Cyber Crime and Information Warfare- The New Arenas for WAR

Anwesha Pathak*
Rohit Sharma**

Abstract

With the advent, advancement and development of the Internet and particularly the World-Wide-Web has accelerated the perception in mankind for his dependency on information technology. As a consequence, various problems of national and international law and ethics have emerged which have increasingly been grabbing the attention of cyber experts, public policy makers and national security experts, especially those concerned about the future of warfare. A new form of warfare, "Information warfare", is defined to occur when one nation seeks to obtain strategic leverage over another by subverting, disrupting or damaging information systems. Compared to other forms of warfare, information warfare possesses several distinct features. The distinct features of information warfare and the legal/ ethical ramifications of these features are characterized in order to stimulate a deeper consideration of this new context.

The authors here will focus on the measures to prevent cyber crime, effects of these crimes on teenagers and more importantly Legal Issues Concerned with Information warfare & e-Crime.

Keywords: Chipping, Espionage, Information warfare, Offensive Software

Introduction

Military affairs which were previously based on wars with hardcore weapons such as long-range missiles, heavy machine guns, tanks, fighter planes etc. which took place at a large piece of land have now changed and have taken a very innovative way. Innovative here means a way through which these wars are now limited to a small room and a desktop with an internet connection which is able to devastate the security of the whole country. In other words, we can say that Information warfare is the latest innoment in the vast history of warfare. Information warfare may be defined as an attack on information systems of military advantage using tactics of destruction, denial, exploitation or deception or all. The spread of information warfare is connected from the rapid dispersion of information technology.

Flowchart-1, below shows us of how information was derived from Fischer (1984). It is to be noted that the cycle (flowchart) here has eleven different levels that shows the processing of data gathering to data entry to data reception to data processing and storing and so on. The last 2 stages here are related from data retrieval and thereafter the usage of this data.

Currently cyber experts all around the world are searching for tough protection in each stage of the flowchart, but there is a technical problem often termed as a 'cyber threat problem' that for every solution or for every protection a new kind of threat can be developed, sooner or later. The threat of Information warfare will continue to rise as the costs of beginning are too low and day by day these costs are cutting down due to which many of the foreign governments realized the need of a separate strategic information warfare branch under their military and other security based organizations. Few of the foreign nations have already got within them this facility. The system of information is so critical that one nation attacks other nation's information system, instead of attacking its military. The reason behind this is that the first option is cheap and cost effective as compared to the second option. Also it destroys and devastates the internal security issues of the latter country resulting in huge loss in economical matters.

Anwesha Pathak*
B.A. LL.B. 3rd Yr., New Law College
Rohit Sharma**
B.A. LL.B. 3rd Yr., New Law College

Legal and Ethical Challenges of information warfare

The following six sections analyze the most significant legal and ethical questions of information warfare as a new form of warfare. Many of the questions have been raised before in previous contexts but the unique characteristics of information warfare bring urgency to the search for new relevant answers.

It should be noted that this analysis is also pertinent to other military situations generally referred to as Operations Other Than War (OOTW) such as peace-keeping missions, preludes to conflict, alternatives to conflict, sanctions, and blockades. For example, in an information warfare analogy to the U.S. blockade of Cuba during the Cuban missile crisis, there are information warfare techniques (i.e. jamming and denial of service attacks) which could be used to block and thus isolate rogue nations from international communications without circumventing physical sovereignty much in the same way the British decided to sever all transatlantic telegraph cables that linked Germany to international communications at the outset of World War I.

The Sections are as follows:

1. What Constitutes an Act of War in the Information Age?

The nation-state combines the intangible idea of a people (nation) with the tangible construct of a political and economic entity (state). A state under international law possesses sovereignty which means that the state is the final arbiter of order within its physical geographical borders. Implicit to this construct is that a state is able to define and defend its physical geography. Internally a state uses dominant force to compel obedience to laws and externally a state interacts with other states, interaction either in friendly cooperation or competition or to deter and defeat threats. At the core view of any nation-state's view of war should be a National Information Policy which clearly delineates national security thresholds over which another nation-state must not cross. This National Information Policy must also include options which consider individuals or other non-state actors who might try to provoke international conflicts. Increasingly the traditional attributes of the nation-state are blurring as a result of information technology. With INFORMATION WARFARE, the state does not have a monopoly on dominant force nor can even the most powerful state reliably deter and defeat INFORMATION WARFARE attacks. Increasingly non-state actors are attacking across geographic boundaries eroding the concept of sovereignty based on physical geography. With the advent of the information age, the U.S. has lost the sanctuary that it has enjoyed for over 200 years. In the past, U.S. citizens and businesses could be protected by government control of our air, land, and sea geographical borders but now an INFORMATION WARFARE attack may be launched directly through (or around) these traditional geographical physical defenses.

War contemplates armed conflict between nation-states. Historically war has been a legal status that can be specified by declaration and/or occur by way of an attack accompanied by an intention to make war. The modern view of war provides a new look at just war tradition, "jus ad bellum", (when it is right to resort to armed force) and "jus in bello", (what is right to do when using force). The six requirements of "jus ad bellum" were developed by Thomas Aquinas in the 13th century:

(1) the resort to force must have a just cause

(2) it must be authorized by a competent authority

(3) it is expected to produce a preponderance of good over evil

(4) it must have a reasonable chance of success

(5) it must be a last resort

(6) the expected outcome must be peace

There are two requirements for "jus in bello"

(1) the use of force must be discriminate (it must distinguish the guilty from the innocent)

(2) the use of force must be proportional (it must distinguish necessary force from gratuitous force)

The application of just war reasoning to future information warfare conflicts is problematic but there is a growing voice that there is a place for the use of force under national authority in response to broader national security threats to the values and structures that define the international order. Looking at one aspect of the application of just war reasoning to information warfare, the problem of proportionality - It is impossible to respond to every information warfare action, there are too many. At what threshold in lives and money should the U.S. consider an information warfare attack an act of war. How many lives for a certain information warfare attack or what is the threshold in monetary terms or physical destruction.

Article 51 in the United Nations Charter encourages settlement of international disputes by peaceful means. However, nothing in the Charter "impairs the inherent right of individual or collective self-defence if an armed attack occurs..." Note that infringement of sovereign geographical boundaries by itself is not considered an "armed attack". Also note that experts do not equate "use of force" with an "armed attack". Thus certain kinds of data manipulation as a result of information warfare which are consistent with "use of force" would not constitute an "armed attack" under Article 51. Article 41 of the United Nations specifically states measures that are not considered to be an "armed attack":"Complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communications..." information warfare might still be considered an Act of War, however, if fatalities are involved. If data manipulation is such that the primary effects are indistinguishable from conventional kinetic weapons then information warfare may be considered an "armed attack". The paradigm shift is that weapons are devices designed to kill, injure, or disable people or to damage and destroy property and have not traditionally included electronic warfare devices.

2. What are the Legal and Ethical Implications of the Blurring Distinction between Acts of War from Acts of Espionage from Acts of Terrorism?

It is very important to be precise in what we identify as a crime and what we identify as an act of war. An "armed attack" as stated in Article 51 contemplates a traditional military attack using conventional weapons and does not include propaganda, information gathering, or economic sanctions. Espionage is a violation of domestic and not international law.

The threat analysis section of the 1997 Defence Science Board Report indicates that "a significant threat includes activities engaged on behalf of competitor states." This introduces the new concept of low-intensity conflict in the form of economic espionage between corporations. In the age of multinational corporations that view geographical boundaries and political nation-states as historical inconveniences - should economic warfare between multinational corporations involve the military?

The new information warfare technologies make it difficult to distinguish between espionage and war. If espionage is conducted by computer to probe a nation's databanks and military control systems when is it an act of war versus an act of espionage? Does it depend on whether the intelligence was passively read versus information actively destroyed and/or manipulated? Does it depend on whether the intelligence was used for military advantage or whether the intelligence was used for political or criminal advantage? Does the answer depend on whether a state of war exists or not?

A different scenario is modifying internal computer software (via viruses, trojan horse, or logic bomb) or hardware (chipping) before shipment to cause an enemy's computer to behave in a manner other than they would expect. If during peacetime, gaining entry to a computer's internal operating system could be considered a criminal offense or act of espionage despite the fact that the action in question took place before the enemy had acquired ownership of the computer. Is this prudent preparation for information warfare or is this a hostile action that could precipitate a war? If the computer hardware "chip" is commercially manufactured and altered, what are the legal and ethical ramifications of a company inserting internal hardware hooks in cooperation with a national security "request" from a government? Lastly, is information warfare a potential step which might lead to an escalated conventional military conflict which could have been avoided by other means?

3. Can information warfare be Considered Nonlethal?

Nonlethal weapons are defined as weapons whose intent is to nonlethal overwhelming an enemy's lethal force by destroying the aggressive capability of his weapons and temporarily neutralizing their soldiers. Nonlethal is most often referred to immediate casualty counts and not on later collateral effects. In response to the power of public opinion and instant global media coverage, the U.S. military has begun to develop a new kind of weaponry designed to minimize bloodshed by accomplishing objectives with the minimum use of lethality. This weaponry includes sticky foam cannons, sonic cannons, and electromagnetic weapons which temporarily paralyze an opponent without killing them.

Is it more ethical to use a sophisticated smart bomb precisely targeted to kill 10-20 soldiers immediately or is it more ethical to choose a nonlethal weapon which has the same tactical effect with no immediate casualty count but an indirect collateral effect of 100-200 civilian deaths?

The function of the target against which the weapon is used and the existence or lack of a state of war determines one legal framework for analysis. For instance, disabling the electronics of a fighter plane or air defence radar during wartime is the goal of a large investment in electronic warfare equipment by the U.S. and is considered fair and ethical. However, disabling the electronics of a civilian airliner or air traffic control during either peacetime or wartime violates the principles of discrimination of combatants and proportionality of response and is considered unethical and an illegal act against humanity.

4. Is it Ethical to Set Expectations for a "Bloodless War" Based on information warfare?

As nonlethal weaponry of all types (especially information warfare weapons) advance from novelty to norm, however, many potential pitfalls will need to be faced. The most important of these is the expectation that such weapons will ultimately allow wars to be fought without casualties. Nonlethal military capabilities are not new although information warfare weapons are the newest weapons in the nonlethal arsenal. Military forces have used riot-control chemical agents, defoliants, rubber bullets, and electric stun weapons for decades. As U.S. military forces are involved in missions that require extended direct contact with civilians (e.g. Somalia, Bosnia), force can no longer be viewed as either on or off but rather as a continuum with nonlethal weapons on one end and nuclear devices on the other end. In more traditional conventional warfare, information warfare attacks to disrupt, deny and destroy C4I capabilities

(Command, Control, Communication, and Computer Intelligence) are a core part of military tactics and strategy.

If information warfare weapons can be used to remotely blind an opponent to incoming aircraft, disrupt logistics support, and destroy or exploit an adversary's communications then many of the problems associated with the use of ground forces for these missions can be avoided. It is important to point out that although nonlethal weapons are not meant to be fatal, they can still kill if used improperly or against people particularly sensitive to their effects. Because these technologies are potentially lethal in these circumstances, the term "nonlethal" has not been universally accepted within the U.S. military. For example, the U.S. Marines Corps uses the term "less lethal" to imply that there is no guarantee of non-lethality.

Asserting that information warfare will ultimately allow future wars to be fought without casualties is a widespread misconception likely to prove counterproductive and even potentially dangerous. First, all nonlethal weapons are not equally applicable to all military missions. Second, overselling of nonlethal capabilities without providing a context can lead to operational failures, deaths, and policy failure. Third, unrealistic expectations about nonlethal weapon capabilities inhibit their adoption by military forces who need to build confidence in these weapons.

There is a large asymmetry in global military power when comparing the U.S. versus other nation-states. In 1994, the U.S. DoD (Dept. of Defense) budget exceeded that of Russia, China, Japan, France and Great Britain combined. This asymmetry makes it unlikely another nation-state would challenge the U.S. in a direct high-technology conventional war except for circumstances which we should not depend upon (e.g. incredible miscalculations and/or ignorant dictators which were both present in the Gulf War). Despite the luxury of a bumbling opponent, the success of the Gulf War has lead the U.S. citizenry to expectations of low casualties in all future conflicts. These expectations go against two cardinal rules of military strategy;

(1) you do not plan to refight the last war and

(2) the future battlefields cannot not be dictated by the United States.

The next battlefield for which the U.S. DoD is preparing is a global battlefield with weapons of information warfare "targeting" civilian infrastructure. Even in this scenario, military and civilian casualties will be likely from either primary or secondary effects from information warfare attacks.

5. Is it Legally and Ethically Correct to Respond to information warfare Tactics with the same Tactics?

If the U.S. is attacked by information warfare weapons, how should the U.S. Government respond?

By changing perspectives from defence to offense, what is in the U.S. arsenal to wage information warfare against an adversary:

A. Offensive Software (viruses, worms, Trojan horses)

B. Sniffing" Or "Wiretapping" Software (enabling the capture of an adversary's communications)

C. "Chipping" (malicious software embedded in systems by the manufacturer)

D. Directed Energy Weapons (designed to destroy electronics & not humans/buildings)

E. Psychological Operations (sophisticated and covert propaganda techniques)

A strategy that uses these weapons in various combinations has the potential to replace conventional military force. The questions remains: is it legally and ethically correct for the U.S. to defend its security interests by resorting to the same information warfare tactics that are being used against it? Should information attacks be punished by information counterattacks? The options include maintaining our superpower status at all costs; covertly listening to our adversaries but not actively disrupting operations; or contracting mercenaries in no way officially affiliated with the U.S. government to do our dirty work. Cracking computers to deter and punish computer cracking erodes any moral basis the U.S. has for declaring the evils of information warfare. It is also harder to predict secondary effects due to the globalization of systems. Retaliation may produce effects ranging from nothing to being counterproductive through destruction of U.S. interests. A nation-state or non-state actor that sponsors an attack on the U.S. might lack an NII (National Information Infrastructure) of their own for the U.S. to attack in punishment and thus not be intimidated by a U.S. information warfare deterrence strategy.

The problem is that there are no characterized rules of engagement for information warfare conflicts which can take forms of isolated operations, acts of retribution, or undeclared wars.

The most serious problem for using information warfare retaliation to counter information warfare attacks is that adversaries could counter and/or copy information warfare capabilities. Every breakthrough in offensive technology eventually inspires a matching advance in defensive technology so forth thus escalating an information warfare weapons race. A last issue related to retaliation is the dilemma faced by the intermingling of the military and civilian sides of society. Given the uncertainty of deterrence and identifying the enemy, which strategy is appropriate for retaliation; (a) a strategy that attempts to separate the military from civilians and in so doing has a diminished impact which potentially prolongs the duration of the conflict; or (b) a strategy that attempts to minimize lethality and duration but deliberately targets civilian systems?

6. Can Protection from information warfare Take Place in the United States Given Our Democratic Rights?

How much government control of the U.S. NII is feasible in a free society?

Most of the information warfare technology is software which is easy to replicate, hard to restrict, and dual-use by nature (uses for both civilian and military). In the 1997 Defence Science Board report, it states that the DoD is "confused" about when a court order is required to monitor domestic communications. This raises basic questions about the constitutional and ethical balance between privacy and national security in a new information warfare context.

A "Big Brother" approach that places all of a nation's telecommunications under a single government jurisdiction is improbable given the diffusion and complexity of technology and the shrinking size of government. Most systems were built to serve commercial users who will vehemently object to unfunded mandates (i.e. taxes) and new requirements not driven by business demand (e.g. CLIPPER chip encryption and key escrow accounts). Regardless, it is critical to the future security of the U.S. that we find a way to protect our infrastructure from information warfare attack and have contingency plans for potential information warfare crises. If the information warfare attack is detected and the enemy identified but the U.S. is unable to react promptly due to bureaucratic inefficiency or indifference from private industry, it may be too late to react at all.

Current political discussion has floated tax incentives and direct subsidies to promote industry cooperation. In a related matter that may provide a precedent, the government has pledged to provide telephone companies with at least $500 million to ensure that FBI officials can access telephone conversations over digital circuits (as opposed to accessing telephone conversations over analogue circuits which is technically much easier).

Conclusion

To be sure, cyberspace is hardly the first or the only policy domain which lies beyond the control of any single nation state. International air traffic, the law of the sea, funds transfers, and such environmental considerations as ozone depletion and global warming, among others, have required concerted international efforts. One would expect that the development of international arrangements in response to telecommunications-related crime will occur in a manner not unlike those which have accompanied other extraterritorial issues, from drug trafficking, to nuclear testing to whaling. Whether the realm of telecommunications will be able to achieve a better record of success than these other enduring global issues remains to be seen

References

1. Department of Homeland Security, A Comparison of Cyber Security Standards Developed by the Oil and Gas Segment. (November 5, 2004) Guttman, M., Swanson, M., National Institute of Standards and Technology; Technology Administration; U.S. Department of Commerce.,
2. Generally Accepted Principles and Practices for Securing Information Technology Systems (800-14). (September 1996) National Institute of Standards and Technology; Technology Administration; U.S. Department of Commerce.,
3. An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12. Swanson, M., National Institute of Standards and Technology; Technology Administration; U.S. Department of Commerce., Security Self-Assessment Guide for Information Technology Systems (800-26).
4. The North American Electric Reliability Council (NERC). http://www.nerc.com. Retrieved November 12, 2005.
5. isasecure.org site
6. ISO webpage
7. NERC Standards (see CIP 002-009)
8. NIST webpage
9. Ssrn.com
10. Westlaw.co.in
11. Google.com