Goettingen Journal of International Law 3 (2011) 1, 373-396

Information Warfare and Civilian Populations:

How the Law of War Addresses a Fear of the Unknown

Lucian Dervan*

Table of Contents

A. Introduction 375
B. Computer Network Operations and International Law 380
I. The Applicability of International Humanitarian Law to Information Operations 381
II. The Three Pillars of the Law of War 383
1. Necessity 384
2. Distinction 387
3. Proportionality and Unnecessary Suffering 389
C. Conclusion 395

* Assistant Professor of Law, Southern Illinois University School of Law, and former member of the King & Spalding LLP Special Matters and Government Investigations Team.

doi: 10.3249/1868-1581-3-1-dervan

Abstract

Imagine a civilian communications system is being temporarily relied upon by an opposing military force for vital operations. If one launches a computer network attack against the communications system, the operation may disable the opposing force's ability to function adequately and, as a result, prompt their surrender. The alternative course of action is to launch a traditional kinetic weapons attack in the hopes of inflicting enough casualties on the troops to induce surrender. Given these options, the law of war would encourage the utilization of the computer network attack because it would result in less unnecessary suffering. But is the same true if we are unsure of the collateral consequences of the computer network attack on a large civilian population that also relies on this communications system? For instance, because civilians use the same communications system to gather critical information, disabling the system might result in rioting, civil disorder, serious injuries, and deaths. Further, civilians may be unable to call for help, seek out medical assistance, or locate emergency response centers. Given these unknown yet potentially severe collateral consequences to civilians, it becomes less clear that a proportionality analysis under the law of war would favor the computer network attack over the traditional kinetic operation. In this article, Professor Lucian E. Dervan examines the application of the law of war to information operations and analyses the role of the Geneva Convention's utilitarian goals in determining the validity of computer network attacks against dual-use civilian objectives.

A. Introduction

Mobile telephones are vital military instrument for the Taliban in Afghanistan.[1] The devices are used to detonate bombs, coordinate military movements, and communicate with leadership regarding future operations.[2] Despite their usefulness, mobile telephones also pose a significant risk to the Taliban.[3] Over twelve million civilians in Afghanistan have mobile telephones and their use is not limited to communicating with family and friends or calling for medical or police assistance in times of need.[4] For many Afghani civilians, mobile telephones serve as a weapon with which to provide information regarding the Taliban to coalition forces.[5] Of course, because the civilians are often under the watchful eyes of Taliban forces during the day, most tips are provided at night, under the cover of darkness.[6]

In 2008, in response to the growing nighttime flow of information between civilians and coalition forces, the Taliban ordered the mobile telephone industry to shut down some cell-towers from 5:00 p.m. to 6:30 a.m.[7] According to the Taliban, this trial program to stop civilians from informing on Taliban movements was a success and, as a result, they

1 Y. Trofimov, 'Cell Barriers Bow to Taliban Threat' (22 March 2010) available at http://online.wsj.com/article/SB10001424052748704117304575137541465235972.html (last visited 28 April 2011); ("The Taliban are using the cellphone system as an instrument of war against the Afghan government and the U.S.-led coalition.").

2 *Id*. ("'Cellphones are a powerful tool for the Taliban: They offer a cheap and effective means to direct insurgent activities or pass intelligence…' Militants all over the world use mobile phones to trigger explosions.").

3 *Id*.

4 *Id*. ("Sardar Wali, a 19-year-old student from the Khwaja Mulk village north of Kandarhar city, said that, when his father became suddenly sick one night last year, the cellphone blackout prevented the family from calling a taxi to ferry the man to the hospital."); M. Pueschel, 'Cell Phones May Have Potential in Global Health Arena', (26 August 2010) available at http://fhp.osd.mil/new.jsp?newsID=180 (last visited 28 April 2011), discussing the "potential use of cell phones as innovative, cheap and efficient tools for public health".

5 Trofimov, *supra* note 1.

6 *Id*. ("American troops, meanwhile, had painted phone tip-line signs on walls outside U.S. bases. Informers are usually reluctant to call in tips during daytime, when they can be spotted by Taliban sympathizers, military officers say.").

7 *Id*.

ordered a nationwide shutdown of all cell-towers during the night.[8] At first, mobile telephone phone companies resisted these demands, unwilling to deprive their twelve million Afghan customers a vital service.[9] In response, however, the Taliban destroyed over forty cell-towers, valued at sixteen million dollars.[10] As might be expected, the mobile telephone providers then acquiesced.[11] Today, millions of Afghans are thrust into isolation during the night as cell-tower after cell-tower goes dark.[12]

While the Taliban gained control over a vital communications network using kinetic force, many militaries around the world have begun to utilize sophisticated information operations to achieve similar results without firing a single bullet and without the cooperation of civilian leaders or private business organizations. The term "information operations" refers to operations that involve the use of "electronic means to gain access to or change information in a targeted information system without necessarily damaging its physical components"[13]. Though there are various types of information operations, the most common is the use of computer network attacks to gain access to, disrupt and/or assert control over vital computer systems.[14] As an example, rather than destroying mobile telephone towers in

8 *Id.* ("[T]he Taliban noted that "the trial implementation of the decision has yielded positive results," and decreed a sweeping national ban on night-time calls to 'protect the Afghan people.'").

9 *Id.*

10 *Id.*

11 *Id.* ("'We understand that in some areas, unfortunately, there is no other way,' Mr. Sangin [Afghan Communications Minister] says, 'We don't have security to protect the towers.'").

12 *Id.*

13 Department of Defense, Office of General Counsel, 'An Assessment of International Legal Issues in Information Operations' (May 1999), 5 [Assessment of International Legal Issues]; 'War in the Fifth Domain', *The Economist* (1 July 2010) 25, 25-27.

14 *Id.* (Assessment of International Legal Issues), 5 ("The proliferation of global electronic communications systems and the increased interoperability of computer equipment and operating systems have greatly improved the utility of all kinds of information systems. At the same time, these developments have made information systems that are connected to any kind of network, whether it be the Internet or some other radio or hard-wired communications system, vulnerable to computer network attacks."); D. B. Hollis, 'Why States need an International Law for Information Operations', 11 *Lewis & Clark Law Review* (2007) 4, 1023, 1030 ("Much IO, however, centers on employing computers themselves in previously unavailable methods through the concept of 'computer network operations.'"); According to the United States Department of Defense, information operations can be broken down into six component parts: Psychological Operations, Electronic Warfare, Computer

Afghanistan, the Taliban could have hacked into the mobile telephone companies' computer networks and seized control of the programs that regulate the cell-towers' operations. Such an attack, which could have been executed from anywhere in the world, would have allowed the Taliban to dictate the times during which civilians could utilize their mobile telephones without using kinetic weapons to permanently destroy the cell-towers.[15] Information operations, therefore, are less expensive to execute than traditional military operations and allow for a more targeted and less destructive result.[16] A real-world example of an information operation occurred during the 2008 Russian intervention in South Ossetia, a separatist region of the former Soviet Republic of Georgia.[17] As traditional kinetic military operations were undertaken against Georgian targets, computer network attacks were simultaneously launched.[18] These attacks defaced government websites and prevented communication between the Georgian President and the civilian population.[19] The attack also disabled certain

Network Operations, Military Deception, and Operational Security: W. E. Richter, 'The Future of information Operations', *Military Review* (2009) 1, 103, 103-104. This article focuses on computer network attacks.

15 Department of Defense, *supra* note 13, 5 ("[G]lobal communications are almost seamlessly interconnected and virtually instantaneous, as a result of which distance and geographical boundaries have become essentially irrelevant to the conduct of computer network attacks.").

16 J. Markoff, 'Before the Gunfire, Cyberattacks' (12 August 2008) available at http://www.nytimes.com/2008/08/13/technology/13cyber.html (last visited 28 April 2011). ("'It costs about 4 cents per machine […] You could fund an entire cyberwarfare campaign for the cost of replacing a tank treat, so you would be foolish not to.'").

17 S. Watts, 'Combatant Status and Computer Network Attack', 50 *Virginia Journal of International Law* (2010) 2, 391, 397; M. Schwirtz, A. Barnard & C. J. Chivers, 'Russia and Georgia Clash over Separatist Region' (8 August 2008) available at http://www.nytimes.com/2008/08/09/world/europe/09georgia.html (last visited 28 April 2011); M. Schwirtz, A. Barnard & A. E. Kramer, 'Russian Forces Capture Military base in Georgia' (11 August 2008) available at http://www.nytimes.com/2008/08/12/world/europe/12georgia.html (last visited 28 April 2011).

18 *Id.* (Watts), 397; Markoff, *supra* note 16, detailing the computer network attacks by Russia against Georgia during the conflict over South Ossetia. To date, the Russian government has denied involvement in the information warfare operations against Georgia and, as is the case with many such computer network attacks, there is little evidence to link the Russian government to the operations.

19 Watts, *supra* note 17, 397.

government, news, transportation, and banking websites, creating disorder and panic amongst the civilian population.[20]

Of course, information operations and computer network attacks extend well beyond communication networks and government websites. Such computer network attacks can cripple all manner of vital infrastructure, including electric power grids, water supply stations, food distribution networks, air traffic control systems, and emergency services apparatus, including evacuation notices and coordination of medical response teams.[21] The importance of controlling computer networks through information operations has become so vital to modern warfare that nations around the world are currently engaging in limited computer network attacks in preparation for possible future armed conflicts.[22] In 2009, U.S.

20 *Id.* ("Later reports revealed that the CAN campaign had preceded the physical invasion by as much as twenty-four hours and that hackers may have launched computer network probing operations as early as July 20th."); Markoff, *supra* note 16 ("Weeks before bombs started falling on Georgia, a security researcher in suburban Massachusetts was watching an attack against the country in cyberspace.").

21 The USA Patriot Act of 2001 defines critical infrastructures as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." USA Patriot Act of 2001 section 1016, text available at http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR: (last visited 28 April 2011), 42 U.S.C., § 5195c. Included within this definition are the following: agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry, and postal and shipping. S. M. Condron, 'Getting it Right: Protecting American Critical Infrastructure in Cyberspace', 20 *Harvard Journal of Law & Technology* (2007) 2, 403, 406, National Strategy for Homeland Security: The President of the United States, 'National Strategy for Homeland Security' (16 July 2002) available at http://www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf (last visited 28 April 2011), 30.

22 S. Gorman, 'Electricity Grid in U.S. Penetrated by Spies' (8 April 2009) available at http://online.wsj.com/article/SB123914805204099085.html (last visited 28 April 2011). ("Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials."). Eric Jensen quotes a passage from a Chinese army publication entitled "Unrestricted Warfare."

> "[I]f attacking side secretly musters large amounts of capital without the enemy nation being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment in the opponent's computer

intelligence officials revealed that cyber operatives from China and Russia had infiltrated American electric power grid computer networks and planted malicious computer software programs to disrupt power supply in the event of a future military conflict.[23] Along with targeting the U.S. power supply, these cyber operations targeted computer networks controlling water, sewer, and other vital infrastructure systems.[24] As the world's appreciation and contemplation of the importance of information operations grows, these undertakings are likely to continue to increase in sophistication and prominence.

While information operations offer concrete advantages to militaries, they also pose two significant dangers to civilians. First, because militaries often utilize information systems and infrastructure resources that are primarily civilian in nature, a growth in information operations will result in increased targeting of civilian objectives. Second, various unpredictable collateral consequences can result to a civilian population from the infiltration and manipulation of vital computer networks. Given these dangers, this article will examine the lawfulness of computer network attacks under international law. In particular, this article will analyze whether traditional international legal principles regarding the law of war can adequately adapt to the utilitarian advantages of this new generation of warfare.

> system in advance, while at the same time carrying out a network attack against the enemy so that the civilians electricity network, traffic dispatch network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots and a political crisis. There is finally the forceful bearing down by the army, and military means are utilized in gradual stages until the enemy is forced to sign a dishonorable peace treaty.", E. T. Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense', 38 *Stanford Journal of International Law* (2002) 2, 207, 207 [Computer Attacks on Critical National Infrastructure].

23 Gorman, *supra* note 22.

24 *Id.* In 2000, a computer network attack in Australia resulted in the release of 200,000 gallons of sewage into parks, rivers, and the grounds of a hotel.

B. Computer Network Operations and International Law

Imagine it is the year 2015, and the nation of Agnia has been closely monitoring a developing situation in the neighboring state of Centuria, with whom it has been engaged in cross-border skirmishes for five years. According to satellite imagery, ten-thousand troops from the Centurian military have begun massing on the outskirts of one of Centuria's largest cities, Atlantis. Atlantis is located only one mile inside Centuria, has a population of one million, and contains many ethnic Agnians. According to intelligence reports, the mayor of Atlantis, an ethnic Agnian, has lead large anti-government protests during the past two weeks, which have included calls for the city and the surrounding region to become an independent country or be subsumed by Agnia. Leaders in Agnia fear that the Centurian military is preparing to attack the city and regain control of its population through force. Sympathetic to the desires of the citizens of Atlantis, the President of Agnia asks her military commanders to prepare a computer network attack directed against Centurian troops with the objective of preventing or limiting their intended military operations.

The Agnian military commanders quickly return with a plan that recommends two separate operations to disrupt the Centurian military.

> (1) First, the Centurian military is relying on electric power for operation of much of its equipment. Therefore, the Agnian military commanders recommend use of a computer network attack to temporarily cut off power to the specific power grid being utilized by the Centurian military. While this directed attack will not result in power loss to the entire city of Atlantis, it will result in a loss of power for civilians who rely on the same power grid currently being utilized by the Centurian military. It is estimated this attack will negatively impact approximately twenty-thousand civilians. Further, the Agnia military commanders have warned the President that there is a possibility that the computer network attack will inadvertently cause a total power failure in Atlantis, thus depriving all one million citizens of power.

> (2) Second, the Agnian military commanders recommend targeting the Atlantis civilian communications infrastructure, which controls the dissemination of all satellite, internet, broadband, and mobile communication services in the region. This communications system is currently being utilized by the Centurian military for its own vital information gathering and communications purposes. According to the Agnian military commanders, a computer network attack will temporarily disable all civilian and military information gathering and communications in the region. The commanders are unsure what collateral consequences might result from depriving the civilians of Atlantis use of the communications system.

Before these attacks are launched, a determination must be made regarding whether these non-kinetic operations are permitted under international law. Should these operations be deemed impermissible, the Agnian military commanders will recommend a traditional kinetic weapons attack against the Centurian military. The commanders believe that this attack will result in the deaths of at least one-thousand Centurian troops, but will result in few, if any, civilian casualties.

I. The Applicability of International Humanitarian Law to Information Operations

While outside the scope of this article, the initial question for consideration in this hypothetical situation is whether the proposed computer network attacks are a "use of force" as described by the United Nations Charter. The United Nations Charter states that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations"[25]. If Agnia's actions are considered a "use of force", the computer network attacks may constitute a violation of the United Nations' mandate against breaches of the peace.[26]

Much debate has occurred in academia regarding whether computer network attacks constitute a "use of force." Some scholars argue that

[25] Art. 2(4) Charter of the United Nations.
[26] See Arts 23-32 and 51 Charter of the United Nations.

information operations directed at critical national infrastructures are by definition "uses of force" that permit the aggrieved nation to respond with proportional self-defense pursuant to the United Nation's Charter.[27] Other scholars have argued that computer network attacks that result in damage that otherwise would require kinetic weaponry constitute a "use of force"[28]. Finally, some scholars contend that a determination regarding whether a computer network attack is a "use of force" depends on the particular circumstances of the operation and whether the results of the attack are sufficiently severe.[29]

While the debate regarding whether computer network attacks are "uses of force" under the United Nations Charter is a fascinating topic and significant to the future regulation of information warfare, this article's focus is on the ramifications of such operations to civilians under the framework of *jus in bello*. As such, the more important question for consideration is whether international humanitarian law applies to this

27 Jensen, 'Computer Attacks on Critical National Infrastructure', *supra* note 22, 208-209 ("[A]ttacks against a nation's critical national infrastructure from *any* source constitutes a use of force. Such attacks, therefore, give the victim state the right to proportional self-defense – including anticipatory self-defense.").

28 D. Brown, 'A Proposal for an International Convention to Regulate the use of Information Systems in Armed Conflict', 47 *Harvard International Law Journal* (2006) 1, 179, 187-88.

29 M. N. Schmitt, 'Computer Network Attack and the Sue of Force in International Law: Thoughts on A Normative Framework', 37 *Columbia Journal of Transnational Law* (1999) 3, 885, 914-915. In his 1999 article Michael Schmitt argues for this later proposition and proposes six criteria for such an analysis – (a) the severity of the attack, (b) the immediacy of the negative consequences, (c) the directness of the negative consequences, (d) the invasiveness of the harm into the state, (e) the ease of measurability of the harm, and (f) the ability to recognize the action as presumptively impermissible unless falling within one of the two United Nations exceptions to use of force. Using these factors, Schmitt argues one can ascertain whether the characteristics of a particular computer network attack are similar to traditional forms of armed conflict or whether the acts are more appropriately outside this international wartime regulatory regime.; see also J. Barkham, 'Information Warfare and International Law on the Use of Force', 34 *New York University Journal of International Law & Politics* (2001) 1, 57, 58 ("Applying these criteria determines whether the attack is 'armed force' or political or economic coercion […] Once the IW attack is deemed to be a use of force, the extent of the attack can be measured to determine whether there has been an armed attack, which would trigger Article 51.").

situation.[30] As the information operations proposed in this article are significant and would occur within the context of existing border skirmishes, we will assume that the parties are engaged in an "armed conflict" in which the law of war applies.[31]

II. The Three Pillars of the Law of War

Over many centuries the international community has established laws of war based on the guiding principle of *jus in bello*, which means justice in war.[32] During the last century, these principles were codified into various international agreements, each of which serve to promote the ideal that civilians must be protected in times of war.[33] This ideal is contained within the Geneva Convention through the adoption of the requirement that all military operations governed by the law of war satisfy three key criteria.[34] Military operations must be militarily necessary, a distinction must be made

30 The "laws of armed conflicts" establish the bounds governing the manner in which hostilities are conducted. B. Van Schaack & R. C. Slye, *International Criminal Law and Its Enforcement: Cases and Materials*, 2nd ed. (2010), 214.

31 The law of war only applies where there is an "armed conflict", see Art. 2, Geneva Convention Relative to the protection of Civilian Persons in Time of War of August 12, 1949 (GC IV), 75 U.N.T.S. 287; E. T. Jensen, 'Unexpected Consequences from Knock-Out Effects: A Different Standard for Computer Network Operations?' 18 *American University International Law Review* (2002-2003) 5, 1145, 1150 [Unexpected Consequences from Knock-Out Effects] ("Once two nations are in armed conflict with each other, the law of war applies."). Information operations may be sufficient to constitute an armed conflict, see M. N. Schmitt, 'The Principle of Discrimination in 21st Century Warfare', 2 *Yale Human Rights & Development Law Journal* (1999), 144-145 [Computer Network Attacks] ("Humanitarian law does not apply in situations not amounting to armed conflict, such as riots, strikes, demonstrations, isolated acts of violence, or traditional criminal activity, even if military forces are employed to address them. In such cases, domestic and international human rights law tempers the violence."); R. W. Aldrich, 'How Do You Know You Are at War in the Information Age', 22 *Houston Journal of International Law* (2000), 223, 232; Watts, *supra* note 17, 411-412 ("Despite lingering ambiguity concerning states' CAN capabilities, a broad range of commentators accepts that CNAs between states could constitute armed conflict of sufficient scale and intensity to trigger the law of war generally and, specifically, the 1949 Geneva Conventions and their 1977 Protocols.").

32 Schmitt, 'Discrimination', *supra* note 29, 143, 145.

33 *Id.*, 144. ("The protection of civilians and civilian objects during armed conflict is a core purpose of humanitarian law, a branch of international law also known as the law of armed conflict and the law of war.").

34 Discussed in detail i*nfra* section A.II.1 through A.II.3.

between military and civilian targets, and the attacks must be proportional.[35] Though the law of war has witnessed many advances in technology and weaponry, it has remained relevant because of its adaptability[36], an adaptability that is vital when considering its application to the proposed information warfare operations by Agnia.

1. Necessity

While information operations may represent a new type of weaponry, the law of war still requires consideration of the principles of necessity, distinction, and proportionality. As described above, therefore, the first question Agnia must consider is whether a military necessity exists to strike the proposed targets.[37] In this regard, Protocol I to the Geneva Conventions requires that the attacks be directed at military targets with the objective of defeating the opponent military.[38]

35 Art. 48, 51, 52(2), and 57 Protocol Additional to the General Conventions of 12 August 1949, and Relating to the Protections of Victims or International Armed Conflicts (Protocol I), 12 December 1977, 1125 U.N.T.S. 3 (1979); B. Van Schaack & R. Slye, *International Criminal Law and Its Enforcement: Cases and materials*, 2nd ed. (2010), 266.

36 Schmitt, 'Discrimination', *supra* note 29, 145-46 ("Because evolution in the conduct of warfare affects the individuals and objects which humanitarian law seeks to shelter, it is not surprising that law has proven responsive, both proactively and reactively, to warfare's changing nature.").

> "In the aftermath of World War II, bipolarity and wars of national liberation dominated by inter-State conflict, while new technologies and sensibilities led to heightened concerns over the methods and means of warfare. The Additional Protocols to the Geneva Conventions, Environmental Modification Convention, Biological Weapons Convention, Conventional Weapons Convention, and Landmines Convention resulted. So too did numerous arms control treaties designed to limit the testing, possession, and spread of nuclear weapons, the unprecedented power of which had been so dramatically illustrated at Nagasaki and Hiroshima.", *Id.*

37 Department of Defense, *supra* note 13, 8 ("Targeting analysis must be conducted for computer network attacks just as it traditionally has been conducted for attacks using traditional weapons.).

38 J. R. Heaton, 'Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces', 57 *Air Force Law Review* (2005), 155, 180-81 ("The purpose of this principle is to ensure that every military action is driven by a military requirement and is intended to subjugate the enemy in the shortest amount of time and at the least possible expense of men and materiel. Under this principle, acts which lack any direct

> "*Attacks shall be limited strictly to military objectives*. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use 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."[39]

Pursuant to this paragraph, a selected target is valid if (a) it makes an effective contribution to the military action and (b) its destruction will offer a definite military advantage.[40] Where the selected target is part of the opponent's military infrastructure, such as weapons depositories or military communications centers, attacking the target will almost always satisfy the requirement of necessity.[41] The analysis of the proposed attacks by Agnia is complicated by the fact that each operation focuses not on purely military targets, but on dual-use civilian facilities and networks.[42]

military purpose, such as indiscriminate bombing of civilian dwellings or food supplies, are prohibited.").

39 Art. 52(2) Protocol Additional to the General Conventions of 12 August 1949, and Relating to the Protections of Victims or International Armed Conflicts (Protocol I), 12 December 1977, 1125 U.N.T.S. 3 (1979) [Protocol I] (emphasis added); Article 51(4) Protocol I also contains relevant restrictions regarding the targeting of military objectives rather than civilian objectives:

> "Indiscriminate attacks are prohibited. Indiscriminate attacks are:
> (a) those which are not directed at a specific military objective;
> (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or
> (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol;
> and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction."

40 *Id.*; D. E. Graham, 'Cyber Threats and the Law of War', 4 *Journal of National Security Law & Policy* (2010), 87, 98 ("'Military necessity' authorizes the use of force required to accomplish the mission. It does not authorize acts otherwise prohibited by the [laws of war].").

41 Department of Defense, *supra* note 13, 8 ("During an armed conflict virtually all military infrastructures will be lawful targets, but purely civilian infrastructures must not be attacked unless the attacking force can demonstrate that a definite military advantage is expected from the attack.").

42 Where it is unclear whether an object which is normally dedicated to civilian purposes is being utilized for a military purpose, the Geneva Convention requires the party presume the target is not making an effective military contribution. Protocol I, *supra* note 39, Art. 52(3). In the hypothetical examined herein, however, it is clear that the

"Dual-use" targets are ones that "simultaneously serve both civilian and military objectives," including facilities and networks that are primarily for civilian utilization but which are being temporarily used by the military.[43] The Atlantis power station and civilian communications system are both dual-use targets because, while they primarily serve the civilian population, they are currently also being utilized by the Centurian military. While dual-use objectives complicate a necessity analysis, they do not enjoy absolute protection from attack. Rather, the two prong analysis for necessity remains applicable in determining whether these are permissible targets.

First, do the Atlantis dual-use targets make an effective contribution to the Centurian military? This determination is influenced by consideration of the targets' nature, location, purpose, and use.[44] Each dual-use target provides a vital resource to the region and is within the area in which the Centurian military is massing. Further, though originally intended to solely support the needs of the civilian population of Atlantis, these facilities and networks are currently being utilized by the Centurian military for significant information gathering, communications, and support functions. Finally, just as electric power and communications capabilities are vital to the effective subsistence of the civilian population, they are vital to the continued and successful completion of Centuria's military endeavors. As such, these targets do make an effective and, in fact, significant contribution to the military actions of the opposing force. Second, will disabling these facilities and networks offer a definite military advantage? As described above, these facilities and networks are vital to the Centurian military operation. As such, a strong argument exists that targeting these objectives will offer a significant and definite military advantage to Agnia. Based on this analysis, it appears that these proposed targets, though dual-use, satisfy the requirement of military necessity.

power station and civilian communications systems are both being utilized for military purposes.

43 Jensen, 'Unexpected Consequences from Knock-Out Effects', *supra* note 31, 1157; J. M. Meyer, 'Tearing Down the Façade: A Critical Look at the Current Law on Targeting the Will of the Enemy and Air Force Doctrine', 51 *Air Force Law Review* (2001) 143, 178 (discussing dual-use objectives).

44 Protocol I, *supra* note 39, Art. 52(2).

2. Distinction

A concept related to necessity under the law of war is the requirement that military operations utilize weaponry that can distinguish between civilian and military targets and that when attacks are carried out an effort is made to distinguish between civilian and military objectives.

> "In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."[45]

Just as occurred with the necessity analysis, the presence of dual-use targets complicates satisfaction of the distinction requirement.

With regard to the power station attack, the use of an information operation permits the specific targeting of only that power grid being utilized by the Centurian military. As a result, the operation is designed to utilize available weaponry that distinguishes between power grids serving only civilian customers and those being utilized by the Centurian military. Had Agnia decided to target the entire power station, despite its ability to more precisely target only the power grid that was properly classified as a military target, such an act would constitute a violation of the tenet of distinction.[46] In this scenario, therefore, the availability of an information

[45] Protocol I, *supra* note 39, Art. 48; see also Protocol I, *supra* note 39, Art. 51(4): "Indiscriminate attacks are: (a) those which are not directed at a specific military objective; (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objectives without distinction."

[46] M. N. Schmitt, 'Wire Warfare: Computer Network Attack and *Jus in Bello*', 84 *International Review of the Red Cross* (2002), 365, 390 [Wired Warfare] (analogizing the failure to specifically direct an information operation when possible to the use of SCUD missiles by Iraq in the first Gulf War:

> "The SCUD is not an inherently indiscriminate weapon. Indeed, it is easily capable of being aimed with sufficient accuracy against, for instance, military formations in the desert. However, the use of SCUDS against population centres was indiscriminate even if the Iraqi intent was to strike military objectives situated therein; the likelihood of striking

operation actually assists the civilian population by limiting this attack to military objectives.

The analysis is more complex when one considers the proposed operation against the civilian communications network. Currently, it is estimated that 98 percent of all classified governmental communications and 95 percent of all military communications in the United States flow through civilian communication systems, not dedicated military networks.[47] As a result, the composition of modern information systems makes it much more likely that civilian assets will be targeted during times of war. This is particularly true because, unlike the power station example above, the interconnected nature of civilian communications systems makes it almost impossible to isolate military communications for attack. As a result, operations directed against civilian communications systems must disrupt or disable the entire network, shutting down not only military operations but also all civilian information gathering and communication functions. Given these operational realities, Agnia's proposed computer network attack is troubling because of its potential significant impact on civilians who are likely highly dependent on this communications system for important information, particularly during times of unrest and conflict. Further, these concerns regarding potential civilian collateral consequences are more acute when one considers that the utilization of the Atlantis communications system by the Centurian military is likely limited when compared with the total usage by the civilian population. Though these are significant concerns which will be addressed again during the proportionality analysis under the law or war, these issues do not prevent this operation proceeding under the tent of distinction. Rather, if the Atlantis civilian communications system is properly considered a target of military necessity and there is no existing information warfare mechanism by which to disrupt only the military communications, this proposed attack is permissible.[48]

protected persons and objects so outweighed that of hitting legitimate targets that the use was inadmissible.").

47 E. T. Jensen, 'Cyber Warfare and Precautions Against the Effects of Attacks', 88 *Texas Law Review* (2010) 7, 1533, 1534 [Cyber Warfare]; Jensen, 'Computer Attacks on Critical National Infrastructure', *supra* note 22, 211.

48 Others considering this issue have reached similar conclusions: Schmitt, 'Wire Warfare', *supra* note 48, 384 ("[I]f an object is being used for military purposes, it is a military objective vulnerable to attack, including computer network attack. This is true even if the military purposes are secondary to the civilian ones.").

3. Proportionality and Unnecessary Suffering

The final prong of analysis to determine the legitimacy of the proposed computer network attacks is proportionality, an analysis that will highlight the uniqueness of information operations and the need for flexibility in determining the permissibility of such military operations. Proportionality conveys the centuries old notion that during war "the right of the parties to the conflict to choose methods or means of warfare is not unlimited… It is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering."[49] This limitation on the methods and means of warfare is intended to protect both combatants and civilians. As such, along with the above general prohibition, the Geneva Convention contains a specific requirement that consideration be given to the impact of proposed operations on civilians.

> "[A]n attack shall be cancelled or suspended if it becomes apparent that the objective is not a military one or is subject to special protection or that the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[50]

Pursuant to the above sections of the Geneva Convention, even where a target is of military necessity and, to the extent possible, a distinction has been made between the military and civilian components of the target, the proposed operation may still violate the law of war if it would result or may be expected to result in unnecessary suffering by either combatants or

[49] Art. 35(1)-(2) Protocol I, *supra* note 40; see also Article 22 Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land, 18 October 1907, available at: http://www.unhcr.org/refworld/docid/4374cae64.html (last visited 28 April 2011) [Hague Convention IV], ("The right of belligerents to adopt means of injuring the enemy is not unlimited."); and Art. 23(e) (prohibiting the use of "arms, projectiles, or material calculated to cause unnecessary suffering").

[50] Art. 57(2)(b) Protocol I, *supra* note 40; *see also* Art. 51(5) Protocol I, *supra* 37: "Among others, the following types of attacks are to be considered as indiscriminate: (…)(b) an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated".

civilians. At its core, therefore, the proportionality analysis is an examination of the utilitarian ramifications of an operation. Importantly, it is this core utilitarian aspect of the law of war that allows it the flexibility to adapt to new and evolving weaponry, including information warfare.

With regard to the directed attack on the power grid providing energy to the Centurian military, satisfying the proportionality requirement is assisted, in part, by the advent of information operations. First, rather than disabling the power supply to the entire city of Atlantis, a computer network attack in this situation allows for directed targeting of only the power grid within which the Centurian military is operating. This significantly limits the attack's impact on the civilian population and, although civilians living within the same power grid will be impacted, a strong argument exists that these collateral consequences do not amount to unnecessary suffering, particularly given the significant military advantage to be gained through the attack. Second, an information operation is distinct from a traditional kinetic attack because it does not destroy the asset being targeted. As a result, once the military advantage is secured or the reason for the operation dissipates, power to the grid can be restored. With traditional kinetic weaponry, such quick remediation is impossible. As an example, kinetic attacks against Iraqi power stations during the first Gulf War lead to decades of power supply problems for the civilian population.[51] By comparison, the proposed attack by Agnia is both specifically directed at a limited portion of the total power supply and can be reversed once the military necessity of the operation has passed.

While the above proposed directed attack on the Atlantis power station appears to satisfy the proportionality requirements of the law of war, there remains a hidden danger in undertaking this operation that must be considered.[52] As admitted by the Agnian military commanders, though

51 Department of Defense, 'Assessment of International Legal Issues', *supra* note 14, 8-9 (discussing the bombing of Iraq's power grids during the first Gulf War); see also Associated Press, 'Iraq suffers hot summer amid power problems' (7 September 2009) available at http://www.msnbc.msn.com/id/32726457/ (last visited 28 April 2011): "During the 1991 Gulf War, U.S. warplanes targeted the power grid. It was further damaged in the 2003 invasion, the looting that followed and finally by insurgent attacks designed to cripple the country".

52 Schmitt, 'Discrimination', *supra* note 32, 168. ("If first-tier collateral damage and incidental injury (i.e., damage and injury directly caused by the kinetic force of the

information operations offer the ability to more precisely target certain objectives, interfering with computer networks can result in significant unintended consequences. In some situations, an information operation might be directed at a single network believed to control a precise system, but which might unexpectedly also control other vital portions of the civilian infrastructure. Further, where a virus or other malicious program is utilized to disable a specific computer network, it is possible that the virus might spread to other unintended computer systems.[53] Such secondary effects are called "knock-out effects"[54]. As an example, consider again the proposed computer network attack on the Atlantis power station's computer network. The intended goal of the operation is to disable only the power grid that supplies the region being occupied by the Centurian military. It is possible, however, that while launching this attack an error in the computer program might shut down the entire power station and deprive the whole city of Atlantis of energy. This lack of power might in turn result in the city's water treatment plant and other vital pieces of infrastructure becoming inoperable. Further, unknown to the Agnian military, the same computer network that controls the power station might also control other vital portions of the infrastructure, including portions of the infrastructure vital to the survival of the civilian population.[55] For these reasons, "knock-out

attack) become rarer, it is probable that humanitarian attention will increasingly dwell on subsequent-tier, or reverberating, effects.").

53 Schmitt, 'Wired Warfare', *supra* note 48, 389.

> "In many cases, once a vital code is launched against a target computer or network, the attacker will have no way to limit its subsequent retransmission. This may be true even in a closed network, for the virus could, for instance, be transferred into it by diskette. Simply put, a malicious code likely to be uncontrollably spread throughout civilian systems is prohibited as an indiscriminate weapon."

54 *Id.*, 392-93 ("The most cited example is that of the attack on the Iraqi electrical grid during the 1990-91 Gulf War. Although it successfully disrupted Iraqi command and control, the attack also denied electricity to the civilian population (a 'first-tier' effect), thereby affecting hospitals, refrigeration, emergency response, etc.") Both the terms "knock-on effects" and "knock-out effects" are used to describe these secondary collateral impacts.

55 Art. 54(2) Protocol I, *supra* note 37, specifically prohibits attacks directed at infrastructure that is vital the survival of civilians:

> "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."

effects" can be devastating to the civilian population. How, therefore, should the possibility of such unexpected and unpredictable collateral consequences flowing from information operations be addressed by the law of war? Should these potential ramifications to the civilian population result in our rejecting this information operation in favor of the assured, yet limited destructive results of the alternative kinetic attack against the Centurian forces?

While the possible collateral impact on civilians from "knock-out effects" are significant, information operations offer discernable concrete benefits and allow for the remedying of unforeseen consequences. These advantages to this modern form of warfare strongly support the favoring of information operations over traditional kinetic attacks on utilitarian grounds. First, and perhaps most significant, along with being less expensive, computer network attacks are bloodless as compared to traditional kinetic weaponry.[56] As a result, instead of causing significant long term damage and inflicting large numbers of casualties, a computer network attack advances the Geneva Convention's goal of minimizing suffering.[57] Second, computer network attacks offer a distinct advantage not previously available in war because they can be reversed. As an example, should the proposed information operation against the power station result in a larger impact on the civilian population than predicted, the operation may be remediated by launching a second computer infiltration to place the power station back online.[58] Importantly, countries that rely on information operations should

56 Jensen, 'Unexpected Consequences from Knock-Out Effects, *supra* note 32, 1161 ("Given the bloodless nature of CAN and its ability to affect armed conflict, it can and should be a readily available weapon in the commander's arsenal."); J. T. G. Kelsey, 'Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare.', 106 *Michigan Law Review* 2008) 7, 1427, 1445 ("[W]ar via the Internet is potentially cheaper than waging a conventional campaign.").

57 *Id.*(Kelsey), 1447 (arguing that the law of war should permit information operation that might otherwise be considered unlawful where they have the advantage of "dealing blows to an enemy with a low cost in human life and possibly little physical damage to civilian objects."); R. G. Hanseman, 'The Realities and Legalities of Information Warfare', 42 *Air Force Law Review* (1997), 173, 198 ("to an extent the new technology holds the promise of enabling destructive acts that are not really "violent." Such weapons will be less dependent on big explosions. Few explosions means less property destroyed and fewer unplanned human casualties.").

58 This article does not purport to argue that reversing information operations is easy or reliable. Nevertheless, in considering the utilitarian advantages of information

be required to prepare such remedial operations in advance and in anticipation of the possibility of knock-out effects.[59] Such remediation would not be possible with traditional kinetic weaponry, which would inflict irreversible devastation once unleashed. As a result, though the proposed computer network attack holds the possibility of causing significant unintended collateral damage, because of the concrete humanitarian benefits of such operations and the likelihood of remediating any unintended consequences before they result in disproportionate suffering, engaging in this operation, despite the dangers, appears consistent with the goals of the law of war.[60]

operations as compared to kinetic weaponry, the ability to reverse an attack should be considered. Further, if militaries rely on utilitarian arguments in proposing computer network attacks, they should be obligated to prepare strategies for responding to any unforeseen consequences in advance of initiating the operation to minimize any delay in remediating unexpected collateral consequences. See J. P. Terry, 'The Lawfulness of Attacking Computer Networks in Armed Conflicts and in Self-Defense in Periods Short of Armed Conflict: What are the Targeting Constraints?' 169 *Military Law Review* (2001), 70, 86-87.

59 *Id.*, 86-87.

> "[A]ny weapon developed to provide [computer network attack] capability must be both predictable and capable of being armed and disarmed; otherwise they will unduly threaten innocent civilians in the target state *and* the user state. Downs is correct when he suggests that weaponeers should, in general, co-develop a detection and immunization program for all viruses they intend to use. In this way, a [digital data warfare] attack gone wrong cannot inadvertently do harm to the attacker."

60 An argument also exists that where the collateral consequences are speculative they do not violate the proportionality doctrine because they were not "expected" to occur. See Protocol I, *supra* note 37, Art. 57(2).

"With respect to attacks, the following precautions shall be taken:
(a) those who plan or decide upon an attack shall:
(i) do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives within the meaning of paragraph 2 of Article 52 and that it is not prohibited by the provisions of this Protocol to attack them;
(ii) take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss or civilian life, injury to civilians and damage to civilian objects;
(iii) refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."

see also E. T. Jensen, 'Unexpected Consequences from Knock-Out Effects', *supra* note 32, 1179-81 (arguing that only those consequences that are expected to occur are considered indiscriminate and, therefore, computer network attacks that lead to

In examining the proposed attack on the Atlantis civilian communications system, the same types of considerations regarding utilitarianism must be made to determine the operation's legitimacy. As discussed above, civilian communication systems are interconnected in such a manner as to make it nearly impossible to isolate specific military communications from general civilian utilization of the networks. As a result, the entire system must be targeted and disabled. Just as the collateral consequences of the attack on the power station are unclear, so too are the ramifications from disabling a city's communications network. Here, however, the analysis is slightly different. Unlike the power station example, it is clear that this operation will impact the entire city of Atlantis. What remains uncertain, however, is whether the resulting detriment to civilians will be severe enough to warrant abandoning this information operation in favor of a traditional kinetic attack on Centurian forces. It is possible the proposed attack will result in the civilian population being inconvenienced, but not subjected to unnecessary suffering or deprived of necessities vital to its existence.[61] It is also possible, however, that the attack may result in severe consequences for the civilian population. For instance, the city may experience riots or other civil unrest due to a breakdown in emergency response systems. This alone might result in significant civilian casualties. Further, civilians may have difficulty gathering information regarding food and water distribution centers, where to receive medical treatment or other assistance, or where to take shelter or evacuate the city should armed conflict ensue. Given the possible direct and significant impact on civilians resulting from a disruption of the Atlantis civilian communications system and the limited use of the system by the military, does this proposed attack satisfy the requirement of proportionality?

Once again, if one focuses on the utilitarian goals of the Geneva Convention, it appears that the ascertainable benefits of information operations and the remedial abilities of computer network attacks outweigh

unexpected collateral consequences do not violate the law of war). Where the possible impact on a civilian population from a knock-out effect is contemplated, however, particularly based on past experience, and the consequences are sever, reliance on this doctrine alone may be insufficient.

61 Schmitt, 'Wired Warfare', *supra* note 48, 397 ("For instance, turning off the electricity to a city to disrupt enemy command, control and communications may be acceptable if doing so does not cause excessive civilian suffering.").

the speculative dangers of these undertakings to civilians.[62] First, as discussed above, while the possible collateral consequences to the civilian population are uncertain, it is clear that choosing to launch an information operation rather than engage in traditional kinetic attacks offers significant benefits. Information operations are more cost effective and can result in less loss of life. Further, they do not require the destruction of the objective. Rather, information operations can seek only to disable a target for a specific period of time, a fundamental advantage as dual-use civilian targets grow in prominence. Second, because computer network attacks are often reversible, if the speculative dangers of the operation come to pass the attack can be reversed. In this example, should the lack of a communications system result in significant negative consequence for the civilian population of Atlantis, the Agnian military could execute an operation to restore the system to full functionality. Again, this would require certain anticipatory planning on the part of the Agnian military, thus allowing them to respond quickly should such events transpire. Requiring such anticipatory planning seems a small cost, however, in return for the significant benefits to both civilians and military personnel from favoring information operations over traditional kinetic attacks.[63]

C. Conclusion

The law of war has evolved as battlefields and weapons have changed. Today, warfare has drifted into the ether and is taking place within computer networks and information systems. As a result, the law of war must adapt as it has in the past to take advantage of the benefits of this new type of

62 Hollis, *supra* note 15, 1055: "Perhaps states should allow [Information Operations] a wider, albeit virtual, impact on civilian populations if the result is less physical harm overall, or even on an individual basis, than traditional warfare."

63 It is important to note that this article is advancing the theory that unintended and unexpected collateral consequences should not prohibit the utilization of modern weaponry that holds the potential to significantly reduce the amount of death and suffering during war. This does not mean, however, that where the collateral consequences of a proposed computer network attack are probable that the analysis is the same. In such situations, the risks associated with a computer network attack, particularly where assurance could not be provided regarding the reversibility of the mission, may lead to a determination that the operation does not satisfy the proportionality requirements of the law of war. As with all proposed military operations, the application of the law of war must be conducted in a case by case manner applying all ascertainable facts.

weaponry, including the unique ability to remediate unexpected consequences. Though war will never be without tragedy or loss, if information warfare holds the possibility that war might be more humane for civilians and militaries alike the law of war should seize these advantages and not reject these utilitarian advancements for fear of the unknown.