Robert Jones
PHIL 400

I. An Introduction to Information Warfare

An ever-evolving but by no means new concept, information warfare can broadly be described as a struggle over strategically useful information and communication processes. Naturally, information warfare takes on a variety of forms, from malicious attacks on enemy computer networks to the manipulation of existing communication and information networks to deny or subvert data. Therefore it is important that we clarify the particular forms of information warfare we are discussing before we can discuss their ethical implications and applications on the modern battlefield.

In an essay for for the National Defense University titled “What is Information Warfare?” Martin Libicki identifies Information Warfare as not a singular concept or method of warfighting, but rather an amalgamation of seven different loosely-related concepts. He outlines these as command-and-control warfare, intelligence-based warfare, electronic warfare, psychological warfare, hacker warfare, economic information warfare, and cyber warfare. Some of these, such as intelligence-based warfare and command-and-control warfare (which seek battlefield dominance through superior intelligence gathering and denial and disabling of enemy intelligence and command centers, respectively), are concepts that have been in use for a long time. Rather than walk down those roads again, this essay will focus on those methods of information warfare that have come to the forefront in the past twenty years and are not yet commonly-utilized methods in warfighting. Specifically, we will be examining hacker warfare and the closely-related modern evolutions of intelligence-based warfare.

Intelligence-based warfare, while not a new concept, has undergone a dramatic transformation in the past twenty years. While the battlefield has always hosted a struggle for intelligence (usually in the form of reconnaissance), computerized networks have made collecting, storing, disseminating, and sharing information faster and easier, as well as allowing for said information to be applied directly to operations rather than being funneled through a command structure. But just as these computerized networks have made certain information processes easier, they have also made theft, corruption, or destruction of that information easier, as computerized networks are more vulnerable to attack and fraud from remote locations. As computer systems become more advanced, the need to develop, maintain, and exploit information systems to maintain a battlefield advantage will become ever more pressing.

Hacker-based warfare on the other hand, is a much newer but closely-related concept. The term refers to malicious computerized attacks on information networks that are done by exploiting gaps in a system's security structure (although keep in mind that these gaps may be physical, such as the physical theft of a password or physical access to a terminal connected directly to the network). More frequently, these attacks are done through remote access, and carried out through the use of worms, viruses, or trojans, special pieces of software designed specifically to disrupt computer systems. Up to this point, the vast majority of hacker attacks have been on civilian targets, which are less secure than their military counterparts, and they have been domestic in nature (the computerized equivalent of car theft and joyriding rather than a legitimate attack on the United States and its infrastructure). However, hacker-based warfare may also be considered a means of waging war, as we will see later on.

Each of these concepts can be further subdivided into their offensive and defensive aspects for discussion. Defensive intelligence-based warfare (which has long been the foremost concern of the United States with regard to information warfare) is concerned with the development, maintenance, and defense of its information gathering networks. Likewise, offensive intelligence-based warfare is concerned with the denial or subversion of opposing intelligence systems. In a similar fashion, defensive hacker warfare consists of the active defense of intelligence networks (including civilian networks, which we'll discuss later) against malicious computerized attacks (the similarities between defensive intelligence-based and hacker warfare are small), and offensive hacker warfare consists of the active pursuit of malicious attacks on opposing networks. Unlike offensive Intelligence-based warfare, which concerns itself merely with the computerized networks of an opponent, offensive hacker warfare seeks not only to disable these systems, but also to attack the enemy more directly, usually through the denial of critical services controlled by computer systems.

As a result of its continued technological growth, the United States is part of a unique asymmetry regarding information warfare. As computerized networks develop and spread, the United States is both better equipped to engage in offensive information warfare and more vulnerable to some of its effects. That is, as computerized networks spread, larger areas and systems will become more vulnerable to hacker attacks while information gathering and sharing capabilities increase. The same is true for critical civilian services such as utilities. As these services become more automated, the need for security of their networks and redundancy in their systems will increase. And while military networks are often much less vulnerable to attack than civilian networks, attacks

on civilian networks can be equally devastating or disrupting. Additionally, few nations match the level of computerized progress that the United States has achieved, forcing it to deal with this problem alone.

A final point of consideration is the offensive hacker warfare that may be adopted by terrorist cells in the near future, which has been labeled ‘cyber-terrorism.’ Raids of Al Qaeda computers in 2003 gave indications that members of the organization had recently been conducting reconnaissance on critical infrastructures in the United States. Additionally, many of these same operatives had already had or had begun to receive training in computer security and programming (some at universities in the United States). While most utilities and critical processes are not currently very susceptible to remote attack due to their current level of automation and redundancy, there are several examples of past attacks by domestic hackers that have caused major, if only short-term damage, specifically with the stock market.

II. Ethical Considerations in Information Warfare

There are a number of important ethical questions that can be raised regarding these methods of Information Warfare, especially hacker warfare. For defensive hacker and intelligence-based warfare, the real issue seems to be determining whether or not the United States Department of Defense should be responsible for the protection and security of civilian systems, and in what ways, if any, this level of security should be pursued.

To date, the actual impact of hacker attacks on military networks has been minimal, despite reported increasing numbers of attacks annually on Department of

Defense systems. And as absolute security from hacker attacks is as simple as removing a system from the global network (a process called “air-gapping,” in which a computer or network is simply not connected to the larger outside network), key military systems are often impenetrable, as access depends on going through terminals that are hardwired to the corresponding network (and a key focus of hacker warfare is accomplishing its aims from a remote location). However, civilian and other less secure networks are still open to considerable risk, including critical systems such as phone lines, energy and utilities, monetary transfer networks, safety systems, and defense contractor networks. It is clear that for some of these systems, an increased level of security is necessary.

In what ways then, should the Department of Defense take a more active role in the security of civilian networks? While most of these systems have yet to experience a catastrophic failure from an attack, the possibility of such an attack occurring is not impossible. Likewise, security for many systems remains relatively low due to the low frequency of major attacks on those networks. But is this infrequency a compelling reason to avoid expending resources in an attempt to secure those networks? Another concern is related to the security itself: regardless of the level of security of these systems, hacker attacks will grow increasingly more sophisticated in an effort to break new defensive barriers. Are these attacks helpful for increasing security or a harmful byproduct of increased security? If the latter is the case, then increasing security on some systems may increase the risk to less protected systems.

Offensively, the question concerning hacker warfare is whether or not it should be waged at all by the United States. Given the strong security of military networks, the majority of offensive hacker warfare would be directed at weaker civilian networks for

the purposes of attacking an opposing nation. Given the nature of military and civilian networks, and the history of hacker warfare, the picture we have of this method of warfighting quickly becomes clearer: hacker warfare is not by itself a critically damaging means of waging war. Consider past domestic examples, such as the Sasser worm, Sobig email virus, or the Blaster worm. Regardless of how widespread or devastating the damage that resulted from these programs, hacker attacks on civilian networks in the United States have been shown to be incapable of causing severe long-term damage, or indeed, little more than severe annoyance. Computers can be rebuilt, data recovered. At best, hacker attacks against the United States from opposing nations can present distractions for the political leadership from their role in national security and alienate those members of the public that are uninvolved in the larger conflict. But instead of being used as a simple method of attack, the true value of hacker warfare would seem to be supplemental.

It is not difficult to imagine the inherent utility in being able to remotely disable an opponent's power or water supply, to disable or subvert their communications, steal important information, or generally render their information gathering systems useless, even for a short period of time. Although using hacker warfare to disable the power grid in a region may not directly affect an enemy military force, it can supplement a more traditional attack (in this case, disabling lights, communication, and causing general disarray), with the possibility of reducing friendly casualties. Similarly, disrupting or subverting enemy communications can yield similar beneficial effects for a military force.

We should not however, forget to concern ourselves with the civilian consequences of hacker warfare. Consider the previous example. Disabling power grids or communication systems in less-developed regions is certain to cause loss of civilian life, especially in those urban areas where hospitals, police, fire, and other rescue workers depend on those networks to safeguard a civilian populace. And these attacks raise similar defensive concerns. Should the United pursue offensive hacker warfare, it would need to secure itself against its own attacks prior to engaging in them, or else risk being attacked with its own means of warfare. And any tools that the United States produces to defend itself against its own hacker warfare would need to be publicly distributed, and as a result, could eventually be acquired and put to use by other nations (rendering them worthless as means of attack). In this way, defensive hacker warfare creates serious problems for its offensive counterpart.

Likewise, terrorist attacks against the United States can also benefit from this concept of hacker warfare as supplemental. Terrorist cells could use computer systems to disable or disrupt vital power or communication networks prior to or in conjunction with a more traditional attack, amplifying the devastation and effect of such an attack. And although such a scenario has yet to occur, it would be ridiculous to claim that the simple lack of imagination or historical action on the part of these organizations is a compelling reason to avoid expending resources in an attempt to more effectively secure certain critical civilian networks.

III. Solutions

Any solution to the ethical concerns regarding hacker warfare must address both issues of offensive and defensive information warfare, adhere to the principles of Jus in bello (proportionality of means, protection of noncombatants), and above all be practical. Given that intelligence-based warfare is incapable of causing casualties, and hacker warfare capable of doing harm to civilians only indirectly, most if not all cases of its use are going to satisfy both of our Jus in bello criteria, giving us more time to consider the practicality of their use and application.

When we consider whether or not hacker warfare should be waged at all, we must consider the alternative to doing so. That is, simply choosing to not pursue hacker warfare and strengthening security for networks only as needed, perhaps with the additional assurance of an international treaty calling for a widespread ban on hacker warfare. Such a ban would theoretically prevent certain nations from engaging in hacker warfare but more importantly would provide a means of punishing offenders.

Unfortunately, given the nature of hacker warfare such a treaty might not be enforceable. Due to the very nature of hacker warfare, it can be difficult to identify and locate the perpetrators of malicious attacks on systems (as once hackers have successfully infiltrated a system, they can frequently alter the records of their intrusion and remove any evidence of their tampering), much less prosecute them for their actions. As early as 1995, the Department of Defense estimated (successful attacks frequently go undetected) that it had been the target of about 250,000 hacker attacks on its systems. A 1999 study by the U.S. Government Accounting Office estimates that 120 countries or groups are involved in the development of information warfare systems. The difficulty of detection and tracking, coupled with the willingness of other nations (in particular, China, France,

and Israel), to pursue aggressive policies of hacker warfare, seem to indicate that such a treaty is not a practical solution.

So then what level of involvement should we pursue in hacker warfare? At present, the United States is already highly involved with the development of security software for its own systems and offensive intelligence based warfare against other nations or groups. While a minimal level of security on civilian systems is at best impractical and at worst impossible, it is not unreasonable to consider such safeguards on certain groups of civilian networks. In particular, we should consider this option for critical civilian networks (such as those that govern power, communications, and other utilities). Given both the importance and vulnerability of these networks, especially in the event of a traditional terrorist attack, it is in the best interests of the United States to ensure that the networks governing these utilities adhere to a minimal standard of computerized security.

Offensive hacker warfare requires deeper consideration. Given the aforementioned aggressive policies of other nations with regards to hacker warfare, it is obvious that the United States needs to maintain an aggressive policy with regard to hacker warfare as a means of gaining information (in other words, as a method of waging Intelligence-based warfare), or subverting enemy intelligence. On the other hand, as a supplemental tool to more traditional methods of warfare, we must enforce a policy that is less likely to cause civilian casualties.

As an alternative to bombing or other means of force, hacker warfare is not likely to cause many civilian casualties, and substantially less collateral damage, creating a strong case for its use, despite the depleted number of opposing combatant casualties it

could produce. Unfortunately however, the instances where hacker warfare is possible as a legitimate alternative to more traditional means of operation (for instance, using teams of hackers to disable power grids or communication lines to facilitate a military operation instead of bombing power or communication centers), are extremely limited. Given this, and the fact that civilian casualties from offensive hacker warfare are likely to be minimal, if any, the United States should set aside resources to more aggressively pursue offensive hacker warfare as both a means of intelligence-based warfare and a supplement to traditional methods.

Works Cited

1. O'Connell, Robert. *Of Arms and Men*. New York: Oxford University Press, 1989.

2. Dyer, Gwynne. *War*. New York: Crown Publishers, Inc., 1985

3. Johnson, James Turner. *Morality and Contemporary Warfare.* Yale University, 1999.

4. Leonhard, Robert R. *The Principles of War for the Information Age.* New York: Ballantine Books, 1998.

5. Iklé, Fred Charles. *Every War Must End.* New York: Columbia University Press, 1971.

6. Lorber, Azriel. *Misguided Weapons: Technological Failure and Surprise on the Battlefield.* Washington, D.C.: Brassey's, Inc., 2002.

7. Libicki, Martin C. 1995. "What is Information Warfare?" *Distributed document from the Center for Advanced Concepts and Technology.*

8. Various. "Frontline: Cyberwar!: Vulnerabilities: What are Al Qaeda's Capabilities?" PBS Frontline. 24 April, 2003 http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/vulnerable/alqaeda.html

9. IWS – The Information Warfare Site. Launched December 1999. http://www.iwar.org.uk/