

Ethical Issues of Cyberwarfare

by Randall R. Dipert
Department of Philosophy/
National Center for Ontological Research (NCOR)
University at Buffalo
Buffalo NY 14260
rdipert@buffalo.edu

- I. Introduction
- II. Cyberwarfare and the Morality of Going to War (*Jus ad bellum*)
- III. The Varieties of Cyberharm and Cyberattack
- IV. Special attributes of Cyberwarfare and Proposed *Jus ad cyber-bellum* Criteria
- V. Cyberharm and International Law
- VI. Tolerable Peaceful Levels of Cyberwarfare: Rules for Cyber Cold War
- VII. Conclusion

I. Introduction

U.S. Secretary of Defense Robert Gates has recently announced the founding of a U.S. Cyber[Space] Command, USCYBERCOM. It would be headed by a professional military general officer, and subordinate to the U.S. Strategic Command.¹ Defensive cyberoperations (NetOps) now fall under the Joint Functional Component Command for Network Warfare (JFCC-NW); I surmise that *de facto* they are scattered around the separate military services, DoD agencies, and other Federal agencies. Since 2005, command of offensive cyberoperations rests with the Director of the NSA. I assume that as a matter of policy, and *de facto*, decisions are made there about all offensive cyberoperations against other nations, multinational corporations, and international political organizations, as well as the development of policy.

These developments would come as no surprise to anyone who has been following the news in the last two years, of cyberattacks on components of U.S. defense cyber-infrastructure, and the probable strategic, military cyberattacks by Russia on Georgia, and by China, North Korea, and possibly Iranian attacks on U.S. defense and economic targets. A centralized command is a natural next step after separate efforts within the NSA, the U.S. Air Force, and the Army, among the more publicized efforts.

¹ WSJ Dec 21, 2009 “[T]he Pentagon's new Cyber Command has gotten off the ground slower than expected because of congressional uncertainty about its scope and mission. ¶The Pentagon had said the entity -- designed to gather all the military's cyber defense and cyber offense programs under a single rubric -- would be operational by October. ¶Nearly three months later, the command doesn't yet have a chief. Lt. Gen. Keith Alexander, the current head of the National Security Agency, has been tapped to run the command, but his nomination has been held up on Capitol Hill. ¶It may be months before the general receives his confirmation hearing.” Howard Schmidt was chosen in December, 2009 to be the Cybersecurity Coordinator for the entire federal government, working under the National Security Advisor to President Obama. *Washington Post* Dec 22, 2009. Although it is unclear, I assume that Schmidt will mainly coordinate *defensive* cybersecurity.

While responding to cyberharm of all sorts, including by apolitical and anarchic hackers, as well as economically motivated industrial cyberespionage, have been a subject of discussion for decades, what is new is the acknowledgement of actual or possible strategic attacks that have been coordinated by the central commands of governments (or other political organizations) and that are perpetrated on the websites, internet infrastructure, and software of other governments. What is still more recent is the open discussion of a need for an organized capacity for *offensive* cyberattack on hostile nations and political organizations.

In this paper, I will discuss the different forms this cyberharm may take, and will characterize those that count as strategic or military *cyberattacks*. I will then frame the central ethical questions that such cyberattacks and cyberwarfare might precipitate. Lastly I will set about addressing these questions using concepts from Just War theory and various existing philosophies of the morality of war, mainly by analogical reasoning from more familiar ethical situations. I will also discuss what may be some unique characteristics of cyberwarfare.

II. Cyberwarfare and the Morality of Going to War (*Jus ad bellum*)

While there is coming to be an extensive literature on various technical aspects of cyberattacks, including by state on other states, and the slow formation of military and governmental agencies for defensive—and one may guess, offensive—cyberwarfare, there is little or no literature (of which I know) coming from the now fairly numerous students of the morality of war. Likewise, there is nothing in the unclassified domain that constitutes a doctrine or strategy.² While the idea of putting unruly hackers into uniforms may seem odd, there is a good sense in which the categorization of these state-on-state cyberoperations as “military” is correct: they are organized, largescale efforts by one nation to develop the capacity to harm another nation, and defend against harm, and some of these efforts—in the U.S. and in China, where cyberoperations are organized in regiments and battalions—are located within existing military commands.

As Michael Walzer notes at the beginning of *Just and Unjust Wars*, the key necessary condition of morally permissible war is rather blandly and uniformly described as *aggression* by an enemy. This is also the only stated condition in the U.N. Charter under which a nation may justifiably defend itself before the Security Council takes action. (Chapter VII, Article 51: self-defense against an “armed attack”). The paradigm form of aggression in the case of symmetric or regular war is the invasion of sovereign territory by armed, centrally commanded, enemy soldiers of another sovereign state that are prepared to use deadly force.

This view is retained by most writers who roughly follow the just war tradition, such as Nick Fotion in *War & Ethics: A New Just War Theory*.³ Namely, attacks are either

² This repeats the observation of LTG Keith Alexander [Director of the NSA and nominated as commander of CyberCommand, “Warfighting in Cyberspace,” *Joint Forces Quarterly* July 31, 2007. Alexander discusses the possibility of extracting doctrine from developed doctrines in Electronic Warfare (EW) and Information Operations IO), such as those stated in JP [Joint Services Publication] 3-13.

³ At least for regular Just War Theory (JWT-R) applied to traditional state-on-state warfare. The language of “attack” may be broad and vague enough to include non-paradigm cases of aggression I am about to discuss, although Fotion gives only examples of violent, armed invasions.

invasions or physical destruction within a nation's territory. Yet "customary" and accepted just causes of war have included a wider array of phenomena that are broadly categorized as *casus belli*: embargos, systematic attacks on and harassment of citizens and businesses abroad, blockades, blocking of necessary supply lines such as a pipeline, attacks on military or civilian ships in international waters, and so on. A cyberattack by one nation on another is more like one of these.⁴ Although it was clearly used as a pretext for largescale war, the obstruction of the movements of goods and people between East Prussia and the main body of German in the 1930's (the Danzig Corridor) could reasonably have led to justified acts of war. Likewise the isolation of Berlin from the West by land routes (the Berlin Blockade) could have led to a justified war if the airlift had not been successful. In diplomatic language, and as a warning that these actions might risk war, such events are broadly conceived as intentional damage to *vital* interests of a state. Most discussions of *jus ad bellum* have taken scant notice of them.⁵

Attacks on another nation that kill or destroy buildings or other artifacts, but that do not include invasion by enemy soldiers, cover a broad range of activity, from small arms fire and artillery fired across a border, to the use of mortars and rockets. Cruise missile attacks and for that matter attacks by unmanned aircraft likewise would seem to count as aggression that would, in certain circumstances, provide just cause for a wider counterattack. Even these actions still are traditional in the sense that they involve macro-physical objects that are intentionally directed to intrude into the airspace of another nation and cause physical destruction.

An unprovoked cyberattack by one nation on the civilian or military infrastructure of another nation is not very much like these more traditional forms of aggression or attack. A cyberattack does not involve intrusions into the territory or airspace by soldiers or even by physical objects. A better analogy would be that a cyberattack is more like Electronic Warfare (EW), such as jamming the radio communications of another nation from outside its borders or the intentional use of electromagnetic radiation, such as a laser, or an electromagnetic pulse (EMP) weapon to destroy or hinder the functioning of human beings, machinery, or infrastructure from beyond a nation's borders. (There is a nominal sense in which the photons "invade" the ether of another nation, but that in itself seems harmless; radio waves constantly pass through nations' airspace without complaint. In the case of EMP weapons, it is not the electromagnetic radiation, the photons themselves, that violate a nation's sovereignty and cause the ethical problem; it is the secondary production of magnetic fluctuations, and then induced electrical current, that is the problem.)

Neither real historical examples nor Just War Theory gives us much direct help in thinking about such matters. Yet we could indeed imagine a cyberattack that caused as much or more damage to a nation's infrastructure and institutions as would more conventional attacks by bombs or artillery. The further physical damage could have been intentional or not, and foreseeable or not. We could even imagine a disruption caused by a cyberattack killing large numbers of human beings—by damaging or maliciously

⁴ See Martin Libicki, *Cyberdeterrence and Cyberwar* (Rand Project Air Force, Rand Corporation, 2009) Appendix I (What Constitutes an Act of War in Cyberspace) pp. 179f. Libicki notes that NATO explicitly rejected Russia's cyberattack on Estonia as an act of war that would trigger the mutual defense obligations.

⁵ A interesting exception is Walzer himself, who in the preface to the 4th edition, calls them "soft" force and threat of force, or "force short-of-war."

“invading” the software of a large nuclear reactor, medical information systems, or airplanes, for example.

The hard moral questions about cyberattacks and cyberwarfare are these:

1. In what circumstances would a cyberattack provide reasonable “just cause” for a counterattack, including by more usual forms of invasive physical attack?
2. What is it about some intentional actions, including cyberattacks, such that they would count as sufficient attacks or aggression to serve as a morally justified *casus belli*?
3. In peacetime, to what extent may a government or military intentionally damage the functioning of a hostile nation’s civilian or military informatics infrastructure without triggering the conditions for a reasonable *casus belli* against it by its target nation? That is, what is a morally permissible level of offensive cyberattacks in peacetime?

III. The Varieties of Cyberharm and Cyberattack

The broadest useful notion in the discussion of cyber-ethics is *intentional cyber-harm*: this is intentional harm caused by an agent, *via* an informatics network such as the internet, in which the functioning of a system (a person, a machine, software or an economy) is in some way impaired or degraded. An attack is intentional cyber-harm to a specific system. A virus playfully set free on the internet by mischievous hackers is not in this sense an attack, although it might do harm. An attack is intentionally causing harm to a specific organization, system, etc. A less frequent further target of a cyberattack might be an artifact, such as vehicle (say, by disabling it through corrupting the OnStar system), or a person (by disabling their pacemaker, and so on). The vehicle or person would be the indirect target of a cyberattack, since by its nature the direct attack is specifically on the functioning of software, etc., and it is the malfunctioning of these systems that causes the intended harm to a person, organism, or artifact.⁶

It is important first to separate three ways in which the internet and software could be utilized to harm a country or military. I will focus on harm brought about through the internet, although similar intentional harm could be affected by the physical distribution of faulty software or even hardware (e.g., in the ROM of computers sold in the target country). (1) Information, in the form of websites or other files, may be destroyed, defaced or altered, (2) Software may be hacked into and damaged or altered, via the internet, (3) Malware may be distributed in a target country that is deliberately defective or remotely controllable: (a) to cease functioning on command, (b) as instruments of espionage, such as recording and later transmitting keystrokes, or (c) used to damage still other software and hardware, (4) the functioning of the internet (or an intranet) in the target country can be impaired (such as by denial-of-service attacks), and (5) information intended to be secret, can be obtained through unauthorized access to software or databases. Naturally, any of these activities can be performed by isolated individuals with no political motive (nuisance or anarchic hackers).

I focus on cyberattacks (intentional cyberharm) that is instigated or controlled by political organizations (or their military services) on other political organizations or

⁶ These notions of organization, person, artifact and organism have precise, and carefully interrelated, definitions in work in formal ontology for the military that my research group, NCOR, and others are developing—including a nascent ontology for all data interchange in the federal government (UCORE-2).

military services.⁷ These are international cyberattacks. If the attacks between political entities are sufficiently “widespread” we might then speak of a cyberwar. This modifies the useful definition of Brian Orend of or ‘war’ as “*actual, intentional and widespread armed conflict between political communities.*” (I would further stipulate that war in its usual sense involves the intentional use of deadly force on human beings.) A cyberwar might then not literally be a war in this stricter sense, unless death or severe injury of human beings was the further intended result.

So far as I can see, there are no serious concerns that restrict what a nation may morally take as strictly *defensive* measures to prevent nuisance harm, or to block cyberattacks. However, defensive cybersecurity efforts could violate the privacy or other civil rights of innocent party, or incidentally cause damage to one’s own economic or computer community. Defensive actions against cyberattacks could include blocking a system’s or nation’s internet from certain foreign or hostile IP addresses and the physical severing of all information conduits (satellite, cable, radio, and so on), when this is possible. As for (5) cyber-espionage, there seems to be for now the general understanding that the only possible moral countermeasures are cyber-defenses (cyber-counter-espionage), including retaliatory cyber-espionage. This toleration may change as cyber-espionage, and threats and harm become more serious, and might in the future include diplomatic, economic, and cyber-retaliation.⁸

Since much will later turn on the nature and quantity of cyberharm, it would be useful to sketch the forms cyberharm may take. (1) One of the most common cyberattacks is Denial of Service, Distributed Denial of Service (DoD, DDoS). This technique relies on flooding an IP address or network with messages, effectively blocking the information packets of legitimate users. Since every internet message packet contains a source IP address and a target IP address, a simple countermeasure is to filter out all packets coming from certain IP addresses. The cyberattacker can defeat this simple countermeasure by “spoofing” and constantly varying the pretended source IP address. Another technique is to plant malware (a *botnet*)—that may be activated by a date or external command from a *bot-master*-- in a very large number of unwitting computers that, once initiated, send information packets from their various and correct IP addresses (or combining the distributed attack with IP address spoofing) to a single target IP address. Most of these techniques can be defeated by requiring a confirming dialogue between the source and target (“handshaking”), although the activity of filtering packets with suspicious IP addresses, and the initiation of confirming dialogues, may itself overwhelm the computational power of the target computer. Sites such as Google or sites within the U.S. Department of Defense probably have the computational power to keep

⁷ The usual cases are of states (including nations) that have sovereignty over a territory. I use the locution “political organization” to include insurgent and rebel groups with political goals, as well as political organizations that are not localized to a territory (such as international terrorist organizations). Compare Libicki’s op. cit. rather vague definition: “*cyberattack*, for the purposes of this discussion, is the deliberate disruption or corruption by one state of a system of interest to another state.” p. 23.

⁸ As Libicki, op. cit. xvi and ppp. 41f, notes, the threat of cyber-retaliation is less likely to deter than with nuclear weapons, since in the Cold War there would have been no epistemic problem of determining who launched a nuclear attack. In cyberattacks, identification of the attacker may not be immediately evident, and might be problematic ever to determine the attacker and the attackers’ exact affiliation with a state. However, with the possibility of low-level nuclear attacks by non-state organizations or proxy non-state actors, the epistemic parallel becomes much closer.

up with a huge number of such attacks in real time (for now). A smaller business website operating on a single server might not.⁹

Another way of categorizing harm uses a (much debated) distinction in computer science, between *data* that an algorithm operates on, and the *algorithm*, a computer or network might be running. (5.a) *Theft* of data occurs when an unauthorized user gains access to private data—such as schematics of nuclear weapon design or social security numbers, which can then be used to harm the interests of the data’s rightful owner. Government-on-government computer espionage falls into this category. These are sometimes casually described as “attacks”;¹⁰ because they are usually unsuccessful and do no harm, a better word would be that they are hostile probes of weakness. I will not consider such espionage a cyberattack, although the further use of information gained to commit cyberharm would be.¹¹ Successful attacks would require getting past IP-address confirmation exchanges, password protection, and encryption of the data (if any). Countermeasures would include adding further layers of security or, in the worst case, making the data inaccessible altogether from the internet. (2.b) *Corruption* of data is perhaps a worse problem, since the changes to the data might be subtle: imagine corruption of a list of the GPS coordinates of all of a hostile nation’s fixed ICBM sites, or changing bank account data so that it skims pennies from a large number of bank accounts.

Another form of cyberharm involves changing the programs—the algorithms—of a target computer system (or the algorithm of an application program, such as a spreadsheet or inference engine). This may involve appearing to make updates to software (most seriously in the Operating System), but which in fact causes the software to cease to function, or function in a way unintended by the regular users. This is the realm of the more usual computer viruses. Notice that the effect of changing a program may be to allow easier access to data, which is then stolen or corrupted and then falls into (2.a).

IV. Special attributes of Cyberwarfare and Proposed *Jus ad cyber-bellum* Criteria

What I earlier called the “hard [moral] questions” about cyberwarfare can be answered through analogical reasoning, comparing cyberwarfare with morally similar cases about which we have clearer thinking, and by looking to the ethical foundation that grounds what is wrong with one nation harming another nation in any way. My proposal for the

⁹ Libicki, op. cit., xiv note 1 considers these “minor nuisance[s] to organizations” in a way that excessively minimizes their economic and organizational damage. Day-to-day defense operations, and even emergency responses, of the U.S. military are probably more dependent on internet access and email than we could guess.

¹⁰ “New Cyber Chief Faces Dynamic Challenges” by Nicholas Zifcak in *Epoch Times* (Dec 24 2009) “According to the 2009 Annual Report to Congress of the U.S.-China Economic and Security Review Commission, in 2008 the number of reported cyber attacks against the Department of Defense was 54,640. In 2009, from Jan. 1 to June 30, the number was 43,785.”

¹¹ This agrees with Libicki, op.cit., who lumps espionage into a category of mere “computer network exploitation.” He considers at length whether a cyberattack might be launched as retaliation for espionage (pp. 102f) and his answers is, for a variety of interesting reasons, no.

morally necessary conditions such that nation B may counter-attack nation C with a cyber- or conventional attack, after a cyberattack by C are:¹²

- (1) The attack of C on B was unjust and substantial,
- (2) The source of the attack by C was, with overwhelming likelihood, ordered or permitted at the highest levels of a government,
- (3) Reasonable measures had been taken by nation B to defeat or minimize the cyberharm that a hostile nation or other non-state cyberattacker (black or gray hat hackers) might cause,
- (4) The expected damage to the enemy (C) is likely to be commensurate to the damage (B) has suffered, or is the minimum necessary to stop continuing cyberattacks,

Comments:

On (1): if the damage intentionally inflicted on B is primarily to its offensive capability, then this is for ethical purposes insubstantial damage. If damage is to defensive capability or civilian infrastructure then damage is to be measured by the amount of increased vulnerability (in the case of harm to defensive installations, such as radar systems) or damage to the civilian population in which measurement takes place in this order: human lives, human well-being, material infrastructure. Thus a cyberattack on the FAA flight data systems that foreseeably resulted in the crash of several airliners and deaths of hundreds of people, would probably exceed the threshold necessary to launch a conventional attack. Likewise, a massive cyberattack on defenses a nation has against physical attack (such as radar, spy satellites, command and control systems), would risk giving the attacked nation reason to believe that a conventional attack was imminent, and thus possibly trigger the conditions of justified preemptive war.¹³ It is often difficult sharply to distinguish defensive from offensive—such as in command and control systems, including communication.

On (2): in conventional warfare, the identity of the attacker is not usually problematic. In cyberwarfare, identifying the attacker *is* especially problematic—due to problems of identification of IP addresses and the presence of diverse non-state agents with similar capabilities (especially clever black hat hackers or groups of them). When information technology is concentrated or carefully controlled by a government, as it is in, say North Korea, then if the IP nationality can be determined with great likelihood, the source is very likely to be the government itself. Likewise the presence of a large, indigenous community of black-hat hackers may give a nation's capacity for offensive military cyberattacks some sort of smokescreen. The enemy cannot determine if the source is governmental or military, or corporate or simply mischievous and anarchic.

On (3): this is an unusual condition, without clear analogy in the case of conventional warfare. We would not normally consider, for moral assessment, whether the attacked nation (B) had built enough bomb shelters or had failed to develop countermeasures to rocket or mortar attacks. Some condition like this nevertheless seems required in the case of cyberwarfare because civilians are in possession of the tools that are as destructive as what nations can organize, namely computer programming skills

¹² Additional conditions would undoubtedly be needed, but they would be shared with whatever criteria one has for morally justified non-cyber wars.

¹³ In the technical sense of an attack being imminent and highly likely.

and internet access, and because one can expect occasional attacks or mischief from them. Civilians do not have tanks.

On (4): we have not yet witnessed (so far as I am aware) a case where sufficient damage was done in order to justify a largescale conventional attack. It would likely take a large number of deaths or the irreversable crippling of an economy or vital economic sector. Although I hesitate to give terrorists a roadmap to the happy world of cyberterror, such an attack might be on the control systems of airliners, of nuclear power plants, or of highly automated weapons, damaging large medical information networks, infecting large numbers of individual computer systems that control cars, medical instruments, and so on. Even then, the likelihood of stopping such a destructive cyberattack may be small, since the source might not physically located in a small number of sites. Although this is more a matter of the general theory of the justification of wars, I believe that narrowly requiring “Likelihood of Success” is game-theoretically mistaken: the goals may be the modification of this and other enemies’ behavior in the future, through punishment and deterrence.¹⁴

V. Cyberharm and International Law

The internet, either as it is now, or as it might shortly become if internet commerce and internet industrial communication continues to grow, could perhaps best be likened to an element of the civilian infrastructure, such as the power grid, electronic communication, or even a country’s water and sewer systems. They are all equally networks whose functioning can be disrupted.¹⁵ In the past, this disruption was accomplished by destroying physical objects, specifically artifacts and artifactual structures such as generators, transformer stations, communication nodes, and so on. It is virtually no stretch of the imagination to speculate about disrupting these networks by cyberattacks on their software.

If we imagine that a real war has begun, the only traditionally permissible attacks that damage civilian infrastructure are those whose purpose is to impair military operations, or directly connected warmaking capacity, and which are militarily necessary to pursue the just goals of a war. This is usually taken to include key components of the electrical grid, for example if these are necessary to support the enemy’s military communication and command and control. It may also include components of the transportation infrastructure, such as roads and bridges, airports, and so on, if these have likely military value. Rather than the traditional doctrine of military necessity, I would prefer to stipulate that the military value of the destruction must exceed, or be proportional to, the everyday civilian use of this infrastructure.

¹⁴ Such wider goals, and what counts as “success,” are discussed in the works of Thomas Schelling and others in game theory.

¹⁵ The fact that these networks’ functioning is interrupted or harmed, as opposed to the destruction of wires and transformers, is ontologically non-trivial. In the olden days, we destroyed wires or jammed radio frequencies in order to disrupt communication; equivalent or worse impairment of functioning might now be accomplished by cyberattacks.

The likely effects of damage to civilian infrastructure with regard to health is especially important, so that in addition to sites such as civilian or military hospitals, which have long been explicitly addressed by international law, this moral principle would seem also to protect water supplies. Indeed, in Protocol I (1977) to the Geneva Convention, civilian water supply is explicitly protected.¹⁶ The U.S., in the First Gulf War, and possibly in the Second (OIF), has been accused of intentionally damaging sections of the largely civilian water supply system of Iraq; the matter is complicated however, since joint military and civilian use is not carefully addressed by the statute and the overall intent of the statute seems to be to prohibit such damage that is used to drive a population out of an area or destruction of objects that are “indispensable to [human, civilian] survival” rather than merely conducive to good health.

The extensive Protocol I to the Geneva Convention that covers this general type of damage, seems to be flawed in a way that one can almost say is ontological, and thus renders it fundamentally inapplicable to cyberwarfare and certain software- or data-forms of damage to civilian infrastructure. Namely, Chapter III (Articles 52-56) is concerned with what are there called “civilian objects.” These are limited, in language and by examples, to material entities such as cultural and religious objects (Art. 53), the environment (Art. 55), the just discussed category (Art. 54) of “objects indispensable to the survival of the civilian population,” and to “[public] works and installations containing dangerous forces” (Art. 56), such as nuclear (radiation) and dikes and dams facilities (flood).

As an introduction to the Chapter there is a general ban on a residual class of non-military objects that are called “civilian objects.” There are several limitations of this treaty that render it of little application to cyberwarfare, and indeed, to economic warfare. One is that it discusses only (material) *objects*, and not the *functioning* of these objects. This failure is ontological insofar as severe damage to software, data, operating and control systems, does not require the damage or destruction of objects in the usual sense. There are other flaws as well. First, there is an emphasis on prohibiting damage to these entities as military objectives, that is, of intentional attack; this leaves open a wide category of possibly severe incidental damage. Second, the key concept of “civilian object” is defined very narrowly as those objects that do not “make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.”

¹⁶ Protocol I (1977) to the Geneva Convention “Art 54. Protection of objects indispensable to the survival of the civilian population ¶1. Starvation of civilians as a method of warfare is prohibited. ¶2. It is prohibited to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population, such as food-stuffs, agricultural areas for the production of food-stuffs, crops, livestock, drinking water installations and supplies and irrigation works, for the specific purpose of denying them for their sustenance value to the civilian population or to the adverse Party, whatever the motive, whether in order to starve out civilians, to cause them to move away, or for any other motive. ¶3. The prohibitions in paragraph 2 shall not apply to such of the objects covered by it as are used by an adverse Party: (a) as sustenance solely for the members of its armed forces; or (b) if not as sustenance, then in direct support of military action, provided, however, that in no event shall actions against these objects be taken which may be expected to leave the civilian population with such inadequate food or water as to cause its starvation or force its movement.”

VI. Tolerable Peaceful Levels of Cyberwarfare: Rules for Cyber-Cold War

It now appears that there were concrete proposals for a cyberattack on Iraq in 2003, before the physical attack commenced.¹⁷ However a more likely scenario for the future is that there will be cyberwarfare “skirmishing” among the major players, perhaps lasting decades. These would take the form of aggressive internet probing of military and industrial secrets, and perhaps numerous Denial-of-service attacks, and corruption of data and software, especially if the origins of the attack can be somewhat disguised (China, the U.S.) or if the government is not sensitive to world opinion (N. Korea). Any weakening of industrial or military power of other nations through cyberattacks would likely enhance a nation’s own geopolitical power

In short, what we are likely to see in the next years, perhaps decades, is something like the Cold War between the West and the Soviet Union. The espionage “cat and mouse games” of the Cold War are well known, and there was also extensive probing of each other’s territorial defenses, by the incursion of small numbers of air, sea, and ground forces, never giving sufficient to trigger reason the believe that a largescale attack was imminent. What we are likely to see is the informal development of similar “equilibrium” in the accepted quantity and seriousness of the cyberattacks.

It is relatively clear what the reasonable (and thus moral) constraints on a Cyber Cold War would be. There should be no, or only minor, targeting of strictly defensive computer control systems. There should be no attacks that disable or panic global financial or economic systems. There should be no interference in the vital economic and security interests of a major power, especially one with the power to attack with conventional physical force.¹⁸

Obviously the most desirable ethical principle would be not ever to harm, through cyberattacks, the interests of other peoples and government. Since it is likely that many global players (industrial and governmental) would not abide by such a principle, then the “containment” of harm would seem to urge the development of defensive and even offensive cyberwarfare capacity by any nation whose information infrastructure is large and sensitive to harm. The offensive capacity is necessary in case defensive cybersecurity efforts are not sufficiently successful, and retaliatory cyberattacks are necessary to achieve some equilibrium.

There are some marked dissimilarities with the Cold War, however. First, a Cyber Cold War would be multilateral rather than bilateral: it would involve many nations, with different interests and not allied by treaty. Furthermore, the parties would include major non-governmental players such as private companies or even individual or groups of individual hackers, perhaps with political interests. It is unlikely, in the more capitalistic

¹⁷ NYT August 1, 2009. Namely, by corrupting data in the international financial informatics network, thus depriving the Iraqi government of internationally deposited funding, as well as crippling Iraq’s own more primitive computer banking system. The plan was not implemented for fear of diverse side-effects—such as a massive loss of confidence in the security of the international banking system: “John Arquilla, a military strategy expert, said, ‘Cyberwarriors are held back by extremely restrictive rules of engagement.’” A possible result of such a corruption of bank account data might have been a worldwide panic of the sort that occurred in fall, 2008.

¹⁸ See Libicki, *op. cit.* p. 181, a chart “Ranking Various Forms of Harm in Cyberspace.” The top most harmful categories include casualties and still more harm, “Interfere with Nuclear Systems” and “Affect Military Operations.” This is far too unspecific, since disrupting a training operation, even seriously, is not on a par with blinding radar or rendering defensive electronic systems inoperative.

and constitutionally free countries, that national governments can reign in these potential corporate and individual cyberattackers. Second, even if a nation's interest are attacked, it will often be difficult to determine immediately, which country or organization is the culprit. For example, a harmful cyber-event may be the result of an organized attack by the government of Russia, by rogue elements in the Russian military, by groups of computer attackers tolerated by the government of Russia, by cyberattackers controlled by large criminal syndicates, by organizations supported by Russian oligarchs or corporations, or by individual hackers, political or apolitical. (The example of Russia is not chosen because I believe it to be especially nefarious.)

Finally, computer technology is not dependent on any single controllable bit of technological knowledge (such as what is possessed by a small group of nuclear physicists c. 1948), or on physical substances (such as U-235). It is remarkable, for example, how cyptological techniques and computer systems have spread to a wider and wider public. Cyberattack technology is more like an idea than like a physical thing (or person). These facts would seem to make the creation of international treaties governing cyberattacks between governments, and laws within sovereign territories, extraordinarily difficult to develop, verify, and enforce. It is likely for a long time to be a brutish, if highly informed and non-physical, constrained combat between defensive and offensive operations. It will probably increasingly require greater and greater allocations of money and human resources.

VII. Conclusion

Cyberwarfare appears to be almost entirely unrestricted by traditional morality and laws of war. At least it is not explicitly addressed. Because of a traditional emphasis on damage to material objects, there are not even clear restrictions on “soft- or cyber-” damage that would leave wholly civilian targets, necessary for the well being of the population, inoperable for long periods of time but not, in the strictest sense, damage them as objects.

The relevant entities in cyberwarfare are so unusual in comparison with the ordinary objects of daily live that the only useful way of thinking about them seems to be by analogy. Namely, the relevant cyberentities include such things as the functioning of a system (an occurrent entity in one major ontology¹⁹), software, and more broadly, information entities (generically dependent continuant entities). Consequently, moral reasoning about cyberwarfare requires either the consideration of analogies with more traditional moral problems or broader and clearer moral theories capable of application to all possible ethical events and states of affairs.

It is perhaps understandable that the traditional morality of war, and laws of war, would not want to address such vague notions as the welfare or well-being of the civilian population. The most obvious and undebatable damage of war is on human beings as organisms: they die, that is, stop being organisms at all. Nevertheless, a cyberattack may do such extensive damage to the well-being of a populace, and to the functioning of a government, that it would satisfy the *casus belli* (just cause) requirement of reasonable

¹⁹ In the Basic Formal Ontology referenced at <http://www.ifomis.org/bfo/manual.pdf>. Most other major applied ontologies make similar distinctions. Applied formal ontologies include large-scale efforts in the U.S. Federal Government (UCore-2) and the Department of Defense to standardize the structuring of data accorded to the most comprehensive and widely accepted schemes of describing reality.

criteria for morally going to war. Likewise, there would seem to be a need for additional moral reasoning, and additions to international law, such that militarily unnecessary damage to non-objects, namely the functioning of civilian informatics systems, is limited in time of war.

In writing this paper, three serious worries have occurred to me. First, there is a large array of possible scenarios involving cyberattacks for which there does not exist obvious moral reasoning, or even straightforward analogies, that could guide us. Second, I am disturbed by the extent to which, through easy internet access, much of our defense informatics infrastructure is vulnerable to attack. I am myself engaged in research in developing systems that require regular access to open information sources (notably a variety of ontology and other web-based resources) that would not be available for long periods if a largescale cyberwar would erupt. I have long been disturbed by the departure from the relatively secure arpanet for use in defense applications to a wide-open internet, that has not one, relatively secure hard-wired Ethernet portal, but a variety of possible portals by broadband, cellular phone, infrared, and Bluetooth pathways.²⁰ Third, it is clear especially from General Alexander's comments (notably his 2007 paper) that serious thought is being devoted to the development of policy and strategy. To date it has remained largely shrouded in secrecy. This will be, and maybe even now may be, a serious problem, since the making public of many elements of policy are absolutely required for a deterrent effect.

Finally, it is interesting that, as far as I can see, traditional ethical and political theories—utilitarianism, Kantian theory, natural rights theory, etc.-- cast so little light on this new, and difficult domain. Certainly no one of these theories seems at a special advantage in clarifying the issues. Instead, it is only the vaguest of *prima facie* notions that are most useful in elucidating the issues: (human) well-being, harm, intentional or knowing harm, political entities and their roles as agents, and essential function of states in promoting or protecting the well-being of their citizens.²¹ It has also been my working assumption that fully understanding moral constraints on warfare requires understanding certain conclusions from game theory and working them into more traditional moral thinking about war. To date, there is virtually no effort in this direction.²²

²⁰ In this I came to what I later found out was Libicki's conclusion: "Dampening the Ardor for Network-Centric Operations" (pp. 149f) and an earlier remark "Cyberattacks are Possible Only Because Systems have Flaws." I would prefer to say that it is because such systems of information networks have flaws, and, because of complexity, are likely always to have exploitable flaws; but the chief difficulty is the access to them that we choose to give everyone in the WWW.

²¹ A suspicion of the role that highly developed ethical theories might usefully play for issues in the morality of war is one of the curious remarks in Nicholas Fotion's excellent book, *War & Ethics: A New Just War Theory* (2007, p. 1).

²² I want to thank especially Alan W. Dipert and Catherine Ullman for having given me, on short notice, very useful feedback on an earlier draft. I am a contractor for the U.S. Army, working on a Command and Control Ontology with funding from the Army Net-Centric Data Strategy Center of Excellence, Building 1209, Fort Monmouth, NJ 07703. I allude to this research in my discussion of the entities that are necessary to discuss ethical questions, but not in the ethical views themselves; any views or doctrines expressed in this essay are strictly those of the author, and not of the U.S. Army or the U.S. Department of Defense.

Other issues: cyberwar within the military? Libicki p. 181: legal authority USC 10 (military) vs. USC 50 (intelligence).