3218104/malware/wha

[8] National Cyber Strategy, https://www.whitehouse.gov/wp-content/uploads/2018/09

[9] Schachtman: Military Networks 'Not Defensible' Says General Who Defends them, https://www.wired.com/2012/01/nsa-cant-defend/

[10] Schlein:The Yahoo breach proves we need ways to hit the attackers before they strike https://www.recode.net/2016/9/23/13032420/yahoo-breac

[11] Weichart:The U.S. Needs A Preemptive Cyber Warfare Doctrine https://theweichertreport.com/2016/10/22/the-u-s-need

[15] National Cyber Strategy pg. 20