Clauswitzian Cyber Strategy

By Michael Ecke

Outline

- Definition of War, Cyber War
- Define the role that cyber warfare can play in warfare
- Premises
  - Nations are fundamentally incapable of defending themselves
  - In a cyber conflict the attacker has the advantage
- Define a strategy of preemptive attacks
- Look at the new strategy as defined by the White House

What is war?

- War is the continuation of politics by other means
- Bending the will of the opposition
- What characteristics does war have?
  - Force = Violence

- Question: Is a cyber attack violent?

What is a cyber attack?

- An attempt to exploit a computer system that one should not have access to
- The purpose of which may be:
  - To cause harm to the software
  - To steal valuable information
  - To disrupt a process that the computer is engaging in
- Is this an inherently violent action?
  - (NO)

What is the role of cyber attacks in war?

- Cyber attacks are not violent, they therefore are extremely limited in the scope of a conflict.
- Cyber means must rely on the application of indirect force
  - Sabotage – Think Russian pipeline explosion
    - (If that was indeed an act of sabotage)
  - Subversion – Think elections of 2016
  - Espionage - Stealing information

Why do we need a different strategy?

1. We need a strategy that doesn't rely on defense – something we cannot do
2. We need a strategy that accounts for the imbalance of strength between the attacking and defending positions in a cyber conflict

Our Network is not able to be defended

- "We know where we are today is indefensible" - General Alexander Director of the NSA
- There are too many computers, programmable logic controllers, cell phones and other computerized devices to account for
- Each device is likely to contain errors in its code that will allow for its exploitation
- Updating and defending all these devices is virtually impossible

Defense is the Stronger Position

There are low costs associated with a failed attack

- Attribution is a major problem in cyber security, which makes retribution difficult
- Launching a failed attack does not fundamentally change the position of the attacker
- The defending party has no opportunity to inflict harm on the attacker
- => There is no deterrence in the cyber realm

Remember…

The attacker only must be right once, the defender has to be right all of the time

The goal of war according to Clausewitz

- “Fighting forces must be put in such a condition that they can no longer carry on the fight”
- “To secure the object we must render the enemy powerless; and that in theory, is the true aim of warfare”
- To disarm your opponent

What we have so far…

- The network systems themselves are indefensible
- It is far easier to attack then to defend
- Goal of war is to disarm your opponent
- What does imply about what our behavior should be?

New Strategy

- Preemptive Strikes to the opponent's cyber capabilities
- Goals:
  - Destroy the software used to launch attacks
  - Or, at least deny the service to slow the rate of attack
  - Remove the opponent's ability to wage cyber war against you
  - "Get them before they get you"
  - "The best defense is a good offense"

Why does this make sense?

- No nation can afford to play defense
  - No nation has a good enough defense to play defense
- Playing offense guarantees that a given party will be occupying the stronger position in the conflict
- Allowing small amounts of sand to be thrown into the machine can cause disproportionate damage to the nation

Review of Trumps 2018 Cyber Policy

- Mentions deterrence briefly, using all available means except force
  - Reactionary measure that only works in absence of the attribution problem
- Aims to improve the defenses of our nations critical infrastructure
  - Nice goal, but highly unlikely
- No mention of preemptive strikes only "Peace Through Strength"

What we covered today:

- Definition of War, Cyber War
- Define the role that cyber warfare can play in warfare
- Premises
  - Nations are fundamentally incapable of defending themselves
  - In a cyber conflict the attacker has the advantage
- Define a strategy of preemptive attacks
- Look at the new strategy as defined by the White House