AU/ACSC/019/2001-04

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

INFORMATION WAR CRIMES:

MITNICK MEETS MILOSEVIC

by

Darwyn O. Banks, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Lt Col Steven R. Hansen

Maxwell Air Force Base, Alabama

April 2001

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
01APR2001	N/A	-

Title and Subtitle Information War Crimes: Mitnick Meets Milosevic	**Contract Number**
	Grant Number
	Program Element Number
Author(s) Banks, Darwyn O.	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Air Command and Staff College Air University Maxwell AFB, AL	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes The original document contains color images.	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 40	

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States Government.

Contents

Page

Illustrations

Page

Tables

Page

Acknowledgments

I would be remiss if I didn't acknowledge the invaluable assistance provided by my advisor, Lt Col Steve Hansen, by Dr Abby Gray-Briggs and by the phenomenal staff at AU Library, especially Ms. Diana Simpson. I must also thank my sponsors, Lt Col Richard Aldrich and Lt Col Charles Williamson, the judge advocates at Headquarters, Air Force Office of Special Investigations and at the Joint Task Force-Computer Network Defense, respectively, for their assistance and encouragement of this layman on legal turf.

Abstract

In this paper the author examines areas of overlap between information crimes (also known as hacking and cyberterrorism) and traditional war crimes as defined by the internationally accepted laws of armed conflict paying special attention to the principles of chivalry, humanity, proportionality, and military necessity. The paper further explores the potential culpability of information warfare practitioners should this intersection of information warfare and war crimes become codified into international law.

Chapter 1

Introduction

> *The cyberwar revolution, however, poses serious problems for the U.S. Some are ethical: Is it a war crime to crash another country's stock market?*
>
> —*TIME*, August 1995[1]

The law of armed conflict is an internationally accepted standard which defines the conduct of war between 'civilized nations.' It has served the world well since its earliest inception in the 17th century.[2] As the state-of-the-art and the state-of-the-practice have advanced, the global community has seen fit to revise and update this body of law many times to ensure its continued applicability and/or to address the conundrums posed by the new technologies.

The Information Age dawned just as the 20th century began drawing to a close. With the new age came new civil crimes, *e.g.*, hacking, cyberterrorism, which forced law enforcement communities around the globe to adapt—some better than others. One key question which remains largely unanswered, however, concerns the application of international law in the Information Age. Specifically, how might emerging interpretations of the law of armed conflict re-define war crimes in the realm of information warfare?

Building on examples of information crimes and of war crimes from recent events, this paper focuses on the four defining principles from law of armed conflict as they apply to traditional war crimes: chivalry, humanity, proportionality, and military necessity and explores ways in which these may apply to war in the Information Age.

Mitnick

> *I have gained unauthorized access to computer systems at some of the largest corporations on the planet, and have successfully penetrated some of the most resilient computer systems ever developed.*
>
> —Kevin Mitnick[3]

In February 1995 law enforcement agents from the Federal Bureau of Investigation finally tracked down and arrested wanted cyber-criminal, Kevin D. Mitnick, in North Carolina.[4] The California-based fugitive led authorities on a cross-country chase for more than two years while fleeing from charges he gained unauthorized access to the computer systems of the California Department of Motor Vehicles in 1992. Immediate accusations against him included stealing thousands of data files and more than 20,000 credit card numbers from computer systems at Motorola, Nokia Mobile Phones, Fujitsu, Novell, NEC, Sun Microsystems, Colorado SuperNet and the University of Southern California, to name a few, with estimated damages approaching $80 million.[5]

Fact and fiction converge on the subject of Mitnick. Some accounts credit Mitnick with successfully hacking into the systems of the North American Aerospace Defense Command (NORAD) in the early 1980s and thus becoming the inspiration for the 1983 motion picture, *War Games*.[6] Additional allegations have him gaining temporary control of central telephone offices in New York City and phone switching centers in California, as well as stealing between $1 million and $4 million in proprietary software from computers at Digital Equipment Corporation.[7] Truth or fantasy, the police record on Mitnick does include exploits going back more than a decade to 1981 when juvenile courts sentenced the teenaged Mitnick to probation for electronic theft of computer documents from his local telephone company.[8] Ultimately, Mitnick received indictments on 25 counts of wire fraud, computer fraud, possessing unlawful

access devices, damaging computers, theft of software valued in the millions of dollars, using stolen computer passwords and intercepting electronic messages.[9] After plea bargaining, Mitnick served a total of five years behind bars with more than a few months in solitary confinement because the judge feared he could access computers via the telephone and "launch nuclear missiles by whistling into the phone."[10]

None of Mitnick's exploits, however, violated international law. Despite the borderless potential of his actions, the known effects of Mitnick's documented crimes remained within the United States. Onel de Guzman, on the other hand, is another computer criminal whose effects did cross borders. In May of 2000, de Guzman, a failed Filipino collegian from AMA Computer College, released the "ILOVEYOU" computer virus which had been written in an effort to gain free access to the Internet by stealing passwords to local service providers.[11] The virus quickly infected computers worldwide, including many in the U.S. Department of Defense as well as the British House of Commons.[12] It overloaded e-mail systems and by some estimates caused approximately $10 billion worth of damage.[13] Still, despite the documented international effects of the so-called "Love Bug" virus, de Guzman received more reward than punishment. At the time of the virus' release, The Philippines had no statutes on the books forbidding computer misuse and that country's National Bureau of Investigation had insufficient evidence to convict de Guzman of the closest "traditional" cognates: theft and credit card fraud.[14] Ultimately, the government in Manila dropped all domestic charges filed against him while the man himself received offers of lucrative employment from international computer firms, his lack of a degree notwithstanding.[15]

Unfortunately, The Philippines are not alone. Neither are the industrialized nations, such as members of the G-7, standing above the fray. At present, dissemination of computer viruses is

not illegal in Japan.[16] Until a highly publicized series of hacking attacks in February 2000, the Land of the Rising Sun was the only major industrialized nation that did not prohibit illegal entry to computer networks, *i.e.*, hacking.[17] At the time of the attacks, the headlines of *Mainichi Shimbun*, a nationwide Japanese newspaper, boldly proclaimed: "Welcome, Japan, to the world of cyberwar."[18] But was that really accurate? The messages may have claimed foreign origins, but computer crimes, in and of themselves, are not warfare.

Milosevic

> *I've always considered the international tribunal at The Hague an illegal and immoral institution.*
>
> —Slobodan Milosevic[19]

While Messrs. Mitnick and de Guzman may have steered clear of international law, one criminal who plainly did not is the former Yugoslavian president, Slobodan Milosevic. He stands apart from either of the two aforementioned individuals in that, as of this writing in February 2001, he has yet to come before any tribunal—domestic or international. The charges against him include crimes against humanity and violations of the customs of war.[20] Where Mitnick and de Guzman committed information crimes, Milosevic stands accused of traditional war crimes—specifically murder, deportation and persecution.[21]

With indictments handed down by an internationally chartered judicial body, the International Criminal Tribunal for the Former Yugoslavia (ICTY), Milosevic's crimes clearly reside in the domain of international law. The United Nations Security Council established that international tribunal in February 1993 based upon its investigations of Balkan fighting which found " 'grave breaches' of international norms," such as mass killings, torture, systematic rape, complete destruction of civilian towns and housing, and violent dislocation of the populace—*i.e.*,

ethnic cleansing.[22] While there are no claims that Milosevic personally committed any such crimes, he is culpable under the principles of command responsibility and direct responsibility. The former alleges Milosevic's foreknowledge of such crimes without acting either to prevent the commission thereof or to punish the perpetrators. The latter form of responsibility implies he authorized, planned, instigated and/or ordered the unlawful acts.[23] These indictments against the former Yugoslav president, then, highlight the primary categories of the law of armed conflict.

Notes

1. "Onward Cyber Soldiers," *TIME*, 21 Aug 1995, Volume 146, No. 8.
2. *Encyclopaedia Britannica,* on-line ed., s.v. "Grotius."
3. U.S. Senate, *Cyber Attack: Is the Government Safe?: Hearing Before the Committee on Governmental Affairs*, 106th Congress, 2d Session, 2 March 2000, p. 47.
4. John Markoff, "A Most-Wanted Cyberthief is Caught in his own Web," *The New York Times*, 16 Feb 1995, Vol 144, p 1.
5. John Christensen, "The trials of Kevin Mitnick," *CNN Interactive*, 18 March 1999, available on-line from http://www.cnn.com/SPECIALS/1999/mitnick.background/.
6. Ibid.
7. Kim Murphy, "Ex-Computer 'Whiz Kid' Held on New Fraud Counts," *Los Angeles Times*, 16 December 1988.
8. Christensen, n.p.
9. "Mitnick Gets 22 Months for Hacking," *Associated Press*, 28 June 1997.
10. Troy Anderson, "Mitnick wants to save others from hackers," *DailyNews.com*, 3 July 2000.
11. "Charges Dismissed: Philippines Drops Charges in 'Love Bug' Virus Case," *Associated Press*, 21 August 2000.
12. "Philippines Clears 'Love Bug' Suspect," *Reuters*, 21 August 2000.
13. Alisha Ryu, "Philippines / Love Bug Indictment," *Voice of America*, 29 June 2000.
14. Steve Gold, "Philippines Drops Love Bug Virus Charges," *Newsbytes*, 22 August 2000.
15. Ibid.
16. "Study: Japan Cybercrime Tripled," *Associated Press*, 12 January 2001.
17. Kathryn Tolbert, "Hackers Slam Japanese Government Web Sites," *The Washington Post*, 1 February 2000.
18. Ibid.
19. "Milosevic attacks war crimes tribunal," *CNN.com*, 3 February 2000.
20. Michael P. Scharf, "The Indictment of Slobodan Milosevic," American Society of International Law, June 1999.
21. Lawyers' Committee for Human Rights, "Milosevic Indictment: Frequently Asked Questions," n.p., available from http://www.lchr.org/feature/kosovo/faq.htm.
22. Julia Preston, "U.N. Creates Tribunal to Try War Crimes in Yugoslav Warfare," *The Washington Post*, 23 February 1993, Volume 113, Number 8, p. 3.

Notes

23. Lawyers' Committee.

Chapter 2

The Law of Armed Conflict

The right of belligerents to adopt means of injuring the enemy is not unlimited.

—Protocol IV of the Hague Convention[1]

Two primary sets of treaties comprise the law of armed conflict. The Hague Convention focuses on the means and methods of warfare. This law addresses the violations of the customs of war and discusses how "civilized warring states" should prosecute war. Its counterpart, the Geneva Convention, deals more specifically with the status of non-belligerents and other protected persons, *e.g.*, prisoners of war, wounded belligerents, chaplains, medical personnel, and civilians.[2] The treaties of the Geneva Convention seek to ameliorate the effects of war on both soldiers and civilians.[3]

Additionally, there are more specific precedents set forth in the London Charter of 1945. The Allies—France, the Union of Soviet Socialist Republics, the United Kingdom, and the United States—used this charter to establish the International Military Tribunals at Nürnberg after World War II and held defendants from defeated Nazi Germany individually responsible for actions taken during the war. The London Charter codifies categories of these crimes as follows: crimes against peace, war crimes and crimes against humanity.[4] Crimes against peace include the steps leading up to and including a war of aggression, *i.e.*, planning, preparing, initiating and/or waging such a war. The war crimes category encompasses murder,

mistreatment—*e.g.*, murder or torture—of prisoners of war, deportation for slave labor, killing hostages, destruction of cities, towns or villages not justified by military necessity, and plunder. Crimes against humanity duplicate many of the atrocities from the 'war crimes' category but with an emphasis on civilian victims—*e.g.*, murder, enslavement, deportation, rape and other inhumane acts against civilian populations in war.[5]

Beneath the overarching conventions, the law of armed conflict breaks down into a series of four basic principles. These are chivalry, humanity, military necessity and proportionality.[6] Given the terminology, the first principle, chivalry, might seem to be a throwback to medieval times. In fact, Encyclopedia Britannica defines chivalry as the "honourable and courteous conduct expected of a knight."[7] Realizing, however, that the knight of yore is the soldier, sailor, airman or Marine of today aptly underscores the meaning of this principle in the context of the law of armed conflict.

At the dawn of the 21st century, chivalry has come to be the requirement that nations wage war in accordance with internationally recognized courtesies and formalities.[8] The most practical modern example is the chivalric prohibition against perfidy defined as "acts inviting the confidence of an adversary to lead him to believe he is entitled to, or is obliged to, accord protection under the rules of international law applicable in armed conflict with intent to betray that confidence."[9] Perfidious actions include combatants falsely donning the uniforms of the enemy or the symbology of non-combatants, *e.g.*, chaplains, medics or United Nations peacekeepers. Perfidy can also include faking surrender, cease-fire, armistice and/or incapacitation both to draw one's opponent in close and simultaneously to lull him into a false sense of security.[10] Obviously, the systemic danger of permitting such treachery runs parallel to the risk incurred by the proverbial boy who cries "Wolf!" Continued misuse of protected

symbols could quickly lead combatants to disregard them all, thus nullifying their special status and needlessly prolonging the combat.[11]

The second principle is humanity. This principle proscribes combatants from inflicting "unnecessary suffering" either upon other combatants or upon civilian populations.[12] Under the aegis of humanity, the international community has banned a variety of weapons which cause 'superfluous injury'—*e.g.*, dum-dum bullets which expand on contact and/or cause especially painful wounds, poisoned weapons, laser weaponry specifically designed to cause permanent blindness, and projectiles filled with glass or other fragments which are difficult for medics to detectable and remove.[13] In American military jurisprudence, judge advocates review each new or proposed weapons system before deployment to the field specifically to determine the weapon's legality in accordance with the law of armed conflict's principle of humanity.[14] Also prohibited under this principle are bacteriological, biological and chemical agents which typically have indiscriminate effects—*i.e.*, they affect wide areas and could easily spread to impact nearby civilians.[15]

Military necessity is the third principle. It permits combatants to expend only as much force as is necessary to achieve their aims—typically, the opponents' submission—with minimal cost in terms of time, resources and loss of life.[16] In this sense military necessity precludes the type of overkill that might be expected between mismatched belligerents where one's force greatly outnumbers or outclasses the other's. An extreme example would be a superpower's unlikely and ill-advised recourse to intercontinental ballistic missiles when arrayed against a non-nuclear enemy without the capability or the wherewithal similarly to threaten the superpower.

Additionally, military necessity specifically exempts civilian objects and property from being deliberately targeted unless the destruction or incapacitation thereof would produce a

direct military advantage. Of course, civilian materiel which is of dual use would be a legal target inasmuch as its "damage or destruction would produce a military advantage because of their nature, location, purpose, or use."[17] Citing Protocol IV of the 1907 Hague Convention: "[it is especially forbidden] to destroy or seize the enemy's property, unless such destruction or seizure be imperatively demanded by the necessities of war."[18]

The last principle is proportionality. Closely related to the principle of humanity, proportionality requires combatants to consider the potential effect of their bellicose actions upon the civilian population.[19] Note that proportionality doesn't prohibit all targeting that could impact the populace; in war collateral damage may often be unavoidable. Rather this principle requires a conscious assessment of the military necessity of the target and anticipated military advantage of its destruction against the projected civilian losses, both tangible and intangible. Thus, assuming the defender is not attempting to hide legitimate military targets within them, civilian institutions such as hospitals, schools, mosques, churches or museums rarely provide sufficient military advantage as targets to justify the cost of hitting them.[20]

In addition to the four foregoing principles, international law also includes concepts of reprisal and retorsion.[21] While these two are not strictly part of the law of armed conflict, they do prescribe the methods by which countries may appropriately respond to belligerence directed against them. Thus, in the context of information warfare and potential commission of information war crimes, these concepts become noteworthy for their import to the range of available responses.[22]

The primary distinction between the concepts of retorsion and reprisal is legality. While both entail unfriendly acts, the former is an unambiguously legal recourse taken for retaliatory or coercive purposes. The use of force for the latter would normally be illegal outside of the set of

prescriptive steps reprisal delineates.[23] Examples of retorsion might include such actions as cessation of economic aid, the shutting of ports, travel restrictions, denial of entry visas, revocation of tariff concessions, or display of naval forces.[24] These are unfriendly measures but not prohibited by international law.

Reprisals, on the other hand, do involve the use of force and are illegal unless the following conditions apply. First, the reprisal must itself be a response to the illegal action of another state. Second, the victim of that illegal precursor must give the original assailant state the formal opportunity to redress the situation. Finally, if the victim state does not receive satisfaction, it may retaliate pursuant to the principle of proportionality.[25]

> "A State victim of a violation of an international obligation by another state may resort to countermeasures that might otherwise be unlawful, if such measures (a) are necessary to terminate the violation or prevent further violation, or to remedy the violation; and (b) are not out of proportion to the violation and the injury suffered."[26]

The four principles of the law of armed conflict define the boundaries within which nations, their leaders and their combatants must operate as members of the global community. Drawn from the successive Hague and Geneva Conventions, these principles represent the cumulative efforts over the centuries of states and statesmen to establish better—some might say, 'more civilized'—ways of handling international problems and of resolving international disputes. Heretofore, "war was not subject to any control other than that exercised by the combatants themselves. Any limitations those combatants might have placed on their actions on the battlefield would have been due only to military necessity rather than any belief that to attack civilians or to kill prisoners of war was wrong—let alone illegal."[27]

Beginning with Dutchman Hugo Grotius' 17th century treatise, *De Jure Belli ac Pacis*[28] *(1625*), that conception began to change. Of course, technological advances certainly continued unabated. By 1899 The Hague Conventions specifically include the "Martens Clause" to extend

established custom and humanitarian principles to new technologies which would arise after the close of the 19th century. Even then, the means of warfare were ever-changing. This clause was an attempt "to prevent future unnecessary and/or disproportionate destruction from weapon systems not yet developed."[29] Its ancillary effect set the precedent—quite pertinent to modern discussions of information warfare—which judges an attack by its effects, not its methods.[30]

Even with the Martens Clause, nations still have seen fit periodically to revise and update international law. For example, with the advent of military airpower, the same 1899 Convention in The Hague also accepted a declaration prohibiting the discharge of projectiles or explosives from balloons.[31] Like other turn-of-the-20th-century declarations against asphyxiating gas and expanding dum-dum bullets, this proscription failed to carry over to powered flight.[32] Nonetheless, its consideration set the precedent for the world community to re-assess and update its agreements as required and, more importantly, underscored the protocol that "the right of belligerents to adopt means of injuring the enemy is not unlimited."[33] Therefore, the matter in question is how might the comity of nations eventually limit the means of information warfare?

Notes

1. Laws of War: Laws and Customs of War on Land (Hague IV); October 18, 1907, Chapter I, Article 22.
2. Capt Robert G. Hanseman, "The Realities and Legalities of Information Warfare," *Air Force Law Review* 42 (1997): p 180.
3. *Encyclopaedia Britannica,* on-line ed., s.v. "Geneva Convention."
4. Douglas Hodgson, "International Enforcement of International Humanitarian Law and Recent Developments in International Criminal Law," paper presented at *Millennium 2000 International Humanitarian Law Conference: Exploring the Interface between International Humanitarian Law and International Human Rights Law*, Australian Red Cross, Perth, Western Australia, 13-15 July 2000.
5. Hanseman, p 181.
6. Ibid. See also Desaussure in *Air Force Law Review* 37 (1994): p 41.
7. *Encyclopaedia Britannica,* on-line ed., s.v. "chivalry."
8. Hanseman, p 182.
9. Protocol Additional to the Geneva Convention of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflict, 8 June 1977, Part III, article 37.

Notes

10. Mark R. Shulman, "Discrimination in the Laws of Information Warfare," *Columbia Journal of Transnational Law* 37 (1999): p 959.

11. Department of Defense, Office of the General Counsel, "An Assessment of International Legal Issues in Information Operations," 2nd edition, August 1999, p 6.

12. Hanseman, p 182.

13. DoD General Counsel, p 6.

14. Hanseman, p 174, 182.

15. DoD General Counsel, p 6.

16. Hanseman, p 181.

17. DoD General Counsel, p 5.

18. Laws of War: Laws and Customs of War on Land (Hague IV); October 18, 1907, Chapter I, Article 23(g).

19. Hanseman, p 182.

20. Ibid.

21. Shulman, p. 951.

22. For a more complete treatment of the concept of reprisal as it relates to information warfare, see Maj Daniel M. Vadnais, "Law of Armed Conflict and Information Warfare: How Does the Rule Regarding Reprisals Apply to an Information Warfare Attack?" Research Report no. 97-0116 (Maxwell AFB, Ala.: Air Command and Staff College, 1997).

23. DoD General Counsel, p 51.

24. Travis A. Wise, "University of Oregon School of Law Outlines," available on-line from http://www.law.uoregon.edu/~outlines/Other/SantaClara/Second/intllawwise.pdf.

25. Shulman, p 951.

26. *Restatement (Third) of Foreign Relations Law of the United States* (American Law Institute, 1987), Section 905 cited in Vadnais.

27. *Encyclopaedia Britannica,* on-line ed., s.v. "Law of Armed Conflict."

28. Translated: *On the Law of War and Peace*.

29. Col (ret) James P. Terry, "Responding to Attacks on Critical Computer Infrastructure: What Targets? What Rules of Engagement?," *Naval Law Review* 46 (1999): p 171-2.

30. Lawrence T. Greenberg, Seymour E. Goodman, Kevin J. Soo Hoo, *Information Warfare and Information Law*, (Washington, D.C.: Institute for National Strategic Studies, National Defense University, 1997), p 32.

31. Laws of War: Prohibiting Launching of Projectiles and Explosives from Balloons (Hague IV); July 29, 1899.

32. *Encyclopaedia Britannica,* on-line ed., s.v. "Law of Armed Conflict."

33. Laws of War: Laws and Customs of War on Land (Hague IV); October 18, 1907, Chapter I, Article 22.

Chapter 3

Information Operations and Information Warfare

> *Information warfare is waged against industries, political spheres of influence, global economic forces, or even against entire countries. It is the use of technology against technology; it is about secrets and the theft of secrets; it is about turning information against its owners; it is about denying an enemy the ability to use both his technology and his information.*
>
> —Winn Schwartau[1]

Joint Publication 3-13, *Joint Doctrine for Information Operations*, defines information warfare as the subset of "information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."[2] Information operations, then, are those "actions taken to affect adversary information and information systems while defending one's own information and information systems."[3] The superset of information operations includes a variety of disciplines: operational security, psychological operations, electronic warfare, military deception, command and control warfare, intelligence, public affairs, civil affairs, and physical or computer network attack.[4] This list is representative, but by no means exhaustive as depicted by the "Other" category in Figure 1.

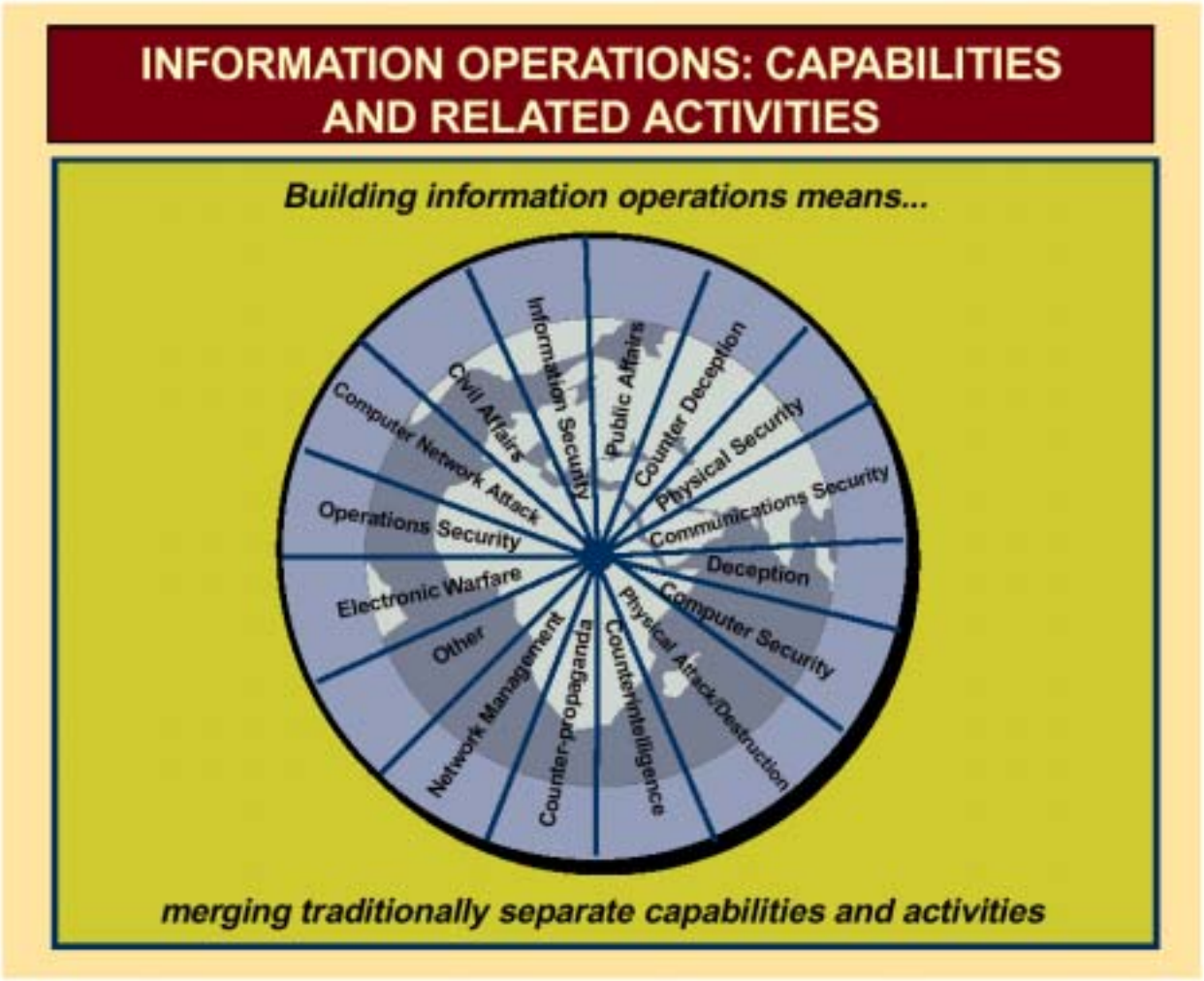

Figure 1: Information Operation: Capabilities and Related Activities[5]

John Petersen posits two generations of information warfare. The first presumes a continuing and not-unreasonable desire on the part of combatants to destroy targets either in actuality or in effect: "the military is looking at future warfare with a perspective that presumes that the extraordinary characteristics of information technology will essentially be used to break things better and therefore kill people more efficiently. ... [F]amiliar military objectives are targeted using new technology."[6] Greenberg, Goodman and Soo Hoo compile an apt list of possible scenarios in this first generation shown in Table 1.

Table 1 Examples of Potential Information Warfare Attacks[7]

"Trap door" hidden in code controlling switching centers of the Public Switched (Telephone) Network causing portions of it to fail on command
Mass dialing attack by personal computers overwhelms local phone system
"Logic bomb" or other intrusion into rail computer systems causes trains to be misrouted and crash
Enemy radio and television network taken over electronically, and then used to broadcast propaganda or other information. "Video morphing" could make the new broadcasts indistinguishable from enemy's own usual broadcasts
Remotely alter formulae for medication at pharmaceutical manufacturers, or personal medical information, such as blood type, in medical databases
Concerted e-mail attack overwhelms or paralyzes a significant network
Divert funds from bank computers, or corrupt data in bank databases, causing disruption or panic as banks need to shut down to address their problems
Steal and disclose confidential personal, medical, or financial information to blackmail, extort and/or cause widespread social disruption or embarrassment
"Computer worm" or "virus" damages data and disrupts systems
"Infoblockade" permits little or no electronic information to enter/leave a target nation (*i.e.*, the servers and gateways known to be primary portals for target)
Nation's command and control infrastructure disrupted with individual military units unable to communicate either with each other or with central command
Stock or commodity exchanges, electric power grids, municipal traffic control systems, and air traffic control systems manipulated or disrupted with accompanying disruption, physical destruction, or loss of life

The examples from Table 1 are far from hypothetical. Many already exist in one form or another with practical—often financial—consequences. The presence of row nine's computer viruses is all but self-evident. Anti-virus vendors currently catalogue more than 53,000 different viruses.[8] Meanwhile, the 'trap doors' from the first row of Table 1 and the 'logic bombs' from row three can reside within either hardware or software. In hardware, they typically reside on the integrated circuits more commonly known as silicon chips. Information war theorists codify the practice as follows: "The modification, alteration, design, or use of integrated circuits for pur

poses other than those originally intended by the designers is called 'chipping.' And chipping provides the Information Warrior with a bevy of opportunities to wage war."[9]

At one end of the chipping spectrum is rampant fraud against cellular phone systems. Wireless telephones routinely broadcast their chip's serial number with every attempted call. Interceptors surreptitiously capture that information, then use it to program fraudulent chips. The billing system charges the calls made with the phony phone chips to the unsuspecting owners of the originals. The annual cost of this fraud to the telecommunications industry and its consumers: $300 million to $350 million.[10]

Chipping's other extreme uses "a circuit that electromagnetically broadcasts a distinctive signal or pattern as a tracking device … [or] a useful tool for gathering information in a clandestine manner."[11] Vendors such as Codex Systems openly advertise sales of such devices to military and intelligence agencies.[12] After all, "replacing or adding a chip to a computer or printer is not too difficult for a repairman or computer dealer."[13] Beyond simple surveillance, there are also "information warfare targets designed to enhance an attacker's relative military position:"[14]

> "The arms industry is an ideal market for government-sponsored chipping. … [T]he electronic goodies inside the weapon system have been chipped; they have been modified perhaps to fail in three months [*sic*] time, or to shoot off course by three degrees, or to blow themselves up after two shots. Or maybe they have a radio beacon installed in them that identifies their exact location to overhead satellites. … From the Information Warrior's viewpoint, chipping takes advantage of unexploited vulnerabilities that exist in virtually every electronic system."[15]

A final example from row seven of Table 1 points to the upheaval associated with loss of financial data. Such economic information warfare has non-trivial impacts.

> "[It] involves the destruction of the marketplace, by preventing buyers and sellers from communicating with each other or erasing records of transactions. … A series of [information warfare] attacks on a country's major banks, draining them of their assets, would cause a major panic …, a serious degradation of that country's financial position relative to the rest of the world and cause long-term damage to the country's well-being."[16]

Extreme cases of financial disruption can also foment political upheaval as occurred in Albania during 1997. In that period a collection of 'get-rich-quick' pyramid schemes[17] which had supplanted the country's formal and informal credit markets failed catastrophically wiping out almost half the nation's reported GDP and much of the personal savings of ordinary Albanians.[18] The resultant rioting brought about the collapse of the government in Tirana and ushered in a period of anarchy and civil war which claimed some 2,000 lives.[19] Such mayhem, death and destruction caused just by phony numbers is hardly inconsequential.

However, Petersen is not content with these more tangible, first-generation effects. For him, "warfare is not about equipment or armies. It is about influencing peoples [*sic*] minds. *Warfare is about achieving behavior change*.... (emphasis in original)"[20] In describing his second generation, Petersen draws upon the philosophies of the ancient Chinese strategist, Sun Tzu: "To subdue the enemy without fighting is the acme of skill. Thus, what is of supreme importance in war is to attack the enemy's strategy."[21] Therefore, second-generation information warfare is less about the 'warfare' and more about the 'information.' Its antecedent likewise moves from the battlefield to Madison Avenue: "What will the second-generation [*sic*] of Infowar look like? Well, it probably looks much like advertising...."[22]

Advertising? While advertising hardly seems to be the province of the military commander,[23] re-examination of joint doctrine shows that "human decision making processes are the ultimate target for offensive information operations."[24] Information operators do, in fact, seek actively to manage the enemy's perceptions.[25] In like manner, advertisers work to subvert human decision-making processes and thereby to accomplish their commercial objectives—*i.e.*, convincing consumers to surrender money for products or services.[26] The decision-making processes are substantially the same whether the objective is increased sales or to help "joint

force commanders influence the outcome of campaigns and major operations."[27] The two sets of processes converge and can be influenced in similar ways. In the end "is a world where ideas, messages, and admonitions are focused on individuals and groups who never figure out that they have been soldiers in a battle. The most successful campaigns, by definition, are never public. The adversary never knows that he or she was in a skirmish."[28]

It follows naturally that unwitting adversaries in perfectly covert campaigns will never know that they are the victims of information war crimes.[29] Moreover, neither will any other member of the world community. Thus, one expects the intersections of information warfare with the law of armed conflict which are most likely to be called criminal to come from the first generation. That does not, however, imply that the second generation will have evolved beyond any such legal considerations; quite the opposite, in fact. Victims' ignorance notwithstanding, "violations of the law of armed conflict subjects [*sic*] individuals to criminal sanctions under national laws (as exist in the U.S.) and to international judgment...."[30] How then, might the principles of the law of armed conflict define an information war crime?

Notes

1. Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway.* (New York: Thunder's Mouth Press, 1994), p 291.
2. Joint Publication 3-13, *Joint Doctrine for Information Operations*, 9 October 1998, para. 3j, p I-11.
3. Ibid., para. 1a, p I-1.
4. Ibid., para. 3g, p I-9.
5. Ibid., Figure I-3, p I-10.
6. John L. Petersen, "Information Warfare: The Future," in *Cyberwar: Security, Strategy and Conflict in the Information Age*, ed. Campen *et al.* (Fairfax, Virginia: AFCEA International Press, May 1996), p 221.
7. Greenberg *et al.*, pp 3-6.
8. McAfee.com, *AVERT Virus Information Library*, available on-line at http://vil.mcafee.com/default.asp?.
9. Schwartau, pp 164-5.
10. City of New York, Department of Consumer Affairs, *Avoiding Cellular Phone Fraud*, available on-line at http://www.ci.nyc.ny.us/html/dca/html/dcacellu.html.

Notes

11. Schwartau, p 168.

12. John Stanton, "Rules of Cyber War Baffle U.S. Government Agencies," *National Defense* 84, no. 555 (February 2000), pp 29-30.

13. Schwartau, p 168.

14. Michael Schmitt, "Computer Network Attack and the Use of Force in International Law," *Columbia Journal of Transnational Law* 37 (1999), p 896.

15. Schwartau, p 169-70.

16. Todd A. Morth, "Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter," *Case Western Reserve Journal of International Law* 30 (Spring/Summer, 1998), pp 596-7.

17. Pyramid schemes use the monies paid in by later investors to pay artificially high returns to earlier investors stimulating a rush of new investors. In short order, however, the interest and principal due to the old investors exceeds the money that the scheme is able to attract from new investors. As soon as payments are interrupted, confidence in the scheme evaporates. See Chris Jarvis, *The Rise and Fall of the Pyramid Schemes in Albania*, IMF Staff Papers, vol. 47, no. 1 (Washington, D.C.: International Monetary Fund, 2000), p 7 for more details.

18. U.S. Congress, Commission on Security and Cooperation in Europe, *The Present Situation in Albania*, 105th Cong., 1st sess., 23 May 1997, p 24.

19. Jarvis, p 1.

20. Petersen, p 224.

21. Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (London: Oxford University Press, 1963), p 77.

22. Petersen, p 224.

23. Recruiters, of course, are the most obvious exception.

24. Joint Pub 3-13, para. 1a(1), p II-1.

25. Ibid., para. 1b, p II-3.

26. Petersen, p 224.

27. Joint Publication 3-0, *Doctrine for Joint Operations*, 1 Feb 95, para. 7b, p II-15.

28. Petersen, p 226.

29. Note that they certainly may still *be* victims of information war crimes. A crime remains a crime whether or not the perpetrator is found out.

30. Hanseman, p 183.

Chapter 4

The Law of Armed Conflict meets Information Warfare

> Information warfare*, in much larger construct, merges the miracles of modern information technology to an information strategy of victory without violence. Here information is a* weapon *and* target *onto itself: not just a magnifier for physical forces engaged in traditional, legal wars. The targets are the opponents [*sic*] political, social and economic infrastructures—thus raising legal, ethical and moral issues that have not been confronted before. (emphases in original)*
>
> —Alan D. Campen, Colonel (ret), USAF[1]

Over time the law of armed conflict and its defining principles have been adapted, amended and applied as necessary to new situations and new technologies. As has been previously stated, one goal of the Hague Convention in 1899 was to prohibit, if only temporarily, "the launching of projectiles and explosives from balloons, or by other new methods of similar nature."[2] In that case the international community took positive action collectively to evaluate and codify the legitimacy or illegitimacy of weapon types and weapon delivery mechanisms. While not impossible, that option is less likely to occur with information warfare.[3] Instead, judge advocates currently expect the law of armed conflict to "be made applicable to new information technologies by analogizing them to their closest pre-Information Age antecedents."[4] The analogies would be drawn from the practical effects of the weapons or technologies.[5]

One rather large effect such information warfare weaponry could have is the effective declaration of war. However, scholars and diplomats alike remain conflicted over whether any peacetime uses of information operations constitute an act or war and if so, which ones: "War, as

we have traditionally understood it, inherently includes armed forces, force and violence."[6] These are the manifestations which the U.N. Charter expressly forbids. Its preamble plainly states that "armed force shall not be used, save in the common interest." Chapter I goes on to proscribe the use of force.[7] What the Charter does not express, however, is a definition of what exactly constitutes such a "use of force." Twice in fact, in 1945 and again in 1970, the U.N. General Assembly and its precursor body have pointedly opted not to place bounds on this question,[8] instead deferring the issue to case-by-case analysis and thus more flexible determinations by the U.N. Security Council.

In this light the question of reprisals and information warfare gains special significance.[9] However, for the purposes of this discussion on information war crimes, the simplifying assumption will be that a bellicose state of affairs already exists, *i.e.*, that both the information warfare attacker and the target already consider themselves to be in armed conflict.[10] As such, the four principles of the law of armed conflict provide guidance equally to the physical and informational attacker about the legality of their actions.

Working back through those four principles, recall that proportionality requires the military commander to estimate the impact of his attacks in order to limit their effect on the civilian population. However, the information warrior cannot know *a priori* precisely where a computer virus or worm might spread once released. That would require precise knowledge of the entire connectivity of the target system which even the owners themselves may not have; hence the vulnerability. Similarly, should the actual impact of a software-based attack against military air traffic control also disable civilian systems, strand passenger aircraft in instrument meteorological conditions and lead to civilian loss of life, the information warrior may face a war crimes tribunal on charges the attack was not proportional or was 'indiscriminate' under Article

51 of the 1977 Geneva Protocols.[11] Although "directed at a specific military objective," the attack did "employ a method or means of combat the effects of which cannot be limited."[12]

In such disproportionate cases, the commander really has little defense except to say wanly: "I didn't mean to do that." To that end, war crimes jurisprudence contains the so-called "Rendulic Rule"[13] which judges commanders' decisions only in light of knowledge that was available to them at the time.[14] One legal opinion, then, suggests that as a precaution, the information warfare commander delineate and record his or her military objectives and intentions before an attack to make this legal defense available.[15]

With or without precautions, the law of armed conflict does allow for collateral damage as a practical reality of war. However, it also bounds the permissible amount of such damage. Through the principle of proportionality, the international community reserves the right to hold attackers who exceed those limits responsible as war criminals whether their means were physical or cyber.

The next principle, military necessity, presents a less thorny issue. Simply stated, the intended target must have military value and receive only enough force to ensure its destruction.[16] From a targeting standpoint, the information warrior—like any other military commander—can easily avoid war crimes charges if he or she refrains from choosing purely civilian objectives: "Stock exchanges, banking systems, universities, and similar civilian infrastructures may not be attacked simply because a belligerent has the ability to do so."[17]

Interestingly though, there is movement afoot to loosen this prohibition: "The methodology of warfare may change during the Information Age that appears to be upon us. … The result may be far less bloodletting in human casualties, although the result of an Information War may be just as catastrophic for the losers."[18] Strict interpretation of military necessity permits attacks

against the persons, but not the personal property, of enemy leadership.[19] Thus, the legal roadblocks to an alleged plan during Operation ALLIED FORCE to attack Milosevic's personal finances:[20] "absent a showing, for example, that monies are being used to directly support a military effort, [law of armed conflict] would not permit raiding Milosevic's personal accounts."[21] However, these contrarian information war theorists argue instead the military necessity of attacking the very fabric of bellicose societies and imperiling the way of life which sustains them: "This proposal openly acknowledges an intent to inflict hardship upon the … populace who must be held responsible for the deeds of their military forces."[22] Of course, lower standards will expose newly legitimate targets of opportunity in technologically advanced states:

> "The concept of military objective will remain beleaguered as civilian activities are further militarized, and military activities are increasingly civilianized …. How is one to distinguish, as an example, a computer chip manufacturer that sells its chips only to civilian end-users from one that has a number of military contracts? … If military officers use Microsoft Word® as their word processing software of choice, for example, does a Microsoft plant become a valid target?"[23]

Military necessity also presents a special case for a lone superpower: "For the United States, therefore, military necessity often cannot mean that an act is strictly necessary."[24] This is because this principle inveighs against overkilling a target. To some extent there exists an overlap with proportionality on this since the overkill from using excessive force is necessarily disproportionate. For the information warrior, especially while 'information weaponry'[25] is new and relatively untested, the possibility of legitimate overkill remains. If, for example, the commander does not know the full extent of the enemy's information defenses, he or she could reasonably opt to increase the 'cyber ordnance' assigned to a target to produce the desired results. The problem is that "[information warfare] weapons are so new and unproved in battle that commanders cannot know with any confidence how much is enough."[26] Too much additional 'ordnance' could run afoul of war crimes law under the principle of proportionality. In

this case, however, even legal arguments bend to practical realities: the "law of armed conflict does not require commanders to dilute attacks to the point where mission objectives may not be achieved or their own forces are jeopardized, and thus the commander's actions seem appropriate."[27]

Third is the law of armed conflict's humanity principle. Like proportionality, humanity requires the military commander to consider the possibility an attack may cause unnecessary suffering and/or superfluous injury,[28] particularly on the civilian populace. The issues for the information warrior lie in the ubiquitous nature of computer and information systems. Interconnectedness is a hallmark of the Information Age. As such, military targets like the aforementioned air traffic control system or an electrical power generation system are more likely to be closely linked with civilian systems in myriad ways. During Operation DESERT STORM the Iraqi government attempted to turn the tables on coalition forces using this rubric. After conventional bombing took out Baghdad's electrical system, the Iraqis alleged that the attack was attempted genocide and, therefore, both inhumane and disproportionate.[29] The Iraqi capitol's waste treatment systems operated using electrical pumping stations. Without electricity, the city sewers backed up threatening epidemic disease and, thereby, genocide.[30] The interconnectedness in this example is physical, but the concerns for the information warrior are the same: "The day is bound to come when an information warfare attack by the United States against military targets results in civilian casualties."[31]

On the other hand, the principle of humanity could also present an argument for the expanded use of information weapon systems and lessen the information warrior's exposure to war crime charges. Humanity might "favor an [information warfare] operation, for example, when the only military alternative is dropping a large explosive on or near the same target."[32] Of

course, this presumes the target's proximity to populated areas. Nevertheless, "the principle of humanity appears to argue in favor of applying information operations if the alternatives threaten greater physical destruction and loss of life."[33] After all, "hurting a civilian's pocketbook is more ethical than bombing him."[34]

Finally, there is chivalry. More than the other three, this principle harks back to the previously discussed theories on first- and second-generation information warfare. Recall Petersen's comparison of second-generation information warfare to advertising. Application of this theory questions the chivalrous nature of a skirmish which the adversary never knows even happened.[35] After all, even Madison Avenue must abide by truth-in-advertising laws requiring advertisers 1) to be truthful and non-deceptive; 2) to have evidence to back up their claims; and 3) not to be unfair.[36] In any event failure to meet these uniquely commercial criteria does not sink to the level of perfidy which the law of armed conflict expressly forbids. Rather, the better analogy might be to a completely permissible ruse of war the intent of which is to mislead the enemy and to induce specific actions on his or her part.[37] These actions may not be in the enemy's best interest, but neither are they perfidious since they do not seek to betray the enemy's confidence given under a protected symbol. The 1977 Geneva Protocols define ruses of war to include "camouflage, decoys, mock operations and misinformation."[38] Plainly, misinformation is the watchword here and very apt for the information warrior's purposes.

This is not to suggest, however, that information warfare is immune to perfidy. A counterexample might be a Trojan horse or other malicious code that is forwarded to the enemy cleverly disguised as e-mail from the Red Cross/Red Crescent Society or, for that matter, as an executable software patch or upgrade from a reputable software manufacturer and/or computer security firm, *e.g.*, anti-virus updates.[39] Nevertheless, "chivalry may not weigh heavily in the

decision over whether to undertake [information warfare], if only because the penalty for under-estimating chivalry is not likely to be applied unless the perpetrator loses the war and the evidence and forum exist to convict her of a war crime."[40]

Mitnick meets Milosevic

So then, when, where and how do Messrs. Mitnick and Milosevic meet? Interestingly, since his release from federal prison in January 2000, the former is working hard at reformation and appears to be taking positive steps to leave his information crimes behind. Fewer than six weeks after becoming an ex-convict, he was freely giving testimony before the United States Senate to advise that legislative body as it sought to understand and to address the issues of information security: "The United States was my adversary in years of litigation…. Despite that, I am ready, willing, and able to assist, and that is why I am here today."[41]

On the other hand, Milosevic, unlike Mitnick, has not seemed content to remain on just one side of the divide between war crimes and information crimes. While under attack during Operation ALLIED FORCE,[42] Milosevic's government actively engaged in computer network attacks against NATO forces, albeit with minimal success:

> "There was a good deal of publicity given to the activities of Serbian hackers who, with a degree of government sponsorship, sought to disrupt NATO information systems. They had limited success against two NATO websites but failed to systematically disrupt NATO information activities or to gain access to closed defence systems. Nonetheless, Serbian use of CNA [computer network attack], however tentative, is a reminder of the potential of this threat."[43]

As of February 2001, Milosevic has yet to see the inside of a jail cell. Indictments from the International Criminal Tribunal for the Former Yugoslavia notwithstanding, the deposed head of state remains at large. Events are still playing themselves out, but U.S. Secretary of State Colin Powell and members of the international financial community have given Serbia "until March 31 [2001] to co-operate with the war crimes tribunal in The Hague."[44]

Conclusion

Examination clearly shows areas where the law of armed conflict and information warfare intersect. That body of law sets broad bounds for information war crimes just as it does for other war crimes. Meanwhile, judge advocates and information war theorists seek to narrow those boundaries determining, for example, what specific aspects of the ever-more-conjoined military and civilian infrastructures will be legitimate information warfare targets.

Recent interpretations of the law of armed conflict have not redefined war crimes to fit the Information Age. Instead, since the Geneva and Hague Conventions—and more specifically, the Martens Clause thereof—judge crimes by their effects and not their methods, the question of information war crimes has focused on new effects unique to the Information Age. Military actions *by any means* which cause effects previously proscribed by one or more of the law of armed conflict's four defining principles are and remain criminal. Each of those principles—chivalry, humanity, military necessity and proportionality—has carry-overs from traditional warfare to information warfare. Additionally, the entire quartet projects into the 21st century. These projections serve as lighthouses to warn information operations commanders and planners away from the shoals of potentially unlawful behavior. The information warrior may not be physically positioned to commit traditional 'crimes against humanity' as defined in the London Charter—*e.g.*, murder, torture, rape, enslavement, plunder, the razing of villages, etc. Nevertheless, the information warrior's attacks can impact the civilian population. Should those attacks be disproportionate, inhumane or found militarily unnecessary, the information warrior cannot expect immunity from war crimes tribunals. All may be fair in love, but not in war. The 1907 Hague Protocol IV and the Martens Clause see to that.

Notes

1. Alan D. Campen, "Coming to Terms with Information War," in *Cyberwar: Security, Strategy and Conflict in the Information Age*, ed. Campen *et al.* (Fairfax, Virginia: AFCEA International Press, May 1996), p 253.

2. Laws of War: Prohibiting Launching of Projectiles and Explosives from Balloons (Hague, IV); July 29, 1899. The text of the declaration only limits aerial bombardment for a period of five years and only in those conflicts where all the belligerents are signatories to the convention.

3. Hanseman, p 184.

4. Ibid.

5. Greenberg *et al.*, p 32. See also Air Force Doctrine Document 2-1.2, *Strategic Attack* (draft), for a doctrinal discussion of strategic effects. "Effects-based means that military actions, such as operations, targeting or strategy, are designed to produce distinctive and desired results."

6. Greenberg *et al.*, p 39.

7. Charter of the United Nations, Article 2(4): "All 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."

8. See U.N. Charter, Chapter VII, Articles 39-42. Historically, the contentious issue has been to determine whether to expand the U.N.'s unambiguous proscriptions on use of the *military* instrument of power to the *economic* instrument—*e.g.*, America's decades-long economic embargo of Cuba or the 1973 Arab oil embargo. The *informational* instrument of power seems likely to face similar contention.

9. See Vadnais for a more complete treatment of reprisal and information warfare.

10. See Air Force Policy Directive 51–4, *Compliance with the Law of Armed Conflic*t, 26 April 1993, para. 1.6.1 for the following definition of 'armed conflict:' "A conflict between States in which at least one has resorted to using armed force to achieve its aims."

11. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 51. Note: The United States has never ratified this revision of the protocol precisely because this requirement can be said to shift responsibility for segregating civilians from military from defender to attacker. See also Shulman, p 954.

12. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 8 June 1977, Article 51, para 4.

13. Lothar Rendulic was a Nazi general acquitted by the Nürnberg war crimes tribunal of the charge of wanton devastation for his 'scorched earth' campaign in Norway. Essentially, this rule acknowledges the axiom that "hindsight is 20/20 vision."

14. Hanseman, p 188.

15. Ibid.

16. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 52, para. 2.

17. DoD General Counsel, p 7.

18. George Walker, "Information Warfare and Neutrality," *Vanderbilt Journal of Transnational Law* 33 (November 2000), pp 1195-6.

Notes

19. The presumption being the leaders concurrently serve as commanders-in-chief of their nations' militaries. See Col Charles J. Dunlap, Jr., "Rethinking Noncombatancy in the Post-Kosovo Era: The End of Innocence," *Strategic Review* 28, no. 3 (Summer 2000), p 13.

20. Gregory Vistica, "Cyberwar and Sabotage," *Newsweek*, 31 May 1999, p 38.

21. Dunlap, p 13.

22. Ibid., p 14.

23. Michael Schmitt, "The Principle of Discrimination in 21st Century Warfare," *Yale Human Rights & Development Law Journal* 2 (1999), pp 159-60.

24. Shulman, p 958.

25. Reference to information warfare weaponry reflects the U.S. Air Force's recent re-alignment to recognize what that service sees as "the growing role of information operations as a war-fighting weapon ... in direct support of the Joint Force Commander." See https://hq8af.barksdale.af.mil/cc/PA/aia-reorg.htm for more details.

26. Hanseman, p 186.

27. Ibid.

28. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Art. 35, para.2.

29. DoD General Counsel, p 7.

30. Ibid.

31. Hanseman, p 187.

32. Shulman, p 959.

33. Ibid.

34. Don Stauffer, "Electronic Warfare: Battles Without Bloodshed," *The Futurist*, January-February 2000, p 26.

35. Petersen, p 226.

36. Federal Trade Commission, "Frequently Asked Advertising Questions: A Guide for Small Business," General Advertising Policies, available on-line from http://www.ftc.gov/bcp/conline/pubs/buspubs/ad-faqs.htm. See also 15 U.S.C. §41ff.

37. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Art. 37, para.2.

38. Ibid.

39. Shulman, p 960.

40. Ibid.

41. U.S. Senate, *Cyber Attack: Is the Government Safe?*, p 6 ff.

42. For a more complete treatment of Yugoslavia's information warfare activities in that conflict, see Maj Wayne Larsen, "Serbian Information Operations During Operation ALLIED FORCE," Research Report no. 00-100 (Maxwell AFB, Ala.: Air Command and Staff College, Air University, 2000).

43. British House of Commons, *Lessons of Kosovo: Fourteenth Report of the Defence Select Committee*, Report #HC347-I, Session 1999-2000, 24 October 2000.

44. "Serbia given Milosevic deadline," *CNN.com*, 4 February 2001.

Bibliography

15 U.S.C. §41ff.

ABCNews.com, 14 June 2000.

Air Force Doctrine Document 2-1.2, *Strategic Attack* (draft).

Air Force Policy Directive 51–4, *Compliance with the Law of Armed Conflic*t, 26 April 1993.

Aldrich, Lt Col Richard W. "Cyberterrorism And Computer Crimes: Issues Surrounding the Establishment of an International Legal Regime." Institute for National Security Studies, U.S. Air Force Academy, Occasional Paper #32: Information Operations Series. April 2000.

_____. "How Do You Know You Are At War in the Information Age?" *Houston Journal of International Law* 22 (Winter 2000), 223-264.

_____. "The International Legal Implications of Information Warfare," *Airpower Journal*, Fall 1996.

American Law Institute. *Restatement (Third) of Foreign Relations Law of the United States*, 1987. In Maj Daniel M. Vadnais, *Law of Armed Conflict and Information Warfare: How Does the Rule Regarding Reprisals Apply to an Information Warfare Attack?* Research Report no. 97-0116. Maxwell AFB, Ala.: Air Command and Staff College, Air University, 1997.

Associated Press, 28 Jun 1997 - 12 Jan 2001.

British House of Commons. *Lessons of Kosovo: Fourteenth Report of the Defence Select Committee*. Report #HC347-I, Session 1999-2000, 24 October 2000.

Campen, Col (ret) Alan D. "Coming to Terms with Information War." In *Cyberwar: Security, Strategy and Conflict in the Information Age*. Edited by Col (ret) Alan D. Campen *et al.* Fairfax, Virginia: AFCEA International Press, May 1996.

_____, Douglas H. Dearth, R. Thomas Goodden, eds. *Cyberwar: Security, Strategy and Conflict in the Information Age*. Fairfax, Virginia: AFCEA International Press, May 1996.

_____, Douglas H. Dearth, eds. *Cyberwar 2.0: Myths, Mysteries and Reality*. Fairfax, Virginia: AFCEA International Press, June 1998.

Charter of the United Nations, 1946.

City of New York, Department of Consumer Affairs. *Avoiding Cellular Phone Fraud*. Available on-line at http://www.ci.nyc.ny.us/html/dca/html/dcacellu.html, 15 March 2001.

CNN.com, 3 February 2000 - 4 February 2001.

CNN Interactive, 18 March 1999.

DailyNews.com, 3 July 2000.

DelaHaya, MSgt Rick. "Intelligence wings realign under 8th Air Force," 14 November 2000, n.p. Available on-line from https://hq8af.barksdale.af.mil/cc/PA/aia-reorg.htm.

DiCenso, Maj David J. "IW Cyberlaw: The Legal Issues of Information Warfare." *Airpower Journal*, Summer 1999.

Dunlap, Col Charles J., Jr. "Rethinking Noncombatancy in the Post-Kosovo Era: The End of Innocence," *Strategic Review* 28, no. 3 (Summer 2000), 9-17.

Greenberg, Lawrence T., Seymour E. Goodman, Kevin J. Soo Hoo. *Information Warfare and Information Law*. Washington, D.C.: Institute for National Strategic Studies, National Defense University, 1997.

Hanseman, Capt Robert G. "The Realities and Legalities of Information Warfare," *Air Force Law Review* 42 (1997): 173-200.

Hodgson, Douglas. "International Enforcement of International Humanitarian Law and Recent Developments in International Criminal Law." Paper presented at *Millennium 2000 International Humanitarian Law Conference: Exploring the Interface between International Humanitarian Law and International Human Rights Law*, sponsored by the Australian Red Cross. Perth, Western Australia, July 2000.

Jarvis, Chris. *The Rise and Fall of the Pyramid Schemes in Albania*. IMF Staff Papers, vol. 47, no. 1. Washington, D.C.: International Monetary Fund, 2000.

Joint Publication 3-0, *Doctrine for Joint Operations*, 1 February 1995.

Joint Publication 3-13, *Joint Doctrine for Information Operations*, 9 October 1998.

Larsen, Maj Wayne. *Serbian Information Operations During Operation ALLIED FORCE*. Research Report no. 00-100. Maxwell AFB, Ala.: Air Command and Staff College, Air University, 2000.

Laws of War: Laws and Customs of War on Land (Hague IV), 18 October 1907.

_____. Prohibiting Launching of Projectiles and Explosives from Balloons (Hague IV); 29 July 1899.

_____. Protocol Additional to the Geneva Convention of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflict (Protocol I), 8 June 1977.

Lawyers' Committee for Human Rights, *Milosevic Indictment: Frequently Asked Questions*. Available on-line from http://www.lchr.org/feature/kosovo/faq.htm.

Libicki, Martin C. *What is Information Warfare*. Washington, D.C.: Institute for National Strategic Studies, National Defense University, 1995.

Los Angeles Times, 16 December 1988.

McAfee.com. AVERT Virus Information Library. Available on-line at http://vil.mcafee.com/default.asp?.

Miller, Maj Robert D. *International Law: How It Affects Rules Of Engagement and Responses in Information Warfare.* Research Report no. 97-0217. Maxwell AFB, Ala.: Air Command and Staff College, Air University, 1997.

Morth, Todd A. "Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter," *Case Western Reserve Journal of International Law* 30 (Spring/Summer, 1998): 567-600.

Newsbytes, 22 August 2000.

The New York Times, 16 Feb 1995.

"Onward Cyber Soldiers." *TIME*, 21 Aug 1995, Volume 146, No. 8.

Petersen, John L. "Information Warfare: The Future." In *Cyberwar: Security, Strategy and Conflict in the Information Age*. Edited by Col (ret) Alan D. Campen *et al.* Fairfax, Virginia: AFCEA International Press, May 1996.

Reuters, 21 August 2000.

Sanz, Timothy L. "Information-Age Warfare: A Working Bibliography," *Military Review*, March-April 1998, 83-90.

_____. "Information-Age Warfare: A Working Bibliography, Part II," *Military Review*, September-November 1998, 41-50.

Scharf, Michael P. "The Indictment of Slobodan Milosevic," June 1999, n.p. Available on-line from http://www.asil.org/insigh35.htm.

Schmitt, Michael N. "Computer Network Attack and the Use of Force in International Law," *Columbia Journal of Transnational Law* 37 (1999): 885-937.

_____. "The Principle of Discrimination in 21st Century Warfare," *Yale Human Rights & Development Law Journal* 2 (1999): 143-182.

Schneider, Fred B., ed. *Trust in Cyberspace*. Washington, D.C.: National Research Council, National Academy Press, 1999.

Schwartau, Winn. *Information Warfare: Chaos on the Electronic Superhighway*. New York: Thunder's Mouth Press, 1994.

Shulman, Mark R. "Discrimination in the Laws of Information Warfare," *Columbia Journal of Transnational Law* 37 (1999): 939-967.

Stanton, John J. "Rules of Cyber War Baffle U.S. Government Agencies," *National Defense* 84, no. 555 (February 2000), 29-30.

Stauffer, Don. "Electronic Warfare: Battles Without Bloodshed." *The Futurist*, January-February 2000. In Dunlap, Col Charles J., Jr. "Rethinking Noncombatancy in the Post-Kosovo Era: The End of Innocence," *Strategic Review* 28, no. 3 (Summer 2000), 9-17.

Sun Tzu, *The Art of War*. Translated by Samuel B. Griffith. London: Oxford University Press, 1963.

Terry, Col (ret) James P. "Responding to Attacks on Critical Computer Infrastructure: What Targets? What Rules of Engagement?," *Naval Law Review* 46 (1999): 170-187.

U.S. Commission on Security and Cooperation in Europe, *The Present Situation in Albania: Briefing to the Commission on Security and Cooperation in Europe. 105th Congress, 1st session, 23 May 1997.*

U.S. Department of Defense. *An Assessment of International Legal Issues in Information Operations*, 2nd edition. Washington, D.C.: Office of the General Counsel, August 1999.

U.S. Federal Trade Commission. *Frequently Asked Advertising Questions: A Guide for Small Business General Advertising Policies*. Available on-line from http://www.ftc.gov/bcp/conline/pubs/buspubs/ad-faqs.htm.

U.S. Senate, *Cyber Attack: Is the Government Safe?: Hearing Before the Committee on Governmental Affairs*, 106th Congress, 2d Session, 2 March 2000.

Vadnais, Maj Daniel M. *Law of Armed Conflict and Information Warfare: How Does the Rule Regarding Reprisals Apply to an Information Warfare Attack?* Research Report no. 97-0116. Maxwell AFB, Ala.: Air Command and Staff College, Air University, 1997.

Vistica, Gregory J. "Cyberwar and Sabotage." *Newsweek*, 31 May 1999, 38.

Voice of America, 29 June 2000.

Walker, George K. "Information Warfare and Neutrality," *Vanderbilt Journal of Transnational Law* 33 (November 2000): 1079-1202.

The Washington Post, 23 Feb 1993 - 1 Feb 2000.

Wise, Travis A. "University of Oregon School of Law Outlines," Santa Clara University, *International Law* outline, 2 November 1999. Available on-line from http://www.law.uoregon.edu/~outlines/Other/SantaClara/Second/intllawwise.pdf.