Principles of Cyberwarfare

Cyberwarfare is different from classic kinetic warfare and therefore requires a review of basic warfare principles to differentiate it from armed conflict in the traditional sense.

Raymond C. Parks and David P. Duggan
Sandia National Laboratories

Classic, kinetic warfare principles have been derived from thousands of years of experience as Tsun Tzu, Carl von Clausewitz, Antoine-Henri Jomini, Basil Henry Liddel-Hart, and others have documented. Some kinetic warfare principles apply to cyberwarfare, others have no meaning in cyberwarfare, and a few may actually be antagonistic to cyberwarfare.

The principles of warfare guide warfighting at the strategic, operational, and tactical levels. They're the enduring bedrock of US military doctrine, derived from practical experience and the wisdom of those who documented that experience. Those who followed these principles have won, and those who did not have lost. Clearly, we do not have thousands of years of experience in cyberwarfare, so we have to start with what we have had. Many cyberwarfare incidents are classified and not available for public discussion. Fortunately, our experience in red-teaming can act as a surrogate for the undisclosed.

As practitioners, we derived the principles of cyberwarfare discussed in this article from the bottom up. As part of Sandia National Laboratories' Information Design Assurance Red Team (IDART), we've had hands-on practice through red-team exercises, which are equivalent to limited cyberwarfare scenarios. We wrote the first version of this article in 2001, when we had approximately five years of experience.[1] The cyber domain has changed, and we, along with our colleagues, have learned since then. While conducting active adversarial analyses of information systems, we identified eight cyberwarfare principles. This is not an exhaustive list, nor is it intended as the final definitive one. Instead, these principles are a continuation of the discussion with the cyberwarfare community that we began with our first article. We chose principles from practical experience. When we follow these principles, we win; when we do not follow them, we lose.

Definitions

To present our cyberwarfare principles, we must define our terms. Dan Kuehl defines *cyberspace* as "an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interconnected information-communication technology (ICT) based systems and their associated infrastructures."[2] This coincides with our original description of the cyberworld as any virtual reality contained in a collection of computers and networks. Many cyberworlds exist, but the one most relevant to current cyberwarfare discussions is the Internet. *Cyberwarfare* is a combination of computer network attack and defense and special technical operations.[3]

We define *kinetic warfare* as warfare practiced in the land, sea, air, and space domains. All current militaries' tanks, ships, planes, and soldiers are kinetic warfare's protagonists.

Kinetic Principles

Kinetic warfare has a history as long as mankind's and

1540-7993/11/$26.00 © 2011 IEEE

includes many attempts to derive principles for practitioners. Many have attempted to pass on the wisdom and insight they've gained, usually through hard lessons. Publications on cyberwarfare frequently cite Tsun Tzu's *The Art of Strategy*.[4] Its primary relevance to cyberwarfare involves our principle that attacks must have a real-world effect. Tsun Tzu recommends manipulating the adversary's decision-making. Clausewitz's *Vom Kriege* (*On War*) seems to have lost popularity with many cyberwarfare writers, but we believe it still has relevance, particularly its assertions on the will to win, the "fog of war," and the friction of war.[5] Cyberwarfare as a part of information operations can affect the enemy's will to fight, and we aimed our strategic cyberwarfare attacks for theoretical exercises and workshops at increasing the fog and friction of war. Liddel-Hart's principle of indirect approach is likewise applicable to cyberwarfare.[6] In our experience, cyberdefenses are best handled, from an attacker's point of view, by avoiding them altogether. In exercises that have had limited defenses, we as attackers have either bypassed the defense or ignored it.

We have no intention of traversing an exhaustive list of kinetic warfare principles here. We consider the following principles, drawn from Figure I-1 of US Department of Defense (DoD) Joint Publication 1, primarily to compare them to cyberwarfare:[7]

- The kinetic principle of *objective* is to direct every military operation toward a clearly defined, decisive, and attainable objective. This is certainly applicable to cyberwarfare. Our adversary models include the principle of objective as part of all adversaries other than unsophisticated attackers.[8,9]
- The kinetic principle of *offensive* is to seize, retain, and exploit the initiative. In kinetic warfare, the inertia of opposing forces means that seizing the initiative is difficult. In cyberwarfare, there's almost no inertia—moving bits is much easier than moving tanks, ships, and aircraft. This makes the offensive principle less relevant in cyberwarfare, which will likely involve simultaneous action and reaction at a frenetic pace. The principle of offensive still applies to a lesser extent because of the inertia in the minds of the attackers and defenders—psychological rather than physical inertia.
- The kinetic principle of *mass* involves concentrating the effects of combat power at a particular place and time to achieve decisive results. Overwhelming force is largely irrelevant to cyberwarfare except when engaging in denial-of-service (DOS) attacks that emulate kinetic warfare actions. Cyberwarfare is different from conventional warfare in that stealth and surprise are supremely important. At the Cyber Strategy Workshop in October 1999, one presenter made analogies between cyberwarfare and submarine warfare. Several other participants pointed out the similarity between cyberwarfare and special operations. Both of these analogies are suitable in our opinion. Law enforcement professionals from both the FBI and Secret Service have told us that our cyberterrorist model closely matches assassins' operational profiles.[8] In none of these cases is mass as important in cyberwarfare as in kinetic warfare.
- Cyberwarfare is inherently an application of the kinetic principle of *economy of force*—to allocate minimum essential combat power to secondary efforts. Because cyberwarfare is the epitome of asymmetric warfare, economy of force for both secondary and primary efforts is inherent.
- The kinetic principle of *maneuver*—placing the enemy in a position of disadvantage through the flexible application of combat power—is applicable to cyberwarfare. However, attackers and defenders do not physically or virtually move their forces—they move the point of attack or defense.
- The kinetic principle of *unity of command* is to ensure unity of effort under one responsible commander for every objective. This is applicable to cyberwarfare in most operations; however, there are certain cyberwarfare attacks, such as crowdsourcing and Anonymous' Low Orbit Ion Cannon, that use unwitting bystanders or loosely controlled volunteers who are not within the command of the protagonist.
- The kinetic principle of *security*—to never permit the enemy to acquire unexpected advantage—applies to cyberwarfare, but in a different sense. The risk to operational forces in cyberwarfare is far less than kinetic warfare, but the risks of failure before achieving the desired effect and having weapons turned back on the user are higher.
- The kinetic principle of *surprise*—striking the enemy at a time or place or in a manner for which it's unprepared—applies to cyberwarfare, perhaps more than kinetic warfare.
- The kinetic principle of *simplicity* is to prepare clear, uncomplicated plans and concise orders to ensure thorough understanding. This applies to cyberwarfare because of the danger of fratricide when one operational unit denies another access or burns a weapon on a lesser target.

Interested readers can find a useful consolidation of additional kinetic warfare writings in the Department of Defense's "Doctrine for the Armed Forces of the United States."[7]

Proposed Cyberwarfare Principles

We base most of these principles on observations of how things work, online and during active engagements. We have experience with more than 300 red-teaming activities ranging from planning attacks to white-boarding exercises to actual hands-on engagements.

Lack of Physical Limitations

Physical limitations of distance and space do not apply in the cyberworld. In cyberspace, physical distance is neither an obstacle nor an enabler to conducting attacks. A cyberattack can be executed with equal effectiveness from the other side of the Earth as from the next room. In kinetic warfare, attacks are carried out by physical objects that must traverse a distance. These types of attacks are limited to those who possess the technology to make that object traverse that distance.

In our red-teaming work, we've planned, developed, and performed attacks that occurred in the room next door, multiple locations around the globe, and all points in between. The advent and widespread use of wireless networks have added the RF aspect of the physical dimension—an attacker in the parking lot can be just as dangerous as one in the server room. Attacks can use intermediary systems, networks, and even human actors to prevent attribution by the defenders.

Acquiring appropriate mass in the kinetic world has physical limitations. The creation of mass in the cyberworld doesn't seem to have this limitation. Attackers can generate multiple copies of a cyberweapon with almost no expense of time or materials; basically it's unlimited and unconstrained as a "material" component of warfare.[10] Even as we wrote this article, the hacktivist group Anonymous illustrated this point with its Low Orbit Ion Cannon, with the download of 30,000 copies as part of Operation Payback.[11]

Kinetic Effects

Cyberwarfare must have kinetic-world effects. It is meaningless unless it affects someone or something in the real world. Attackers can attack entities in the cyberworld as much as they want, but unless something happens in the physical world as a result, they might as well be playing Core Wars. Cyberwarfare can directly affect objects in the physical world, such as the opening of a dam spill-gate or shutdown of an electrical substation. Cyberwarfare in its most subtle form can affect the minds of decision-makers. The former is analogous to kinetic warfare; the latter is more purely a form of information warfare, in which attackers present opponents with information that leads to bad decisions.

Examples of real-world effects abound—the Aurora demonstration by Idaho National Laboratories showed that cyber manipulation of an electrical power grid can cause equipment failures.[12] In the course of our red-teaming, we exposed the possibility of attacks that would open dam floodgates and cause railroad accidents.

Previous attacks have affected both tactical and strategic decision-makers. Attackers can mislead tactical decision-makers about the location and size of enemy and friendly forces. At an operational level, we red-teamed a logistics system to manipulate the arrival time and amount of supplies and reinforcements to cause bad decisions, such as attacking with insufficient ammunition and delaying attack through fear of lack of supplies. In addition, strategic decision-makers might be fooled by attributing actions to other countries or groups than the actual attacker. We co-developed a scenario for a cyberdefense workshop that centered on an adversary attempting to foment war between two countries via cyberwarfare. The participants playing the role of the government leaders could not determine the real adversary.

Stealth

People can take active steps to hide in the cyberworld, but everything we do is visible. The question is whether someone is looking in the right place at the right time.

The cyberworld is an artificial one, created by human beings using hardware and software. Any actions combatants take in that world require data movement or manipulation—some bit in some data stream is changed to reflect their presence and actions. This is good news for defenders, but it's only useful if the defenders are looking. Since writing our previous article, intrusion detection and prevention and attack correlation technology have improved—but the attacker can still use stealth to hide in the bits.

Hiding in the cyberworld is analogous to using camouflage in the physical world. Physical-world combatants can modify their sensor footprint using stealth technology. In the cyberworld, combatants cannot take steps equivalent to absorbing radar energy or cooling infrared signatures. Instead, cyberwarfare protagonists must try to hide evidence in the existing data streams. Sensors looking for cyberattacks must distinguish between bits that are an attacker's artifact and the overwhelming majority that are normal activity. Using normal activity to conduct an attack complicates this. For instance, signature-based intrusion detection systems cannot distinguish between a normal database user and an adversary manipulating the database as that user.

The fact that some data, such as network packets, is ephemeral means that defenders must capture it to a more persistent medium. However, such global data collection creates its own problems with data analysis—the "needle in the haystack" problem.

Mutability and Inconsistency

There are no immutable laws of physics in the cyberworld except those that require a physical-world action to change. Cyberspace is sufficiently mutable so it is neither consistent nor reliable. This principle was originally two separate principles, but because they're so interrelated, we combined them.

First, we address the inconsistency of cyberspace. In the physical world, we can expect that a bullet will act in a certain way when fired—we can predict the bullet's path with ballistics. Every time a shooter fires a bullet, it will act the same, within a variance due to minor physical causes. In the cyberworld, nothing can be taken for granted in this way. The cyberworld, as an artificial construct built by humans, is imperfect. It can and does change in ways that seem chaotic. Software fails, hardware fails, programs run faster than expected; these and a thousand other variations cause unpredictability.[13]

In cyberwarfare, this inconsistency translates to attacks that do not always behave the same way, environments that change midattack, and fluctuations in attack performance. The only aspects of the cyberworld that don't change are those that require a physical-world modification. For example, software performance cannot exceed a computer's processing power capacity unless a physical-world person switches to a faster processor. Communications bandwidth is limited by the telecommunications infrastructure and can only be changed by changing that infrastructure.

An example of real-world experience that supports this occurs during sniffing of packets. We frequently see one set of connections and packet streams during discovery only to find a different set when we attempt our attack.

Another artifact of cyberspace's artificial nature is that it is not reliable. Neither hardware nor software will always work as expected in cyberspace. This is true more of software, but we've seen hardware inconsistencies, usually because of heat or power loads.

One effect of this principle is that we can never be certain that a particular step in an attack will work. We plan attacks using diagrams that show the change in a system's state from the initial adversary access to the point of reaching the goal. Each path through the diagram is an *attack scenario*, and the set of attack scenarios that a particular attacker can achieve is a *scenario set*. Attack scenarios comprise individual attack steps—information gathering, setups, and dastardly deeds. Each attack step has an uncertainty factor. In one engagement, we had carefully collected local privilege-escalation exploits to use after we gained remote user access to a known version of Solaris. However, we were frustrated to find that none of the exploits worked, despite being aimed at the correct version of Solaris. Because this was a red-teaming engagement in cooperation with the defenders, we were talking to the defenders. One of the target network's administrators informed us that a variant of an exploit that was supposedly fixed two versions earlier worked quite well. In another exercise, we conducted system scans with multiple tools, then spent days trying to understand why the results were so different. This effect was even more pronounced when we scanned a global enterprise's networks for exposed services. Three separate scans found different quantities of systems—120,000 systems on one, 160,000 on another, and 140,000 on a third. The changes were due to physical-world changes—laptops disconnected, systems turned on or off, network connectivity lost.

Another effect of the lack of consistency and reliability is that attacks we do not expect to succeed frequently do. In one exercise, we believed that the defenders had successfully hidden unencrypted password traffic in a VPN. Much to our surprise, they had left one service outside the VPN, which provided us with the necessary password to log in as the database administrator. That particular exercise taught us that risk calculation must include the potential benefit to the adversary as well as attack metrics, such as difficulty and probability of success.

Identity and Privileges

Some entity in the cyberworld has the authority, access, or ability to perform any action an attacker desires to perform. The attacker's goal is to assume the identity of that entity, in some fashion.

Again, because the cyberworld is a purely artificial construct, it's built and controlled by humans and their tools. There is no part of the cyberworld that is not controlled by a person or that person's cyberagent. Sometimes the entity with the authority, access, or ability is an avatar. Sometimes the human passes the control to a software element. But there's always something or someone who can do what the cybercombatant wants to do. Most of the steps in any cyberwarfare attack are intended to simply assume the identity of the entity that can perform the desired action.

A classic example is the Unix root exploit. When attackers perform a root exploit, they're attempting to assume the identity of a Unix system root superuser. In our exercises, we used root exploits as steps in attacks that involved changing the target systems' configuration or software.

The cyberworld, as an artificial construct built by humans, is imperfect. It can and does change in ways that seem chaotic.

However, the root exploit is not the only example, or even the most common. During the course of many exercises, we discovered and stole the identities of ordinary users, database administrators, system programs (such as Unix daemons and Windows services), and developers. In every case, we first found out who or what could perform the action, and then we worked to assume that identity.

Dual Use

Cyberwarfare tools are always dual use, whereas the tools of kinetic warfare are more single purpose, primarily used for one purpose of offense, defense, or sensing. Weapons are used to attack, armor is used to defend, and sensors are used to detect the enemy. In kinetic warfare, defenders do not test their defenses by shooting their own troops or equipment. Commanders of an ambushing unit might use night-vision gear to look at their own troops from the enemy's viewpoint to ensure the ambush's success. This use of sensors is both offensive and defensive, but this is an exception to the rule.

Attackers and defenders in cyberwarfare use the same tools. Attackers use vulnerability scanners to look for exploit opportunities as part of an attack. Defenders use the same vulnerability scanners to look for weaknesses in their own systems. Packet capture devices originated because network administrators had to see packet traffic to diagnose network problems. Attackers use packet capture for discovery. Attackers collect exploits to use against their targets. Defenders collect exploits to test their own systems, because mission or business requirements might prevent patching and because those systems can regain vulnerabilities from poor vendor upgrades.

Kinetic weapons are used against representative samples of physical-world defenses and systems to study their effects, but not against actual defenses or systems because of the cost—in both money and time—of reconstituting affected systems. We don't normally bomb our own missile silos, tanks, airfields, and ships. However, cyberweapons are routinely used against actual defenses and systems (as with penetration testing) with the belief that these systems can be rebuilt for almost no cost.

Infrastructure Control

Both defenders and attackers control a very small part of the cyberspace they use. Whoever controls a part of cyberspace that the opponent uses can control the opponent, thus the most recent trend is toward testing one's own networks by attacking them preemptively. Frequently, the limit of the controlled cyberspace is the actual physical perimeter; rarely does a cybergroup control anything beyond its interface with the communications infrastructure. After the Persian Gulf War, open literature hypothesized that the DoD directly controls only 10 percent of the communications infrastructure used for DoD traffic, with the remaining fraction under commercial providers' control. This means that neither the attacker nor defender controls 90 percent of the infrastructure used in the course of its activities. Thus, both parties are vulnerable to attacks on third-party infrastructure. If one or the other can gain control of part of that infrastructure, that party gains a significant advantage.

An example of this quest for control is Domain Name System (DNS) attacks. DNS provides the glue on which applications rely to find each other. Over the years, many publicly disclosed DNS attacks have occurred, which we used in our simulation exercises. Once we gained control of a DNS, the target applications found other applications only if we allowed it. We used this type of attack to bypass an early implementation of Internet Protocol Security (IPsec) during an exercise in June 2000.

Another example of this quest for control is the use of Border Gateway Protocol spoofing to control routes to Georgian government websites during the Russian cyberwar with Georgia.[14] Georgian sites were inaccessible because traffic to them was routed through autonomous systems purported to be controlled by the Russian Business Network.

Information as Operational Environment

The terrain, the weather, the enemy—every part of warfare's operational environment is information. If warriors perform Joint Information Preparation of the Operational Environment (JIPOE) for kinetic warfare, they collect information about each of these factors that represents the underlying physical reality. The collection requires sensors that transform the physical reality into information. In cyberwarfare, it's the information itself that constitutes JIPOE. The communication connections, computer network maps, personnel rosters, websites, links, emails, postings, and every other aspect of the target is already information in cyberspace—there's no conversion from physical measurements to information.

Cyberwarfare is different from conventional, kinetic warfare. Like its parent, information warfare, many of its characteristics depend on human frailties. One of the fundamental differences between cyberwarfare and kinetic warfare is the nature of their environments. Kinetic warfare takes place in the physical world, governed by physical laws that we know and understand with respect to warfare. Cyberwarfare takes place in an artificial, man-made world that's constantly changing. Cyberwarfare can use some principles of kinetic warfare, but others have little or no meaning in cyberspace. For these reasons, the principles of cyberwarfare are, ultimately, different from those of kinetic warfare.

Using the principles of cyberwarfare should lead to success in cyberwarfare. We believe we have some of the principles right, but by no means do we believe we are completely correct. This is the first step in the process of developing the real principles; years of experience will show what will win and what will lose. We do not claim to be the Tsun Tzu or Clausewitz of cyberwarfare—we are the unknown cavemen who first chipped rocks into spearheads and knives and fought over herds of wild animals. □

Acknowledgments

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the US Department of Energy under contract DE-AC04-94AL85000.

References

1. R.C. Parks and D.P. Duggan, "Principles of Cyberwarfare," *Proc. 2001 IEEE Workshop on Information Assurance and Security*, IEEE CS Press, 2001; www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA424310.
2. D. Kuelh, "From Cyberspace to Cyberpower," *Cyberpower and National Security*, F.D. Kramer, S.H. Starr, and L. Wentz, eds., Potomac Books, 2009.
3. US Dept. of Defense Joint Publication 3-13, "Joint Doctrine for Information Operations," 9 Oct. 1998; www.c4i.org/jp3_13.pdf.
4. T. Tzu, *The Art of Strategy*, Doubleday, 1988.
5. C. von Clausewitz, *Vom Kriege* (*On War*), CreateSpace, 2009.
6. B.H. Liddel-Hart, *Strategy*, 2nd ed., Plume, 1991.
7. US Dept. of Defense Joint Publication 1, "Doctrine for the Armed Forces of the United States," 14 May 2007; www.dtic.mil/doctrine/new_pubs/jp1.pdf.
8. G. Schudel, B. Wood, and R. Parks, "Modeling Behavior of the Cyber-Terrorist," *Nat'l Security Forum Int'l Cooperation to Combat Cyber Crime and Terrorism*, Hoover Inst. Press, 1999.
9. R. Duggan, "Insider Adversary Model Briefing," *DARPA IASET Insider Workshop*, DARPA, 2000.
10. S.M. Convertino, L.A. DeMatiei, and T.M. Knierim, "Flying and Fighting in Cyberspace," July 2007; www.au.af.mil/au/awc/awcgate/maxwell/mp40.pdf.
11. J.E. Dunn, "Wikileaks DDoS Tool Downloads Grow Rapidly," *Network World*, 10 Dec. 2010; www.networkworld.com/news/2010/121010-wikileaks-ddos-tool-downloads-grow.html.
12. J. Meserve, "Sources: Stage Cyber Attack Reveals Vulnerability in Power Grid," CNN, 26 Sept. 2007; http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US.
13. G.J. Rattray, *Strategic Warfare in Cyberspace*, MIT Press, 2001.
14. "Georgia Cyberwarfare," Russian Business Network, 9 Aug. 2008; http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare.html.

***Raymond C. Parks** is a senior member of the technical staff at Sandia National Laboratories. He currently develops tools to make process-control system assessment easier and safer. His research interests are cyberwarfare principles, strategy, and operations. Parks has a BS in engineering from the US Air Force Academy. Contact him at rcparks@sandia.gov.*

***David P. Duggan** is a technical manager at Sandia National Laboratories. His current and past work includes enterprise network monitoring, cyber perimeter security, integrated security, and intrinsic security. His research interests are intrusion detection and red-teaming. Duggan has an MS in computer science from the University of New Mexico. He's a life member of the ACM. Contact him at dduggan@sandia.gov.*