



University of Arkansas at Little Rock Law Review

Volume 24 | Issue 3


Article 3

2002

Secret Codes, Military Hospitals, and the Law of Armed Conflict: Could Military Medical Facilities' Use of Encrypted Communications Subject Them to Attack Under International Law?

Philip R. Principe

Follow this and additional works at: <https://lawrepository.ualr.edu/lawreview>

 Part of the [Communications Law Commons](#), [Medical Jurisprudence Commons](#), [Military, War, and Peace Commons](#), and the [National Security Law Commons](#)

Recommended Citation

Philip R. Principe, *Secret Codes, Military Hospitals, and the Law of Armed Conflict: Could Military Medical Facilities' Use of Encrypted Communications Subject Them to Attack Under International Law?*, 24 U. ARK. LITTLE ROCK L. REV. 727 (2002).

Available at: <https://lawrepository.ualr.edu/lawreview/vol24/iss3/3>

This Article is brought to you for free and open access by Bowen Law Repository: Scholarship & Archives. It has been accepted for inclusion in University of Arkansas at Little Rock Law Review by an authorized editor of Bowen Law Repository: Scholarship & Archives. For more information, please contact mmserfass@ualr.edu.

SECRET CODES, MILITARY HOSPITALS, AND THE LAW OF ARMED CONFLICT: COULD MILITARY MEDICAL FACILITIES' USE OF ENCRYPTED COMMUNICATIONS SUBJECT THEM TO ATTACK UNDER INTERNATIONAL LAW?

*Philip R. Principe**

I. INTRODUCTION

In the last decades of the twentieth century, instantaneous communication from virtually any point on the planet became commonplace.¹ The Internet² today is one of the fruits of a communications revolution where tremendous amounts of information can be shared between people located anywhere on the globe. All now have instant access to events in real time wherever they occur.³ People and organizations in the developed world rely heavily on such communications, even taking them for granted, and the United States military certainly is no exception. With thousands of personnel dispersed all over the globe,⁴ the United States military has become

* Juris Doctor, cum laude, The Catholic University of America, Columbus School of Law, Washington, D.C.; Bachelor of Science in Foreign Service, cum laude, Georgetown University, Washington, D.C. Admitted to practice before the courts of the State of Maryland, the District of Columbia, the Commonwealth of Virginia, the United States Court of Appeals for the Fourth Circuit, and the United States Court of Appeals for the Armed Forces. Currently assigned as Area Defense Counsel, Little Rock Air Force Base, Arkansas, Judge Advocate General's Department, United States Air Force. Formerly assigned to the 314th Airlift Wing, Office of the Staff Judge Advocate, Little Rock Air Force Base, Arkansas, 1998-2001. This article was inspired by a position paper published by the International and Operations Law section of the Air Force Judge Advocate General's Department and a response authored by the Little Rock Air Force Base Legal Office. This article cites only unclassified material publicly available to any writer on this subject. The views and conclusions expressed herein are solely those of the author. They are not intended and should not be thought to represent official ideas, attitudes, or policies of the United States Air Force, the Department of Defense, or any agency of the United States Government.

1. Even instantaneous communication from extremely remote, inhospitable areas has become reality. See John F. Burns, *Everest Takes Worst Toll, Refusing to Become Stylish*, N.Y. TIMES, May 14, 1996, at A1 (discussing the leader of a climbing expedition who made a satellite telephone call just below the summit of Mount Everest to his wife in New Zealand immediately prior to his death).

2. The Internet, distilled to its most basic, is "an international network of interconnected computers." *Reno v. ACLU*, 521 U.S. 844, 849 (1997).

3. Although instant access to information can be a force for economic development and liberty, such real time information dissemination can result in the amplification of disruptive effects. Nowhere was this more evident than in the attacks on the World Trade Center in New York City on September 11, 2001. See Felicity Barringer & Geraldine Fabrikant, *A Day of Terror: The Media*, N.Y. TIMES, Sept. 12, 2001, at A25 ("It was one of the rare instances when television brought disaster into American homes in real time.").

4. As of March 2001, there were approximately 1.48 million people on active duty in the United States military. See U.S. DEP'T OF DEF., REPORT ON ALLIED CONTRIBUTIONS TO

equally dependent on this instantaneous communication through computer data networks for routine "housekeeping" functions, as well as for warfighting capability.⁵ This capability rests on the secure dissemination of information, much of it encrypted⁶ and classified.⁷ As military facilities become increasingly linked to classified, encrypted computer data networks, questions arise under international law and the law of armed conflict (LOAC)⁸

THE COMMON DEFENSE B-19 (Mar. 2001), available at http://www.defenselink.mil/pubs/allied_contrib2001/allied2001.pdf.

5. See WHITE HOUSE, DEFENDING AMERICA'S CYBERSPACE: NATIONAL PLAN FOR INFORMATION SYSTEMS PROTECTION 82 (version 1.0 2000), available at http://www.ciao.gov/CIAO_DocumentLibrary/national_plan%20final.pdf [hereinafter DEFENDING AMERICA'S CYBERSPACE] (noting that the Department of Defense uses the Internet for a myriad of its requirements from travel payments to satellite communications to electronic commerce, as well as for direct warfighting).

6. Cryptography is the "[a]rt or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form." Director of Central Intelligence Directive 6/3, Protecting Sensitive Compartmented Information Within Information Systems ¶ E (June 5, 1999), available at http://www.fas.org/irp/offdocs/DCID_6-3_20Policy.htm [hereinafter CIA Directive]. Another definition of cryptography is the "[s]cience of encrypting plain data and information into a form intelligible only to authorized persons who are able to decrypt it." U.S. CRITICAL INFRASTRUCTURE ASSURANCE OFFICE, PRACTICES FOR SECURING CRITICAL INFORMATION ASSETS 53 (2000). The process by which that information is made unintelligible is "encryption." See SIMON SINGH, THE CODE BOOK: THE SCIENCE OF SECRECY FROM ANCIENT EGYPT TO QUANTUM CRYPTOGRAPHY 6 (1999) ("The aim of cryptography is not to hide the existence of a message, but rather to hide its meaning, a process known as *encryption*."). For a discussion of the ancient roots of encrypted and secret communications, see *id.* at 3-14. Some see encrypted, secret communications as a constitutionally protected "ancient liberty." See generally John A. Fraser, III, *The Use of Encrypted, Coded and Secret Communication Is an "Ancient Liberty" Protected by the United States Constitution*, 2 VA. J.L. & TECH. 2 (1997), at http://vjolt.student.virginia.edu/graphics/vol2/home_art2.html.

This article will not address the rights of sovereign states to encrypt and hide information from other states, nor the legality of states' attempts to obtain such concealed information. For a discussion of the legality of the espionage under international norms, see Ingrid Delupis, *Foreign Warships and Immunity for Espionage*, 78 AM. J. INT'L L. 53, 61-70 (1984); Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 321 (1996); Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F. L. REV. 217 (1999).

7. See *infra* notes 34-61 and accompanying text. This increased dependence on computers and computer networks has opened the United States to new vulnerabilities—the U.S. military alone has at least 2.1 million computers and 10,000 local area networks. Michael N. Schmitt, *Bellum Americanum: The U.S. View of Twenty-First Century War and Its Possible Implications for the Law of Armed Conflict*, 19 MICH. J. INT'L L. 1051, 1063 n.53 (1998) (citing Thomas E. Ricks, *Information-Warfare Defense Is Urged*, WALL ST. J., Jan. 6, 1997, at B2); see also Joginder S. Dhillon & Robert I. Smith, *Defensive Information Operations and Domestic Law: Limitations on Government Investigative Techniques*, 50 A.F. L. REV. 135, 143-44 (2001).

8. The law of armed conflict (LOAC) is defined as "[t]hat part of international law that regulates the conduct of armed hostilities." DEP'T OF DEF., DICTIONARY OF MILITARY AND ASSOCIATED TERMS, Joint Pub. 1-02 (as amended through Dec. 19, 2001), available at

regarding the legality of transmission and reception of such encrypted data by military medical facilities.⁹ If such transmissions do violate LOAC, this may ultimately subject those facilities to attack and destruction during armed conflict.

This article begins with an overview of the origins of electronic data transmission and key concepts underlying computer networks, followed by a discussion of the Department of Defense's (DOD) information infrastructure, including networks that transmit classified, encrypted information. Next, it examines the present status of military medical facilities under LOAC. It will discuss when and how these medical facilities may lose their protected status. The article then discusses principles of treaty interpretation and their application to the question of encrypted communications originating from or received by these facilities. It then examines, in light of these principles, whether these facilities' use of DOD classified computer networks transmitting encrypted data affects their status under LOAC. The article concludes that encrypted communications to and from land-based medical treatment facilities alone are insufficient to compromise their status under LOAC in its current state. However, the article recommends that observers from outside the United States government be permitted to verify

<http://www.dtic.mil/doctrine/jel/doddic/> [hereinafter DOD DICTIONARY]. LOAC rests on four basic principles, derived from customary international norms and treaties: "military necessity" or "military objective" (attacks may be made only against those targets which are valid military objectives), "humanity" or "unnecessary suffering" (attacks should not employ arms, projectiles, or material calculated to cause unnecessary suffering); "proportionality" (anticipated loss of life and damage to property incidental to attacks must not be excessive in relation to the concrete and direct military advantage expected to be gained); and "discrimination" or "distinction" (attacks must distinguish combatants from noncombatants and military objectives must be distinguished from protected property or protected places). OPERATIONAL LAW HANDBOOK 8-10 (Jeanne M. Meyer & Brian J. Bill eds., 2002). For a thorough survey of the sources and principles underlying LOAC, as well as international law in general, see Robert A. Ramey, *Armed Conflict on the Final Frontier: The Law of War in Space*, 48 A.F. L. REV. 1, 28-63 (2000).

9. At least one author has wondered about the transmission of Internet messages from hospital ships of neutral parties and the effect such messages may have on belligerent parties if not transmitted "in the clear." See George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1079, 1188 (2000).

What about generally exempt ships, such as hospital ships not aiding an enemy, that send Internet-based messages that might be construed by a belligerent to be encrypted messages? Would this raise suspicions, however unfounded, such that neutral exempt vessel use of Internet-based messages should be banned or restricted? Can system segregation be done with today's technology?

Id.

This article will address the legality of such transmissions from all military medical facilities under international law. But rather than the perspective of the neutral party, the article will examine the perspective of co-belligerents and what, if any, response belligerent parties may take against the opposing side's medical facilities under such a scenario.

that the networks transmitting data to and from such facilities are used solely for medical information.

II. ORIGINS OF ELECTRONIC DATA TRANSMISSION AND NETWORKING

The ancestor of modern electronic information networks is the telegraph system. Its roots stretch back to 1753 when an anonymous letter published in a Scottish magazine described how a message could be sent great distances by connecting the sender and the receiver with twenty-six cables (one for each letter of the alphabet) and sending electrical impulses down wires.¹⁰ Although in limited use prior to 1844,¹¹ Samuel Morse's transmission between Washington, D.C., and Baltimore, Maryland, helped to demonstrate the practicality of the telegraph¹² and catalyze its rapid spread across the United States and Europe.¹³ Voice transmission via cable¹⁴ and eventually radio and television followed, heralding further revolution in telecommunications.¹⁵ It was not until the 1960s, however, that the concepts underlying computer networking were articulated.¹⁶

10. SINGH, *supra* note 6, at 60-61.

11. For an account of telegraphs prior to Samuel Morse's, see Transatlantic Cable Communications, *The Invention of the Telegraph*, at <http://collections.ic.gc.ca/cable/invent.htm> (last visited Jan. 28, 2002) [hereinafter *Telegraph*] (discussing a type of telegraph built in Switzerland as early as 1774). See also SINGH, *supra* note 6, at 60-61; Invention Dimension, *Samuel F.B. Morse: Morse Code*, at <http://web.mit.edu/invent/www/inventorsIQ/morse.html> (last modified Jan. 2000).

12. The advantage to Morse's telegraph was that it used an electromagnet to enhance the signal "so that upon arriving at the receiver's end it was strong enough to make a series of short and long marks, dots and dashes, on a piece of paper." SINGH, *supra* note 6, at 61.

13. "By 1854, there were 23,000 miles of telegraph wire in operation [in the United States alone]." *Telegraph*, *supra* note 11.

14. Invention Dimension, *Alexander Graham Bell: The Telephone*, at http://web.mit.edu/invent/www/inventorsA-H/graham_bell.html (last modified Sept. 2000). Alexander Graham Bell placed the world's first telephone call over telegraph wires between two towns in Ontario, Canada, in 1877. *Id.*

15. See Jeff Madrik, *Economic Scene: Government's Role in the New Economy Is Not a Cheap or Easy One*, N.Y. TIMES, May 11, 2000, at C2.

16. See Barry M. Leiner et al., *A Brief History of the Internet*, at <http://www.isoc.org/internet/history/brief.shtml> (last revised Aug. 4, 2000) [hereinafter *Internet*]. J.C.R. Licklider of the Massachusetts Institute of Technology wrote a series of memos in August 1961 envisioning "a globally interconnected set of computers through which everyone could quickly access data and programs from any site." *Id.* Many have written extensively on the growth and development of the computer networks that came to be known as the Internet, so a review of its history is outside the scope of this article. Instead, this article will emphasize some fundamental concepts underlying computer networks. For a discussion of the history and current structure of the Internet as well as emerging threats in information warfare, see Walker, *supra* note 9, at 1094-1107.

A key concept underlying what would become the Internet is that of “open architecture networking,”¹⁷ i.e., a network that was not designed for just one application but rather as a general infrastructure on which new applications could be conceived.¹⁸ “In this approach, the choice of any individual network technology was not dictated by a particular network architecture but rather could be selected freely by a provider and made to interwork with the other networks through a meta-level ‘Internetworking Architecture.’”¹⁹ Early in the history of the Internet, it became clear that for networks with different technologies and architectures to communicate with one another efficiently, improved data transmission standards and protocols²⁰ had to be developed.²¹ To address this issue, Robert E. Kahn and Vinton G. Cerf developed Transmission Control Protocol/Internet Protocol (TCP/IP) in the early 1970s.²²

TCP/IP is a two-level program: the first level, TCP, directs the assembly of a message or file into data “packets” that are transmitted individually over the Internet and received by a TCP layer that reassembles the packets into the original message.²³ The second level, IP, handles the address portion of each packet so that it arrives at the correct destination.²⁴ As the packets arrive at a gateway,²⁵ a router²⁶ directs the packets via a switch, which provides the actual path in and out of a gateway for a given packet.²⁷ Thus, in packet switched communications, a message from one computer to another is broken up into discrete “packets” of data, each of which carries a destination label, as well as instructions for where the packets fit in the overall message.²⁸

17. See Barry M. Leiner et al., *The Initial Internetworking Concepts*, at http://www.isoc.org/internet/history/brief.shtml#Initial_Concepts, in *Internet*, *supra* note 16.

18. *Id.*

19. *Id.*

20. “In information technology a protocol . . . is the special set of rules that end points in a telecommunication connection use when they communicate.” Whatis.com, *Protocol*, at http://whatis.techtarget.com/definition/0,289893,sid9_gci212839,00.html (last updated May 22, 2001) [hereinafter *Protocol*].

21. Leiner et al., *supra* note 17.

22. *Id.*

23. Whatis.com, *Packet*, at http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212736,00.html (last updated Jul. 31, 2001).

24. *Id.*

25. A “gateway” is an “interface between networks.” U.S. CRITICAL INFRASTRUCTURE ASSURANCE OFFICE, *supra* note 6, at 54.

26. A “router” is “[a] device that connects two networks or network segments and may use IP to route messages.” *Id.* at 57.

27. Whatis.com, *Gateway*, at http://whatis.techtarget.com/definition/0,289893,sid9_gci212176,00.html (last updated Aug. 16, 2001).

28. George Johnson, *From Two Small Nodes, a Mighty Web Has Grown*, N.Y. TIMES, Oct. 12, 1999, at F1.

This “packet switching” method represents a tremendous technical shift from the older circuit switched model of data transmission.²⁹ For example, “in an ordinary telephone system two phones were linked by forming a temporary circuit, a dedicated physical channel through which electrified voices flowed.”³⁰ Since the message is broken down into many different packets, each one could take a different path over the network, and no matter in what sequences the data packets arrived, they could be assembled to re-form the original message.³¹ There are certain advantages to this method of data transmission: first, there is no need to dedicate a circuit to a single transmission, since many data packets can stream down each individual circuit; second, since messages are broken into small fragments, the data flow is smoother; third, if a packet is corrupted, one can simply re-send the packet and not the entire message; fourth, such a network is much less vulnerable to failure, since packets may follow alternate routes to arrive at their destination.³² As the standard data transmission protocol, TCP/IP is at the core of computer networking and is indispensable to the Internet and any packet switched router network today, including those maintained by the DOD.³³

III. DEPARTMENT OF DEFENSE INFORMATION INFRASTRUCTURE

The Defense Information Systems Agency (DISA) is the DOD agency charged with the overall management of the Defense Information Infrastructure (DII).³⁴ “The DII is the web of communications networks, computers, software, databases, applications, weapon system interfaces, data, security services, and other services that meet the information processing and transport needs of DOD users, across the range of military operations.”³⁵ The Defense Information Systems Network (DISN) is a sub-element of the DII and is “DOD’s consolidated worldwide enterprise level telecommunications infrastructure that provides the end-to-end information transfer network for

29. “Leonard Kleinrock at MIT published the first paper on packet switching theory in July 1961 and the first book on the subject in 1964.” Barry M. Leiner et al., *Origins of the Internet*, at <http://www.isoc.org/internet/history/brief.shtml#Origins>, in *Internet*, *supra* note 16.

30. Johnson, *supra* note 28, at F1.

31. *Id.*

32. *Id.*

33. Katie Hafner, *For ‘Father of the Internet,’ New Goals, Same Energy*, N.Y. TIMES, Sept. 25, 1994, at 4.

34. Defense Information Systems Agency, *DISA Mission and Mandate*, at <http://www.disa.mil/main/missman.html> (last revised Oct. 1, 2001).

35. DEFENSE INFORMATION SYSTEMS AGENCY, DEFENSE INFORMATION INFRASTRUCTURE MASTER PLAN § 2.2 (version 7.0 Mar. 13, 1998), available at <http://www.disa.mil/diimp/diimp-2.html> [hereinafter INFRASTRUCTURE].

supporting military operations.”³⁶ The DISN is, in turn, composed of several sub-networks, employing primarily IP and Asynchronous Transfer Mode³⁷ technology.³⁸ The Secret Internet Protocol Router Network (SIPRNet) and the Non-Classified but Sensitive Internet Protocol Router Network (NI-PRNet) are IP subsets of the DISN.³⁹

Taken together, these two data networks provide the essential information necessary to conduct and support the full range of military operations, and [to] support [United States] warfighters, the Office of the Secretary of Defense, the Joint Chiefs of Staff, the Commanders-in-Chief, the Military Services, the Defense Agencies, and other Federal Agencies.⁴⁰

The SIPRNet is a secret-level⁴¹ packet switch network that uses Internet protocol routers and high-capacity DISN circuitry to route data.⁴² It is a

36. Defense Information Systems Agency, *DISN Architecture: Defense Information Infrastructure* § 1.3, at <http://www.disa.mil/DISN/disnar1.htm/disnar1.html> (last revision Mar. 2001).

37. Asynchronous Transfer Mode (or “ATM”) is “a dedicated-connection switching technology that organizes digital data into 53-byte cell units and transmits them over a physical medium using digital signal technology.” Whatis.com, *ATM*, at http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213790,00.html (last updated Aug. 16, 2001).

38. DEFENSE INFORMATION SYSTEMS AGENCY, DISA CIRCULAR NO. 310-55-9, BASE LEVEL SUPPORT FOR THE DEFENSE INFORMATION SYSTEMS NETWORK (DISN) ¶¶ C.1.1.1-2 (Nov. 5, 1999), available at <http://www.disa.mil/pubs/circulars/dc310559.pdf>.

39. *DOD Networks; Government Activity*, GOV’T COMPUTER NEWS, Sept. 11, 2000, at 67; see also INFRASTRUCTURE, *supra* note 35, § 2.4.2. The Joint Worldwide Intelligence Communications System (JWICS) is or soon will be a component of the DISN. See Federation of American Scientists, *Joint Worldwide Intelligence Communications System [JWICS]*, at <http://www.fas.org/irp/program/disseminate/jwics.htm> (updated Jan. 18, 1999) [hereinafter JWICS]; see also Chairman of the Joint Chiefs of Staff Instruction 6211.02A, Defense Information System Network and Connected Systems, ¶ 1.d. (May 22, 1996), available at http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/6211_02a.pdf. JWICS is the router network designed to carry data designated TS/SCI, or Top Secret/Sensitive Compartmented Information. See JWICS, *supra*. For definitions of information sensitivity level designations used by the United States Government, see *infra* note 41.

40. *Hearing Before the House Armed Servs. Comm., Subcomm. on Readiness*, 107th Cong. (May 17, 2001) (prepared testimony of Major General James D. Bryan), available at LEXIS Federal News Service [hereinafter *Bryan Testimony*].

41. The United States Government generally uses three basic terms to classify the sensitivity of information under its control. The lowest level of classification is termed “confidential;” the next highest is “secret;” followed by “top secret.” The classification level of the information is based on the expected damage to United States national security if there were an unauthorized disclosure of the data. Information is classified as “secret” when the unauthorized revelation of the information would be expected to cause “serious damage” to United States national security. See Exec. Order No. 12,958, 60 Fed. Reg. 19,825 (Apr. 17, 1995). The additional designation “sensitive compartmented information” means “[c]lassified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems estab-

worldwide network replacing an older packet-switched network (the Defense Secure Network One (DSNET 1) of the Defense Data Network (DDN)); the initial SIPRNet backbone was activated on March 3, 1994.⁴³ SIPRNet uses TCP/IP protocol service,⁴⁴ and subscribers in both the DOD as well as within other government agencies can use the SIPRNet to transfer information at the classification level of Secret-Not Releasable to Foreign Nationals (SECRET-NOFORN).⁴⁵

The SIPRNet's role is to support national defense command, control, communications, and intelligence (C3I) requirements.⁴⁶ It is used as the underlying transmission infrastructure for the Global Command and Control System (GCCS)⁴⁷ and, in the future, will be used for certain portions of the Global Combat Support System (GCSS).⁴⁸ The SIPRNet is also used "for force projection, for reporting situational awareness, for intelligence purposes, to distribute Air Tasking Orders, for support of drug enforcement operations and for nuclear assurance."⁴⁹ As of May 2001, the SIPRNet

lished by the Director of Central Intelligence." CIA Directive, *supra* note 6.

42. DOD DICTIONARY, *supra* note 8 (defining "Secret Internet Protocol Router Network").

43. Federation of American Scientists, *Secret Internet Protocol Router Network (SIPRNET)*, at <http://www.fas.org/irp/program/disseminate/siprnet.htm> (updated Mar. 3, 2000) [hereinafter FAS, *SIPRNET*]. Prior to 1994, DOD data transmission networks were organized as follows: Military Network (MILNET) for unclassified traffic; DSNET 1 for secret traffic; DSNET 2 for top secret traffic; and DSNET 3 for TS/SCI. *Evolution of Data Services—Corrected Version*, DEF. DATA NETWORK NEWSL. (DDN Network Info. Ctr.), Nov. 3, 1994, at 1, available at <http://www.nic.mil/ftp/mgt/news9409.txt>.

44. The SIPRNet also supports File Transfer Protocol (FTP), Telnet, Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP). Defense Information Systems Agency, *Secret Internet Protocol Router Network (SIPRNET)*, at <http://www.inmspac.disa.mil/siprnet.html> (last revised Jan. 30, 2001) [hereinafter DISA, *SIPRNET*].

45. FAS, *SIPRNET*, *supra* note 43.

46. *Id.*

47. Defense Information Systems Agency, *Global Command & Control System (GCCS) Overview*, at <http://gccs.disa.mil/gccs/overview.html> (last modified June 19, 2000). The GCCS is

the Department of Defense's computerized system of record for strategic command and control functions GCCS provides combatant commanders one predominant source for generating, receiving, sharing and using information securely. It provides surveillance and reconnaissance information and access to global intelligence sources as well as data on the precise location of dispersed friendly forces.

Id.

48. JOINT CHIEFS OF STAFF, CAPSTONE REQUIREMENTS DOCUMENT: GLOBAL COMBAT SUPPORT SYSTEM 7 (June 5, 2000), available at <http://www.dtic.mil/jcs/j4/projects/gcss/crdjrocflag.doc>. The GCSS is the DOD logistics network, and supports the GCCS. See Defense Information Systems Agency, *GCSS Executive Summary*, at <http://www.disa.mil/gcss/execsum.html> (updated Aug. 13, 2001).

49. *Bryan Testimony*, *supra* note 40, ¶ 8. An air tasking order is a "method used to task and disseminate to components, subordinate units, and command and control agencies pro-

served approximately 125,000 personnel over 901 post, camp and station connections, and since 1996, there has been a 200% increase in customers and over 600% in traffic.⁵⁰ According to Major General James D. Bryan, the SIPRNet “has become the most critical data system supporting the war-fighter today.”⁵¹

The security and integrity of this network are of great concern for the United States military, and the network is constantly monitored.⁵² Therefore, the SIPRNet is separated both physically and logically from other computer networks.⁵³ In fact, all SIPRNet nodes⁵⁴ are “housed in United States Military facilities protected to the Secret level.”⁵⁵

jected sorties, capabilities and/or forces to targets and specific missions. Normally provides specific instructions to include call signs, targets, controlling agencies, etc., as well as general instructions.” DOD DICTIONARY, *supra* note 8.

50. *Bryan Testimony*, *supra* note 40, ¶ 8.

51. *Id.*; see also F. WHITTEN PETERS, REPORT OF THE SECRETARY OF THE AIR FORCE, available at <http://www.dtic.mil/execsec/adr2000/af.html> (last visited Mar. 6, 2002). For specific examples of the SIPRNet’s effects on United States military operations around the globe, see *Hearing Before the House Armed Servs. Comm., Subcomms. on Military Readiness and Research and Development*, 106th Cong. (Mar. 8, 2000), available at LEXIS Federal News Service (noting that “during Operation Allied Force in Serbia and Kosovo, the SIPRNet . . . literally replaced regular naval messages as the primary means for communication and coordination among our staffs and ships”).

52. Security on both the NIPRNet and the SIPRNet is maintained by DISA’s Global Network Operations & Security Center, which is manned twenty-four hours a day, seven days a week. Defense Information Systems Agency, *Fact Sheet: Global Network Operations and Security Center (GNOSC) Command Center*, at <http://www.disa.mil/info/fsgnosc.html> (last revision June 14, 2000).

53. DISA, *SIPRNET*, *supra* note 44; see also George I. Seffers, *Fit to Fight the Info War? Critics Say Proposed Test of DOD IT Networks Is Unrealistic*, FED. COMPUTER WK. (Mar. 12, 2001), at <http://www.fcw.com/fcw/articles/2001/0312/news-iwar-03-12-01.asp>. Seffers quoted a joint statement from the Office of the Secretary of Defense and DISA highlighting the security of SIPRNet:

The SIPRNET is a closed system; the Internet is not. The SIPRNET uses protected distribution systems; the Internet does not. Information flowing on the SIPRNET is encrypted; most on the Internet is not. Users on the SIPRNET must be vouchsafed on to the network; users on the Internet need not be.

Some see physical separation between the SIPRNet and other networks as a key to its security. See *Campbell: Keep SIPRNet Separate from NIPRNet*, GOV’T COMPUTER NEWS, July 24, 2000, at 50. However, the separation between the SIPRNet and other networks may be blurred. See Bill Murray, *U.S. Peacekeepers Use Net to Access Classified Network*, GOV’T COMPUTER NEWS, May 15, 2000, at 40 (noting that United States peacekeepers in East Timor arranged for access to the SIPRNet through the Internet); News Release, United States Navy, SPAWAR Information Security Group Scores a First (Mar. 13, 2001), available at <http://enterprise.spawar.navy.mil/spawarpublicsite/docs/nr-2001-013.pdf> (noting success in using bridge method via “Trusted Guard” system to transmit sensitive unclassified personnel data to the Global Command and Control System located on the SIPRNet).

54. A node is a redistribution point or end point for data transmission, and, in general, a

Due to this physical separation from public data networks, hacking into the SIPRNet from a computer not already vouched onto the network would appear to be virtually impossible; thus the SIPRNet has apparently never been compromised by external intruders.⁵⁶ A more likely scenario than external hacking is that of authorized users themselves compromising the SIPRNet's security,⁵⁷ especially in light of its large number of users.⁵⁸ Nevertheless, one can imagine a situation where interception and decryption of the data in transit may be possible, either by tapping into the transmission cables or network nodes, or by installing covert access points surreptitiously.⁵⁹ However, given the technical and logistical difficulties of such endeavors, this type of network breach would require significant resources.⁶⁰

Moreover,

[A]ll SIPRNet-connected systems must first go through certification to determine that they are secure. . . . All links between SIPRNet hosts are encrypted. Not only is the data encrypted at the host level, but any cir-

node has the capability to recognize and process or forward data to other nodes. Whatis.com, *Node*, at http://whatis.techtarget.com/definition/0,289893,sid9_gci212665,00.html (last updated Nov. 23, 1999).

55. *Bryan Testimony*, *supra* note 40, ¶ 9.

56. Heather Harreld & Bob Brewin, *Pentagon Denies Hacker Penetrated Secret Nets*, FED. COMPUTER WK. (Apr. 27, 1998), at http://www.fcw.com/fcw/articles/1998/FCW_042798_380.asp.

57. This may have already happened. See James W. Crawley, *Navy Officer Is Subject of Security Probe*, SAN DIEGO UNION-TRIB., Nov. 23, 2000, at B-3:7 (reporting that a naval officer's personal computing equipment was seized by federal agents after he stated that he had downloaded classified information from SIPRNet onto various computer disks).

58. See *supra* text accompanying note 50. In fact, the large number of users has been an ongoing source of concern. See Daniel Verton, *DOD Taking Steps to Secure Secret Network Further*, FED. COMPUTER WK. (May 5, 1999), at http://www.fcw.com/fcw/articles/1999/fcw_551999_pki.asp ("Looking to protect its classified information network from internal security threats, the Defense Department is considering a new policy that will limit strictly network users' access to information.").

59. Such endeavors are by no means unprecedented. See Lawrence D. Sloan, *Echelon and the Legal Restraints on Signals Intelligence: A Need for Reevaluation*, 50 DUKE L.J. 1467, 1477 n.46 (2001) (citing SHERRY SONTAG & CHRISTOPHER DREW, *BLIND MAN'S BLUFF: THE UNTOLD STORY OF AMERICAN SUBMARINE ESPIONAGE* 171-72 (1998), which describes the submarine USS *Halibut's* successful mission to tap into an undersea Soviet military communications line in October 1971).

60. Nevertheless, this may have occurred. See Bill Gertz & Rowan Scarborough, *Inside the Ring*, WASH. TIMES, Mar. 30, 2001, at A10 (stating that federal officials were investigating whether FBI agent Robert P. Hanssen, accused of spying for Russia, may have aided Russian intelligence in placing secret access points on the SIPRNet allowing covert access to the network).

cuits linking a classified host to a SIPRNet router are encrypted, as are router-to-router links across the DISN wide area network.⁶¹

Granting access to the SIPRNet to most, if not all, military units appears increasingly likely, given its expanding role and indeed that of encrypted communications in general for military operations. Encryption, however, is not limited to the SIPRNet, or even to classified networks. The use of encryption for all DOD electronic communications may come to pass in the near future. According to a White House report, by October of 2001, the encryption of all e-mail throughout the DOD should be encouraged, and no separate policy was noted for medical facilities.⁶²

For example, the Theater Medical Information Program (TMIP) is a joint-services information system whose

primary purpose is to integrate/develop medical information systems to capture the medical record and link all theater levels of care in an integrated, interoperatable fashion to provide enhanced medical care to the warfighter. TMIP's software will be used on the [GCCS/GCSS] backbone and Service computer/communications infrastructure allowing the warfighter to monitor and maintain Theater medical situational awareness.⁶³

Even beyond any encryption solely incidental to TMIP's use of the GCCS/GCSS as part of the SIPRNet, TMIP will specifically encrypt electronic transmissions of patient medical information.⁶⁴

Such transmission of encrypted data by military medical facilities raises legal questions under international law. If these transmissions violate LOAC, this may render such facilities lawful military targets under certain conditions. To determine under what, if any, circumstances such transmissions may violate international law of armed conflict, an examination of the protections accorded military medical facilities and their limitations is necessary.

61. William Dutcher, *NIPRnet Keeps Secrets, Too*, GOV'T COMPUTER NEWS, Aug. 26, 1996, at 59.

62. DEFENDING AMERICA'S CYBERSPACE, *supra* note 5, at 94.

63. *Theater Medical Information Program*, at <http://tmip.hirs.osd.mil> (last visited Mar. 4, 2002).

64. CAPSTONE REQUIREMENTS DOCUMENT FOR THE THEATER MEDICAL INFORMATION PROGRAM para. 4.4.2 (Feb. 25, 1999), available at http://tmip.hirs.osd.mil/Mission/CRD_v1.pdf [hereinafter TMIP CAPSTONE REQUIREMENTS] ("Appropriate encryption devices will be used to protect the electronic transfer of patient medical information between major information transfer points.").

IV. PROTECTIONS FOR MEDICAL FACILITIES IN ARMED CONFLICT

Since antiquity, norms of warfare have included the idea that certain places and properties should not be subject to attack and destruction.⁶⁵ Medical facilities on land, sea, and (in the twentieth century) in the air are part of this traditional protected sphere. The protection of fixed as well as mobile medical facilities and units is recognized in Article 19 of the Geneva Convention I for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, which states that “[f]ixed establishments and mobile medical units of the Medical Service may in no circumstances be attacked, but shall at all times be respected and protected by the Parties to the conflict.”⁶⁶ Medical aircraft are also protected from attack.⁶⁷ Protection for medical ships is contained in Article 22 of the Geneva Convention II for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, which states that such ships, “built or equipped by the Powers specially and solely with a view to assisting the wounded, sick and shipwrecked, to treating them and to transporting them, may in no circumstances be attacked.”⁶⁸ The protection covers the sick-bay areas on warships, as well as shore support establishments protected under Geneva Convention I.⁶⁹

These protections may be lost if these facilities are used to commit acts—outside their humanitarian duties—which are “harmful to the enemy.”⁷⁰ Even in such instances, protection may only cease after due warning has been given, naming, in all appropriate cases, a reasonable time for

65. For a survey of the roots of this idea in Western thought from ancient Greece through the twentieth century, see Joshua E. Kastenberg, *The Legal Regime for Protecting Cultural Property During Armed Conflict*, 42 A.F. L. REV. 277, 281-97 (1997); see also DAVID J. BEDERMAN, *INTERNATIONAL LAW IN ANTIQUITY* 249-55 (2001) (discussing the protection of sacred places and persons from effects of combat). There are a number of “Geneva Conventions” on the laws of war, dating from 1864. See International Committee of the Red Cross, *International Humanitarian Law: Answers to Your Questions*, Questions 2-3, available at <http://www.icrc.org>. This article will focus on two of the Geneva Conventions following World War II that deal with protections accorded to the wounded and sick on land and at sea. See *infra* notes 66-76 and accompanying text.

66. Geneva Convention for the Amelioration of the Condition of Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, art. 19, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter Geneva Convention I].

67. *Id.* at art. 36. The term “medical aircraft” means “aircraft exclusively employed for the removal of wounded and sick and for the transport of medical personnel and equipment” *Id.*

68. Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, art. 22, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter Geneva Convention II].

69. *Id.* at arts. 23, 28.

70. Geneva Convention I, *supra* note 66, art. 21; Geneva Convention II, *supra* note 68 art. 34; see *infra* text accompanying note 72.

compliance, and after such warning has been unheeded.⁷¹ Although the Geneva Conventions do not specifically define “acts harmful to the enemy,” the International Committee of the Red Cross interprets these acts to mean “acts the purpose or effect of which is to harm the adverse Party, by facilitating or impeding military operations.”⁷²

The language in both Geneva Conventions regarding acts “outside their humanitarian duties” is crucial, since “it is possible for humane acts to be harmful to the enemy, or for [them] to be wrongly interpreted as so being by an enemy lacking in generosity.”⁷³ Hypothetical examples of actions that, although possibly harmful to the enemy, are still within medical facilities’ humanitarian duties include interference with tactical enemy operations solely by virtue of their mere presence (i.e., the effect of their lights at night on targeting) and electromagnetic interference with enemy transmissions stemming from the use of medical equipment.⁷⁴

The commentaries to these Geneva Conventions also provide examples of acts that render medical units subject to warning and attack. These include, in the case of medical ships, “carrying combatants or arms, transmitting military information by radio, or deliberately providing cover for a warship,”⁷⁵ and in the case of mobile or fixed medical units include “the use of a hospital as a shelter for able-bodied combatants or fugitives, as an arms or ammunition dump, or as a military observation post; [or] . . . the deliberate siting of a medical unit in a position where it would impede an enemy attack.”⁷⁶

71. Geneva Convention I, *supra* note 66, art. 21; Geneva Convention II, *supra* note 68, art. 34.

72. International Committee of the Red Cross, *Commentaries to Geneva Convention I for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, art. 21, at 200 (Aug. 12, 1949), available at <http://www.icrc.org/ihl.nsf/WebComART?OpenView> [hereinafter *Commentaries to Geneva Convention I*]; International Committee of the Red Cross, *Commentaries to Geneva Convention II for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea*, art. 34, at 190-91 (Aug. 12, 1949), available at <http://www.icrc.org/ihl.nsf/WebComART?OpenView> [hereinafter *Commentaries to Geneva Convention II*].

73. *Commentaries to Geneva Convention I*, *supra* note 72, art. 21, at 201; see also *Commentaries to Geneva Convention II*, *supra* note 72, art. 34, at 191. In fact, without this language, an adverse party could theoretically argue that medical treatment of the opposing side’s own forces constitutes a harmful act, since the obvious goal of medical treatment is to render a wounded soldier capable of fighting once more.

74. *Commentaries to Geneva Convention I*, *supra* note 72, art. 21, at 201; see also *Commentaries to Geneva Convention II*, *supra* note 72, art. 34, at 191.

75. *Commentaries to Geneva Convention II*, *supra* note 72, art. 34, at 191.

76. *Commentaries to Geneva Convention I*, *supra* note 72, art. 21, at 200-01.

V. TREATY INTERPRETATION AND THE LEGALITY OF ENCRYPTED TRANSMISSIONS FROM MILITARY MEDICAL FACILITIES

It is significant that although there is a direct prohibition on the possession or use of a "secret code" by medical ships in Geneva Convention II,⁷⁷ there is no such restriction on fixed or mobile land-based medical facilities in Geneva Convention I. In order to cultivate an informed discussion of meaning and effect of the lack of such a clause, a brief review of treaty interpretation principles is necessary.⁷⁸ The methods of treaty interpretation used by United States courts generally rest on three canons: begin interpretation with the treaty's text, construe treaties liberally and in good faith, and effectuate the intent of the parties.⁷⁹ When commencing an analysis of language in international agreements, United States courts are most often guided by principles of statutory and contract interpretation.⁸⁰ The starting

77. Geneva Convention II, *supra* note 68, art. 34. The commentaries to Article 34 state: The fact that the use of any secret code is prohibited affords a guarantee to the belligerents that hospital ships will not make improper use of their transmitting apparatus or any other means of communication. Hospital ships may only communicate in clear, or at least in a code which is universally known, and rightly so, for the spirit of the Geneva Conventions requires that there should be nothing secret in their behaviour vis-à-vis the enemy.

Commentaries to Geneva Convention II, art. 34, *supra* note 72, at 193. Interestingly, "the equally authentic Spanish and French texts of this article prohibit only the sending . . . of encrypted traffic." J. Ashley Roach, *The Hague Peace Conferences: The Law of Naval Warfare at the Turn of Two Centuries*, 94 AM. J. INT'L L. 64, 75 (2000).

78. This analysis begins with treaty interpretation from the standpoint of American jurisprudence before looking to international law.

79. David J. Bederman, *Revivalist Canons and Treaty Interpretation*, 41 UCLA L. REV. 953, 964-70 (1994). The search for basic principles of treaty interpretation is no small task "because a court's selection of an interpretative method for construing any legal instrument (whether a contract, statute, or treaty) is often driven by the substantive result desired." *Id.* at 956. Moreover, United States courts "frequently apply different substantive canons of construction to different kinds of treaties," depending on whether the treaty is characterized as contractual, legislative, or "something altogether sui generis." *Id.* at 963. The basic philosophies of treaty interpretation are the "textual approach," emphasizing the "plain and natural meaning" of the treaty text; the "limited contextual approach," which puts primacy on the treaty text, but is willing to look at extrinsic materials; and the "policy oriented and configurative" approach, which looks to effectuate the intentions of the parties wherever those may be found, both within the treaty text and outside it. BURNS H. WESTON, RICHARD A. FALK, & ANTHONY D'AMATO, *INTERNATIONAL LAW AND WORLD ORDER* 59-62 (2d ed. 1990).

80. *Iceland S.S. Co. v. United States Dep't of the Army*, 201 F.3d 451, 458 (D.C. Cir. 2000); *see, e.g., Fong Yue Ting v. United States*, 149 U.S. 698, 720 (1893) ("A treaty, it is true, is in its nature a contract between nations . . ."); *The Chinese Exclusion Cases*, 130 U.S. 581, 600 (1889) (same); *Edye v. Robertson*, 112 U.S. 580, 598 (1884) ("A treaty is primarily a compact between independent nations."). Whether the emphasis is on contractual or statutory interpretation principles depends on whether the treaty has the flavor of legislation or contract. Bederman, *supra* note 79, at 963. For a discussion of the limits to the contract analogy and consideration of whether law and economics contractual analysis can be

point for interpretation of any treaty is the language of the treaty itself.⁸¹ The plain language of the treaty is controlling unless "application of the words of the treaty according to their obvious meaning effects a result inconsistent with the intent or expectations of its signatories."⁸² These principles are generally consistent with international norms regarding treaty interpretation.⁸³

Closely related to the idea of plain language as primary interpretive device is the maxim "expressio unius est exclusio alterius." Simply put, this axiom states that "where a form of conduct, the manner of its performance and operation, and the persons and things to which it refers are designated, there is an inference that all omissions should be understood as exclusions."⁸⁴ It, too, is applicable to treaty interpretation and is particularly illuminating in this context.⁸⁵ This axiom is not only an interpretive tool, it is also a basic rule of logic⁸⁶ and has been utilized for centuries.⁸⁷

applied to treaties in a meaningful way, see Jeffrey L. Dunoff & Joel P. Trachtman, *Economic Analysis of International Law*, 24 YALE J. INT'L LAW 1, 29-50 (1999).

81. *Iceland S.S. Co.*, 201 F.3d. at 458 (citing *Sumitomo Shoji Am., Inc. v. Avagliano*, 457 U.S. 176, 180 (1982)). Although this may be an obvious starting point for treaty interpretation, the Supreme Court has "[an] unfortunate tendency to deviate from the text . . . , despite [its] pronouncements that if a treaty's language is clear, no other means of interpretation may be employed." *Bederman*, *supra* note 79, at 965.

82. *Bederman*, *supra* note 79, at 966 (quoting *Maximov v. United States*, 373 U.S. 49, 54 (1963)). This is a longstanding principle of treaty interpretation under United States law:

But this intention [of the Parties to a treaty] is to be collected from the language they have used; if that be clear and plain, there is no room for interpretation; but, if ambiguous in itself, then the intention may be fairly collected from the object and circumstances of the stipulation in question. In a word, the treaty is to be executed as it is, and no new treaty to be made by the labour of exposition.

The Amiable Isabella, 19 U.S. (6 Wheat.) 1, 51 (1821). *But see* *Bederman*, *supra* note 79, at 965 (noting the Supreme Court's tendency to deviate even from the clear language of the treaty text).

83. *See generally* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 325 (1987) [hereinafter RESTATEMENT]; HENRY WHEATON, *ELEMENTS OF INTERNATIONAL LAW* § 287, at 365 (Richard Henry Dana, Jr., ed., 8th ed. 1866) ("Public treaties are to be interpreted like other laws and contracts."). However, United States courts have been less than consistent in the application of these principles. *See* *Bederman*, *supra* note 79, at 964. Some have noted that this "contract law" theory has its limitations because of structural differences between international and domestic law. *See* Detlev F. Vagts, *The United States and Its Treaties: Observance and Breach*, 95 AM. J. INT'L L. 313, 325 (2001) ("In domestic law the explanation for a contract's binding character is not to be found in the simple fact that the contract has been made but in the law of contracts.").

84. 2A NORMAN J. SINGER, *SUTHERLAND STATUTORY CONSTRUCTION* § 47:23 (6th ed. 2000 rev.); *see also id.* § 47:25 ("The maxim emphasizes the language of the statute and the inferences to be drawn from the way it is written. There is generally an inference that omissions are intentional.").

85. LORD ARNOLD DUNCAN MCNAIR, *LAW OF TREATIES* 400 (1961). As Lord McNair succinctly states, "[the maxim *expressio unius exclusio alterius*] would find a place in the logic of the nursery. If I agree that my brother may play with my railway engine and my

The Vienna Convention on the Law of Treaties provides additional guidance on treaty interpretation.⁸⁸ Although not in existence at the time Geneva Conventions I and II were drafted,⁸⁹ the Vienna Convention nevertheless does codify “some of the customary rules governing the interpretation of international treaties.”⁹⁰ Its hierarchy of principles is contained in Articles 31 through 33. The basic principle is contained in Article 31(1), which states that “[a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their con-

motor car, it is obvious that I have not given him permission to play with my model airplane.” *Id.* at 399-400. This maxim is also expressed as “*inclusio unius est exclusio alterius*,” “*expressum facit cessare tacitum*,” “*affermatio est exclusio alterius*,” and “*a contrario*.” *Id.* at 401-02.

86. *Id.* at 402 (citation omitted) (“The maxim *expressio unius est exclusio alterius* is a rule of both law and logic and applicable to the construction of treaties as well as municipal statutes and contracts.”). *But see* *Ford v. United States*, 273 U.S. 593, 611-12 (1927) (noting that this maxim requires caution in its application); MYRES S. MCDUGAL, HAROLD D. LASSWELL, & JAMES C. MILLER, *THE INTERPRETATION OF AGREEMENTS AND WORLD PUBLIC ORDER: PRINCIPLES OF CONTEXT AND PROCEDURE* 330-43 (1967) (critiquing the idea that “*expressio unius*” truly represents a rule of logic).

87. *See* MCNAIR, *supra* note 85, at 402-10 (discussing application of this concept in treaty interpretation in the eighteenth, nineteenth, and twentieth centuries). In fact, the Romans employed this principle, although perhaps not expressed in the formula “*expressio unius*,” to great effect: in a treaty between Rome and the Aetolians in 197 B.C., accomplished with the objective of breaking Macedonia’s power, “it was provided that all the movable property taken as booty should go to the Romans, the lands and conquered towns to the Aetolians.” 1 COLEMAN PHILLIPSON, *THE INTERNATIONAL LAW AND CUSTOM OF ANCIENT GREECE AND ROME* 407-08 (1911). Philip of Macedonia was defeated in Thessaly by Titus Quinticus and the Macedonian ambassadors sued for peace. *Id.* at 416. After Philip’s defeat, the Aetolians claimed the Thessalian cities in accordance with what they believed were the terms of their treaty. *Id.* at 408. Quinticus, however, argued that the clause on which this claim was based “spoke only of captured cities—whereas the states of Thessaly had surrendered of their own free will.” *Id.*; *see also* BEDERMAN, *supra* note 65, at 198.

88. *See* Vienna Convention on the Law of Treaties, May 23, 1969, 1155 U.N.T.S. 331 [hereinafter Vienna Convention].

89. The Vienna Convention is specifically not retroactive and therefore does not directly govern interpretation of Geneva Conventions I and II. *Id.* at art. 4. Nevertheless, the Vienna Convention’s provisions represent evidence of customary international law principles of treaty interpretation, and as such, would influence interpretive methods applied to the Geneva Conventions I and II. *See generally* Jonathan F. Charney, *International Agreements and the Development of Customary International Law*, 61 WASH. L. REV. 971, 975-76 (1986) (noting that Vienna Convention dominates law on international agreements).

90. Angela M. Bradley, *Opposing Interpretations of an International Treaty: The Anti-Ballistic Missile Treaty Controversy*, 2 CHI. J. INT’L L. 295, 297 (2001); *see also* RESTATEMENT, *supra* note 83, § 325 n.4. Although the United States has not ratified the Vienna Convention, “[m]any commentators believe that the Convention’s terms are nonetheless fully binding on the United States as customary international law.” Curtis A. Bradley & Jack L. Goldsmith, *Treaties, Human Rights, and Conditional Consent*, 149 U. PA. L. REV. 399, 424 (2000).

text and in the light of its object and purpose.”⁹¹ The context of a treaty includes “any agreement relating to the treaty which was made between all the parties in connexion with the conclusion of the treaty”⁹² as well as “any instrument which was made by one or more parties in connexion with the conclusion of the treaty and accepted by the other parties as an instrument related to the treaty.”⁹³ The Vienna Convention focuses on the text of international agreements; “[r]esort to extrinsic evidence of the parties’ intent . . . is meant to be only an exceptional occurrence”⁹⁴ when provisions are ambiguous or obscure or “interpretation according to Article 31 leads to a result which is manifestly absurd or unreasonable.”⁹⁵

Applying these principles to the Geneva Conventions I and II, it is clear that the plain text of Geneva Convention I contains no prohibition on land-based medical facilities using “secret codes.” There is nothing ambiguous about the lack of such a provision in and of itself.⁹⁶ Under the above articulated rules, there is no need to look outside the text of Geneva Convention I since it does not meet the threshold for textual ambiguity.⁹⁷ However, given the fact that these conventions were signed simultaneously

91. Vienna Convention, *supra* note 88, art. 31(1).

92. *Id.* at art. 31(2)(a).

93. *Id.* at art. 31(2)(b). Subsequent agreement of the parties regarding interpretation of treaty provisions, subsequent practice of the parties, and any relevant rules of international law are also taken into account, together with the context. *Id.* at art. 31(3). Supplementary means on interpretation, such as preparatory work of the treaty, are used to confirm the meaning “resulting from the application of Article 31, or to determine the meaning when the interpretation according to Article 31 (a) leaves the meaning ambiguous or obscure; or (b) leads to a result which is manifestly absurd or unreasonable.” *Id.* at art. 32.

94. Bederman, *supra* note 79, at 973.

95. Vienna Convention, *supra* note 88, art. 32(b). Although United States courts have historically looked outside treaty text to determine the intent of the parties much more readily than permitted by the Vienna Convention, “[r]ecently, federal courts have become reluctant to deviate from the text of a treaty unless failing to do so ‘leaves the meaning ambiguous or obscure; or . . . [l]eads to a result which is manifestly absurd or unreasonable.’” Bederman, *supra* note 79, at 973-74. The problem has been that the United States Supreme Court has been unwilling to articulate exactly what kind of vagueness would qualify the terms of an international agreement as vague enough to warrant departure from the text itself. *Id.* One situation where courts have looked outside the agreement itself is where language was missing in one instrument, but present in another related provision or agreement. *Id.* (citing *Société Nationale Industrielle Aerospatiale v. United States District Court*, 482 U.S. 522, 534-40 (1987)). The jurisprudence in this area has been muddled, at best. *See id.* at 980-91 (critiquing the Supreme Court’s failure to provide definitive guidance for when a treaty text is vague enough to have to resort to extrinsic sources to ascertain meaning). The best response to this confusion is a coherent set of principles based on the Vienna Convention as well as American jurisprudence, as proposed by Bederman. *See id.* at 1030-34.

96. This author favors a modified version of the limited contextual approach as articulated in the Vienna Convention and expounded on by Bederman. *See supra* notes 79-95 and accompanying text.

97. *See supra* notes 79-95 and accompanying text.

and given their common subject matter, even the most ardent textualist would countenance reading these conventions together. When examining these conventions together, the specific prohibition on medical ships' use and possession of secret codes, coupled with its absence in Geneva Convention I, can be seen as demonstrating the treaty drafters' awareness of this issue. Therefore the omission of a prohibition on the use of "secret codes" in Geneva Convention I and its corresponding presence in Geneva Convention II illustrate that there was no intent to prohibit the use of such codes for any medical facility other than medical ships.⁹⁸ Any other interpretation contradicts the plain language of the conventions themselves, as well as fundamental maxims of statutory and treaty construction.⁹⁹

98. In at least one instance, the Supreme Court found that the omission of certain language in one treaty and its presence in another closely related treaty was evidence that such an omission was not a mere "slip of the pen," but was intentional. *Bederman, supra* note 79, at 980 (citing *Société Nationale*, 482 U.S. at 534-40); *see also* *Western Cherokee Indians ex rel. Owen v. United States*, 86 F. Supp. 981, 984 (Ct. Cl. 1949) ("By no process of liberal interpretation could a [certain provision], which was not mentioned in the treaty, be incorporated into the treaty, no matter what may have been the reason for its omission."); *The Amiable Isabella*, 19 U.S. (6 Wheat.) 1, 71 (1821) ("This Court does not possess any treaty-making power . . . [T]o alter, amend, or add to any treaty, by inserting any clause, whether small or great, important or trivial, would be on our part an usurpation of power, and not an exercise of judicial functions."). Of course, under this reading of Geneva Conventions I and II, the encrypted transmissions stemming from any medical facility covered under Geneva Convention I is not a treaty violation and is therefore permitted. According to this interpretation, the TMIP's use of encryption as part of its use of the GCCS/GCSS and the encrypted transmission of patient medical records could not be a treaty violation so long as the transmission did not emanate from hospital ships covered under Geneva Convention II. *See* notes 63-64, 77-99 and accompanying text. One may argue that the Geneva Conventions should be read and interpreted broadly because of their very nature; in fact, some favor a broad interpretative approach "going beyond the intent of the parties to further goals of international order" when the treaty is *sui generis* or has a constitutional nature, such as the United Nations Charter. Thomas Michael McDonnell, *Defensively Invoking Treaties in American Courts—Jurisdictional Challenges Under the U.N. Drug Trafficking Convention by U.S. Agents*, 37 WM. & MARY L. REV. 1401, 1437 n.164 (1996). However "[e]ven those conventions with a legislative or constitutional flavor are fashioned in a contractual sense, frequently with the very selection of words and phrases being the result of unanimous approval by the signatory States." *Bederman, supra* note 79, at 1022.

99. *See supra* notes 77-98 and accompanying text. There are, of course, limitations to such maxims. *See* MCNAIR, *supra* note 85, at 400 n.1 ("The exclusio is often the result of inadvertence or accident, and the maxim ought not to be applied, when its application, having regard to the subject matter to which is to be applied, leads to inconsistency or injustice."); 2A SINGER, *supra* note 84, § 47:25 ("A literal interpretation will prevail if the meaning of the statute is plainly expressed in its language, if it does not involve an absurdity, contradiction, [or] injustice . . ."). In this instance, there is no evidence that interpreting the lack of a prohibition on coded transmissions from medical facilities in Geneva Convention I as rendering such transmissions permissible results either in injustice or contradiction. For a discussion favoring a more expansive method of treaty interpretation, *see* Michael P. Van Alstine, *Dynamic Treaty Interpretation*, 146 U. PA. L. REV. 687, 691 (1998) ("[T]he [Supreme] Court has consistently refused to view a treaty as a body of integrated norms that is

An alternative view is that a “penumbra” of openness emanating from the corpus of these conventions dictates that no coded transmissions from military medical facilities of any kind may be sent.¹⁰⁰ Therefore any such transmissions would, in fact, constitute a technical breach.¹⁰¹ Even so, parties to Geneva Conventions I and II must still determine whether such a breach would constitute an act harmful to the enemy, outside medical facilities’ humanitarian duties, prior to any medical facility’s loss of protection.¹⁰² Under this interpretation, a determination as to whether the encryption of data within TMIP functions constitutes harmful acts outside medical facilities’ humanitarian duties becomes paramount.¹⁰³

As noted above, the TMIP’s function is to “support all echelons of care through an aggregation of medical data and situation reports that serve the theater of operations as well as the Continental United States (CONUS) sustaining base medical missions.”¹⁰⁴ It will provide United States forces with medical data concerning “[Command and Control] (including medical capabilities assessment/sustainability analysis and medical intelligence); Medical Logistics (MedLog) (including blood and blood product management); Patient Movement (PM); Health Care Delivery (HCD) (including medical surveillance and medical threat); and Manpower, Personnel, Training, and Resources.”¹⁰⁵ The information which is maintained, processed,

capable of generating internal solutions for gaps in its provisions.”).

100. For a discussion of the legal theories supporting penumbral obligations under treaties, see Vagts, *supra* note 83, at 323-30. The idea of penumbral rights and obligations is not alien to American jurisprudence. See generally *Griswold v. Connecticut*, 381 U.S. 479, 484 (1964) (noting that “specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance”).

101. This assumption contradicts the “plain language” of Geneva Conventions I and II. See *supra* notes 77-99 and accompanying text. Such an interpretation would also mean that that any encrypted transmission from a military medical facility violates Geneva Convention I, even if it is an encrypted personal e-mail or the purchase of a commercial item over the Internet via a browser with 128-bit encryption.

102. Of course, a warning must still be given before any aggressive action could be taken. See *supra* Part IV.

103. See *supra* text accompanying notes 63-64 for a discussion of the mission of the TMIP.

104. TMIP CAPSTONE REQUIREMENTS, *supra* note 64, para. 1.1.

105. *Id.* at para. 1.4. The term “command and control” and “medical threat and intelligence” may appear to represent information which may fall outside the humanitarian duties of medical facilities. “Command and control” means the “capability to receive, process, display, and analyze situation information to assist commanders in the decision making process.” *Id.* at para. 4.2.1. “Medical threat and intelligence” means “[t]he body of information and processes used for force medical protection; combat stress control; casualty rate estimation; enemy force strength, location, organization, and weaponry estimates; environmental and epidemiological studies; foreign military and civilian health care facilities and capabilities; and monitoring.” *Id.* at app. D-1. Such information can be used, inter alia, to estimate the amount of medical supplies that may be required, the types of injuries and number casualties expected based on the weapons being utilized, as well as to determine whether a medi-

and disseminated through the TMIP is required for the operation of any large medical facility.¹⁰⁶ Since these types of information processing are necessary for any large medical institution, such functions fall squarely within medical humanitarian duties. Therefore, military medical facilities utilizing the TMIP should be not subject to the loss of their protections under Geneva Convention I.¹⁰⁷

VI. TRENDS IN ENCRYPTION

We have seen the increasing diffusion of encryption throughout the United States military.¹⁰⁸ Moreover, powerful encryption software is readily available,¹⁰⁹ and overall demand for encryption has been on the rise.¹¹⁰ The

cal facility should be evacuated in light of enemy troop location and movements. Based on these definitions and the medical uses for this information, all such data relates squarely to the functions of a military medical facility and not to the types of acts which are "harmful to the enemy." See *supra* notes 70-76 and accompanying text.

106. See Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 463-72 (1995) (discussing health care information contained and collected by public and private health database organizations).

107. Although medical facilities may not lose their protections, one must be mindful of the distinction between the medical facility itself and TMIP transmission infrastructure according to the principle of discrimination. See OPERATIONAL LAW HANDBOOK, *supra* note 8, at 10 (discussing principle of discrimination or distinction, which requires "that combatants be distinguished from noncombatants, and that military objectives be distinguished from protected property or protected places"). However, under this principle, it is this author's opinion that the TMIP's underlying transmission infrastructure itself (which is the SIPRNet, at least for part of its information flow) is a lawful target, despite any incidental effect its disruption may have on medical data flow. With the United States's dependence on information superiority in modern conflict, an effective attack on military information networks could be devastating. See generally Dhillon & Smith, *supra* note 7; Schmitt, *supra* note 7; Walker, *supra* note 9. The DOD acknowledges TMIP could be a target. See TMIP CAPSTONE REQUIREMENTS, *supra* note 64, para. 2.2.

108. See *supra* notes 46-64 and accompanying text.

109. According to one author,

any user of a personal computer can, barring regulation, download a common program called Pretty Good Privacy, or PGP, from the Internet at no charge for personal use. Some academic authors estimate the time needed to crack codes comparable to those used in PGP is upwards of eight trillion times the history of the universe.

Geoffrey Gordon, *Breaking The Code: What Encryption Means for the First Amendment and Human Rights*, 32 COLUM. HUM. RTS. L. REV. 477, 481 (2001). For a variety of reasons, the United States government has been wary of the diffusion of encryption technology, especially abroad. See generally Joe Baladi, *Building Castles Made of Glass—Security on the Internet*, 21 U. ARK. LITTLE ROCK L. REV. 251 (1999); Gordon, *supra*, at 486-87.

110. F. Lynn McNulty, *Encryption's Importance to Economic and Infrastructure Security*, 9 DUKE J. COMP. & INT'L L. 427, 428 (1999) ("In general, interest in encryption is at an all-time high and demand for it in the commercial marketplace is soaring."). However, it remains to be seen what, if any, effects the September 11, 2001 terrorist attacks on the

increasing diffusion of encryption technology militates against extending the bar on encrypted transmissions from medical ships to all military medical facilities. This is demonstrated by the positions of some Western nations regarding encryption equipment on medical transport aircraft, as well as scholarly opinions on the state of the customary law of the sea.

For example, as encryption technology has become commonplace and transparent to the user, even the direct prohibition on medical ships' use of "secret codes" is viewed as outdated. Due to technological changes since 1949, "all messages to and from warships, including unclassified messages, are now automatically encrypted when sent and decrypted when received by communications equipment that includes the crypto function."¹¹¹

In response to these changes, the *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* recommends that "[i]n order to fulfill most effectively their humanitarian mission, hospital ships should be permitted to use cryptographic equipment. The equipment shall not be used in any circumstances to transmit intelligence data nor in any other way to acquire any military advantage."¹¹² According to Louise Doswald-Beck, "[t]his recommendation was agreed to because of evidence that the prohibition of the use of a secret code adversely affects the ability of hospital ships to carry out their mission effectively."¹¹³ Any misuse of this equipment "could be minimized by permitting a qualified neutral observer to be on board to check on the proper use of this equipment."¹¹⁴

An additional example of this evolving view on encrypted data transmission is represented by some Western nations' interpretation of Article 28(2) of the Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts ("Protocol I").¹¹⁵ Article 28(2) states that "[m]edical aircraft shall

United States will have on encryption technology. See Mike Godwin, *Just Say No—Will Strong Encryption Be a Casualty of War?*, AM. LAW., Nov. 2001, at 73; John Schwartz, *As Debate on Privacy Heats Up, Sales Don't*, N.Y. TIMES, Nov. 5, 2001, at G9.

111. Roach, *supra* note 77, at 75.

112. SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA para. 171 (Louise Doswald-Beck ed., 1995) [hereinafter SAN REMO MANUAL]. The SAN REMO MANUAL was completed in 1994 and represents the labor of scholars and naval practitioners whose desire was to update and clarify the customary international law of armed conflict at sea in light of new technology and modern means of warfare, and to implement changes in the law on armed conflict on land and in other areas of international law. Louise Doswald-Beck, *The San Remo Manual on International Law Applicable to Armed Conflicts at Sea*, 89 AM. J. INT'L L. 192, 192-94 (1995).

113. Doswald-Beck, *supra* note 112, at 196. The SAN REMO MANUAL makes this recommendation despite its direct contradiction with Article 34 of Geneva Convention II. See Geneva Convention II, art. 34, *supra* note 68.

114. Roach, *supra* note 77, at 76 (citing Geneva Convention II, art. 31(4)).

115. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Dec. 12, 1977, art. 28(2), 1125

not be used to collect or transmit intelligence data and shall not carry any equipment intended for such purposes."¹¹⁶ France, the United Kingdom, and Ireland, in ratifying Protocol I, all provided an interpretive declaration regarding Article 28(2). Each of these nations interprets this article as permitting use of encryption equipment to facilitate navigation, identification, and communications in support of medical transportation.¹¹⁷ Through this interpretation, these nations have implicitly acknowledged that encryption technology is so commonplace that it has become impractical to utilize aircraft not so equipped for medical transport.¹¹⁸

U.N.T.S. 3 [hereinafter Protocol I]. The impetus for the additional protocols was the International Committee of the Red Cross's belief that international law insufficiently covered certain areas of warfare in the conflicts following World War II, "specifically aerial bombardments, protection of civilians, and wars of national liberation." OPERATIONAL LAW HANDBOOK, *supra* note 8, at 11. Although the United States has not ratified Protocol I, it views many of its provisions as either customary international law or as accepted practice, through not legally binding. *Id.* This includes the provisions on medical units, aircraft, and ships. *Id.* For a detailed discussion of United States acceptance of and objections to provisions contained in Protocol I, see Michael J. Matheson, *The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AM. U. J. INT'L L. & POL'Y 419, 420-29 (1987).

116. Protocol I, *supra* note 115, art. 28(2). "Intelligence data" means "any information which could have an effect on the conduct of military operations: for example, signaling the presence of military positions in a particular sector is clearly intelligence data, but so is signaling the absence of such positions." *Commentaries to Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)*, art. 28(2), at 302, available at <http://www.icrc.org/ihl.nsf/WebComART?OpenView> [hereinafter *Commentaries to Protocol I*]. "Whether or not it has collected or transmitted such data, an aircraft carrying equipment intended for [the collection or transmission of intelligence data] is committing a breach." *Id.* at 303.

117. Ratification of the Additional Protocols by the United Kingdom of Great Britain and Northern Ireland, Jan. 28, 1998, para. e, *reprinted in* 322 INT'L REV. RED CROSS 186, 187 (1998).

Given the practical need to make use of non-dedicated aircraft for medical evacuation purposes, the United Kingdom does not interpret this paragraph as precluding the presence on board of communications equipment and encryption materials or the use thereof solely to facilitate navigation, identification or communication in support of medical transportation as defined in Article 8(f).

Id.; see also Ratification of the Protocols Additional to the Geneva Conventions of 12 August 1949 by Ireland, May 19, 1999, para. 4, *reprinted in* 834 INT'L REV. RED CROSS 418, 419 (1999) (same); Adhésion de la France au Protocole I du 8 juin 1977, 11 avril 2001, para. 5, *reprinted in* 842 INT'L REV. RED CROSS 549 (2001) (En contexte "d'utiliser des avions . . . pour . . . d'évacuation sanitaire, le gouvernement . . . français[] n'interprète pas le paragraphe 2 de l'article 28 comme excluant . . . [les] équipements de communication et . . . de cryptologie, ni l'utilisation de ceux-ci uniquement [pour] faciliter la navigation, l'identification ou la communication au profit d'une mission de transport sanitaire, comme définie à l'article 8.")

118. Although the trend is toward allowing equipment with cryptological functions, the carrying of equipment permitting access to the SIPRNet would appear to violate this provision of Protocol I, because the SIPRNet as a whole is clearly designed to transmit intelligence data. See *Commentaries to Protocol I*, *supra* note 116, at 303 ("Whether or not it has

VII. "TRUST BUT VERIFY"

Encrypted communications represent an ever-increasing share of communications in the military. We have seen that with the proliferation of encryption technology, scholars have proposed that the prohibition on such transmissions by medical ships covered under Geneva Convention II be abolished. In such an environment, extending the prohibition on encrypted transmissions to medical facilities covered under Geneva Convention I is unwarranted. Given the present climate and status of the law, treaty modifications are not required to permit the United States military's operation of the TMIP from medical units covered under Geneva Convention I. If, in fact, the United States espouses this interpretation, it should, at a minimum, strongly consider a declaration to that effect. A declaration would serve to place other nations on notice as to United States' policy on encryption of medical facility data.

However, in the interest of fostering forthrightness under the law of armed conflict, the United States should go one step farther: the authorization of observers or inspectors to verify that the TMIP is only used for the transmission of medical information.¹¹⁹ Of course, practical considerations prevent such persons from being present at every American military medical facility covered under Geneva Convention I. Nevertheless, inspectors at the macro level of the TMIP could certainly verify that the system as a whole only carries medical information. Such an inspection or observer program, with appropriate safeguards for sensitive United States technology and information, conducted perhaps by members of an international body such as the International Committee of the Red Cross, would mollify any criticism by other states that that the United States was violating the spirit of the Geneva Conventions through encrypted medical communications net-

collected or transmitted such data, an aircraft carrying equipment intended for [the collection or transmission of intelligence data] is committing a breach."'). One answer to this dilemma is for the medical aircraft's equipment to have access only to that portion of the SIPRNet relating to the TMIP resides and no other. This data is not "intelligence data" as characterized in the commentaries to Protocol I. See *Commentaries to Protocol I*, *supra* note 116, at 303; *supra* notes 104-07 and accompanying text. Therefore, there would be no violation.

119. The SAN REMO MANUAL suggests placing observers on board medical ships to prevent the misuse of cryptographic equipment. Roach, *supra* note 77, at 76 (citing Geneva Convention II, art. 31(4)). Moreover, observers are not unprecedented in other activities, such as the realm of arms control. See generally Barry Kellman, David S. Gualtieri, & Edward A. Tanzman, *Disarmament and Disclosure: How Arms Control Verification Can Proceed Without Threatening Confidential Business Information*, 36 HARV. INT'L L.J. 71 (1995). Neither are observers unprecedented in the treatment of wounded, sick, and prisoners of war. See Geneva Convention I, *supra* note 66, art. 3(2); Geneva Convention II, *supra* note 68, art. 3(2); OPERATIONAL LAW HANDBOOK, *supra* note 8, at 27 ("Subject to essential security needs and other reasonable requirements, the ICRC must be permitted to visit [prisoners of war] and provide them certain types of relief.").

works. Such a step may also prevent a need to call for modifications to applicable treaties, a process sure to be fraught with numerous obstacles. The United States has often invoked the adage "trust, but verify" in its dealing with other nations and should expect other nations to apply that same aphorism to it with equal force.¹²⁰ International observers/inspectors would permit parties to the Geneva Conventions to verify that the TMIP is in harmony with those conventions and would raise the level of trust that other nations exhibit towards the United States, surely a goal of American foreign policy.

VIII. CONCLUSION

As encryption technology becomes an integral and seamless part of electronic information exchange in every facet of military operations, the application of such technology in military medical facilities raises issues under LOAC. A careful look at the consequences of encrypting data from medial facilities is necessary, as a violation of LOAC could subject such facilities to attack.

Although Geneva Convention I does not restrict encryption of medical data from land-based facilities, Geneva Convention II specifically restricts encrypted communications from medical ships at sea. A textual analysis of these documents does not lend to extending the restrictions of Geneva Convention II to land-based medical facilities. This position is strengthened by recent Western countries' use of encrypted communications from medical aircraft. This position recognizes such encryption technology as an integral part of operating these advanced aircraft, and indeed the operation of advanced medical facility information technologies.

Although encrypted communications from land- and air-based medical facilities do not violate Geneva Convention I, as encryption becomes more invasive, the United States military should take steps to ensure that use of such technology does not unwittingly place these facilities at risk. One way to assure their safety is to make a formal declaration of intent to use encryption and its limits on medical data at these facilities. Another method is to employ neutral observers or inspectors to assure that the objectives of the Geneva Conventions are not eroded by use of such encryption technology. In this way, the United States may offer assurance to other nations that the maxim "trust but verify" applies equally to all.

120. American President Ronald Reagan often invoked the Russian maxim "*doveriyai no proveryai*" ("trust but verify") in arms control negotiations with the Soviet Union. See *The Summit*, N.Y. TIMES, Dec. 9, 1987, at A21 (transcribing remarks of President Reagan and General Secretary Mikhail Gorbachev during signing of treaty pledging the removal of Soviet and American medium and short range nuclear missiles from Europe).