Demystifying Cyber-warfare

Cyber-warfare requires a different approach to warfare than conventional warfare. Nowadays, warfare principles and strategies have evolved and established by experience from philosophers or strategists like Gen. Sun Tzu or Clausewitz, to name two of the many. Some of the conventional warfare doctrines apply to cyber- warfare while some doctrines of conventional warfare are absolutely useless in cyber-warfare. Some standards of conventional, kinetic warfare may actually be incompatible to cyber-warfare.

Felix Juhl und Stefano Campestrin

Cyber-warfare is the sub-set of information warfare, which includes actions taken within the cyber world. The cyber world consists of any network-based environment contained within a conglomerate of computers and networks. There are **several cyber worlds,** but the most relevant one to cyber-warfare is the Internet and related networks which share and exchange data and media with or via the Internet. The closest military definition to our term, cyber-warfare, is a **combination of computer network attack and computer network defence** and eventually special information operations.

The definition of conventional warfare is warfare executed in the "real world". All weapons, tanks and ships, planes or drones and soldiers of current militaries are the means of conventional warfare. Conventional warfare has a history as long as mankind; this includes many attempts to derive doctrines for professionals of arms.

Cyber-warfare must have real world effects

Cyber-warfare is insignificant unless it affects someone or something in the non-cyber world. One can attack entities in the cyber world, but unless something occurs in the "real" physical world as a result, one might as well be playing simulation war-games. Such "physical" effects could be for example the contamination or manipulat of air filter and cleaned air circulation within hospitals or the shutdown of an electrical substation.

Cyber-warfare in its most subtle form can affect the perception of decision-makers in the physical world. The former is comparable to conventional warfare. The latter is merely a form of information warfare, in which one's adversary is provided with information that could lead to wrong decisions and thus (re-)actions.

Examples of affecting decision-makers include both: **on tactical and strategic level.** Tactical decision-makers could be misleading about the location and size of enemy and friendly forces. At operational level, the control of the supply chain could be manipulated and cause wrong decisions like attacking without sufficient ammunition or withholding an attack for fear of lack of supplies. Strategic decision-makers may be misled by attributing actions to other countries or groups than the actual attacker.

Active steps to hide in the cyber world remain more or less visible

The cyber world is artificial, created by humans using hard- and software. Any action that a combatant takes in this "virtual" world, **requires the movement or manipulation of data.** The very fact that each attempt to conduct cyber-warfare means that some bits in a data stream will be changed and reflect one's presence and actions, is really good news for defenders. But, this is only beneficial to the defenders who are looking for cyber-attacks. The author`s long-term experience in large-scale mass data analysis and anomaly detection projects can be summed up in the tragic and simple statement: "Sensors simply don't."

The analogy of hiding in cyber-warfare is the physical world use of camouflage. Physical world combatants can take active steps to modify their sensor footprints – for example by the use of stealth technology. In the cyber world, the combatants cannot take active steps equivalent to absorbing radar energy or cooling infrared signatures. In cyber-warfare instead, **the attacker must attempt to hide any evidence of activity within existing data streams.** Sensors monitoring cyber attacks or anomalies have to distinguish between bits that are artefacts of an attacker and the overwhelming majority of normal activity bits. This is made even more difficult by using normal activity to conduct an attack. Intrusion detection and prevention systems can therefore not distinguish between a standard user and adversary manipulating data or systems unlike a physical user.

Strenghten the Shield: the 53d EW Group © US MoD

There are no absolute rules of behaviour in the cyber world except those who require a physical world action

In the physical world, one can expect that a torpedo will act in a certain way once fired by a submarine. The torpedo's track can be predicted by ballistic calculations. Each time that one fires a torpedo, it will act in the same way, within a small variance due to minor physical factors. In the cyber world, **nothing can be taken for granted in this way.** The cyber world instead, as an artificial habitat, is imperfect. It can alter in ways that seem to be chaotic. The reasons are manifold: software failures, hardware failures, programs run faster than expected or codes behave not as expected in unknown network segments. There is an almost unlimited number of reasons for the unpredictability of the cyber world.

Therefore this principle leads in cyber-warfare to **attacks, which don't deliver constantly the same results** due to changes in the environment and variances in the systems performances. The only aspects of the cyber world that do not change are the ones requiring changes in the physical world. The performance of any malicious software cannot exceed the capacity of a computer's processing power. Not unless a physical world person upgrades the computer with more processing power. Also is the **bandwidth of the communications network limited by the infrastructure** and can only be altered by replacing one physical layer with another.

Out in the cyber world someone has the will, the ability and the means to attack – and he does!

Since the cyber world is built and controlled by humans and their tools, there is no part, which is not controlled by someone or his technology driven agent. Sometimes controls have even passed to software elements. Given the

authority, the capability and the access to computer networks, technology has become the avatar of human being. However, there is always someone or something that can do whatever the cyber-combatant wishes to do. Anyway, most of the steps in any attack in cyber-warfare are simply intended to fake the identity of the entity which carries out the action.

The instruments of cyber-warfare are exceptionally fit for dual-use

The tools and technologies used for conventional warfare are generally speaking designed for one single purpose. Weapons are used to attack, armour is meant to protect and defend and sensors are built to detect. In actual warfare, armed forces do not test their defences by shooting on own troops. A commander of an ambushing unit uses night-vision gear on the watch for the enemy. He could, but hardly does, look from the enemy's direction towards his troops through his very own night-vision gear.

In cyber-warfare, both, the attacker and the defender use tools and technologies. The attacker uses vulnerability scanners to search for exploit opportunities as part of or preparation for an attack. The defender uses the same vulnerability scanners to search for weak spots in their very own systems. **Packet capture devices are often at the origin of these weak spots,** because network administrators need to monitor the actual packet traffic, so as to detect network problems and bottlenecks. Defenders use them to test their own systems, trying to identify vulnerabilities

US Air Force Network Operations Centre © US MoD

from poor vendor upgrades or hidden black boxes, collecting specific exploits. Attackers use the same procedures to discover breaches in the cyber-defence.

Both, the defender and the attacker, control only a very small part of the cyberspace they use

The attacker and the defender in cyber-warfare only actually control that hard- and software which they own. Frequently, this limit is their actual physical perimeter. **Rarely does a cyber group control anything beyond their interface with the communications infrastructure.** Worldwide studies show that most armies are effectively controlling **only about 10% of the communications infrastructure in use for their own operative traffic.** This means, that 90% of the infrastructure used by attackers and defenders are beyond their control.

Even if none of the parties in cyber-warfare controls the infrastructure they use, they still remain vulnerable to attacks on uncontrolled parts of the infrastructure. If one of the combatants gains control of a part of this infrastructure, he also has gained advantage over his counterpart.

Cyberspace is neither coherent nor reliable

Yet another feature of the artificial nature of cyberspace is that it is not coherent or reliable. This is related to the basic understanding of absolute laws: neither hardware nor software will always work as expected. This is true more of software, but as a matter of fact, there is inconsistency in hardware too, usually due to heat, power loads or component failure.

The effect of this fact is that nobody can be certain if a specific step within an attack will work as expected. Yet an opposite effect of the lack of consistency or reliability is that attacks may also fail to succeed, and frequently do so.

Physical limitations of apply to the cyber world

In cyber world, physical distance is not an obstacle to conduct attacks. A cyber attack can be executed with equal effectiveness from **any point of the world** as from the next room or the very same system. In conventional warfare, physical means have to surmount a previously defined space to carry out a specific action. These attacks are limited to those who have acquired technology to surmount space.

The acquisition of the proper mass for an attack in the conventional world has physical limitations in great numbers. The creation of mass in the cyber world has nearly no limitations.

Conclusion

Cyber-warfare is different from conventional warfare – although both depend on the imperfections of humans for many reasons. One of the fundamental differences between cyber-warfare and conventional warfare is the nature of their environment. Conventional warfare takes place in the physical "real" world, governed by laws of physics, which we tend to believe to know and understand. Cyber-warfare instead takes place in a man-made "virtual" world, which is disordered, sometimes chaotic and imperfect. **Cyber-warfare may use some of the doctrines of conventional warfare, but they have mostly little or no meaning in cyberspace.** For these reasons, the doctrines of cyber-warfare are ultimately different from those of conventional warfare but should nevertheless not be taken for granted to be successful.

(Felix Juhl ist Cyber-War- und Targeting-Experte.)

□