NAVAL WAR COLLEGE
Newport, R.I.

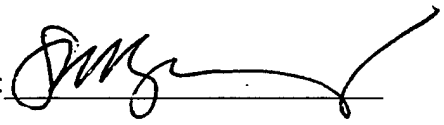
INNOCENT PACKETS? APPLYING NAVIGATIONAL REGIMES FROM THE LAW OF THE SEA CONVENTION BY ANALOGY TO THE REALM OF CYBERSPACE

By

Steven M. Barney
Lieutenant Commander, Judge Advocate General's Corps, U.S. Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: 

5 February 2001

Developments in information operations[1] have provoked considerable debate in legal circles and corresponding concerns among operational commanders over the legal framework to be applied to information warfare. Initially, some U.S. government lawyers suggested the application of modern information systems technology to military purposes was so new that *no* law applied.[2] However, as lawyers and war fighters began to work with the rapidly emerging technology it was recognized that many traditional military activities included under the umbrella term of "information operations" were actually physical attacks on information systems by traditional military means. Applying international law to information operations involving physical attacks is less difficult for commanders and their lawyers because the laws regulating traditional military operations have been reasonably well settled by treaties and through the customary practice of States. On the other hand, it is more difficult to apply international law principles to information attacks involving the use of electronic means to gain access or change data in an enemy's computer system without necessarily causing damage to the computer itself or the telecommunications infrastructure to which it is attached.[3] This "void" in international law may be remedied over time through development of treaties, though one scholar has observed, "[g]iven Internet technology's exponential growth, it would seem extraordinarily useless to go through a lengthy treaty negotiation process to draft an agreement listing prohibited Internet behaviors or actions that would be as out of date as the computers that began to produce the treaty at the start of the drafting and negotiation

---

[1] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13, (Washington, D.C. 1998). "Information Operations (IO) involve actions taken to affect adversary information and information systems while defending one's own information and information systems. Information Warfare (IW) is IO conducted during time of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary or adversaries[...]. Major capabilities to conduct IO include, but are not limited to, OPSEC, PSYOP, military deception, EW, and physical attack/destruction, and could include computer network attack. IO related activities include, but are not limited to, public affairs (PA) and civil affairs (CA) activities." I-1, 1.a.

[2] Walter Gary Sharp, Sr., Cyberspace and the Use of Force (Aegis Research Corporation, 1999) , 5.

[3] Department of Defense, Office of General Counsel, An Assessment of International Legal Issues in Information Operations, (Second Edition) (Washington, D.C., November, 1999), 4.

14

NWCR 98

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	
6. Office Symbol: C	7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): INNOCENT PACKETS? APPLYING NAVIGATIONAL REGIMES FROM THE LAW OF THE SEA CONVENTION BY ANALOGY TO THE REALM OF CYBERSPACE. (U)	
9. Personal Authors: LCDR STEVEN M. BARNEY, JAGC, USN	
10.Type of Report: FINAL	11. Date of Report: 5 FEB 2001
12.Page Count: 29	12A Paper Advisor (if any):
13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.	
14. Ten key words that relate to your paper: INFORMATION WARFARE; INFORMATION OPERATIONS; COMPUTER NETWORK ATTACK; LAW OF THE SEA; INNOCENT PASSAGE; TRANSIT PASSAGE; LAW OF ARMED CONFLICT; NEUTRALITY; INTERNATIONAL LAW.	

15.Abstract: BY APPLYING THE NAVIGATIONAL REGIMES OF THE 1982 UN CONVENTION ON THE LAW OF THE SEA TO THE REGIME OF CYBERSPACE, COMMANDERS AND LAWYERS CAN BETTER DEVELOP A FRAMEWORK FOR UNDERSTANDING HOW INTERNATIONAL LAW CAN IMPACT INFORMATION OPERATIONS. THE SIMILARITY OF THE OCEAN AND CYBERSPACE REALMS PROVIDES A CONVENIENT FRAMEWORK FOR UNDERSTANDING THE LIMITS OF NATIONAL SOVEREIGNTY IN CYBERSPACE, AND THE REGIMES FOR MOVING FORCES THROUGH CYBERSPACE. THROUGH USE OF THE LAW OF THE SEA ANALOGIES THE COMMANDGER MAY SELECT THE THEORY OF TRANSIT THROUGH CYBERSPACE THAT MOST CLOSELY MATCHES MISSION REQUIREMENTS WHILE MINIMIZING ACTIONS THAT COULD INTRUDE ON THE SOVEREIGNTY OF NEUTRAL STATES. THE EFFECT OF THE PROPOSED CYBERSPACE REGIMES ON THE LAW OF NEUTRALITY IS DISCUSSED INCLUDING A PROPOLAL OF HOW PRINICIPLES OF NEUTRALITY CAN BE PRESERVED IN INFORMATION OPERATIONS.

16.Distribution / Availability of Abstract:	Unclassified X	Same As Rpt	DTIC Users
17.Abstract Security Classification: UNCLASSIFIED			
18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19.Telephone: 841-6461		20.Office Symbol: C	

Security Classification of This Page Unclassified

process."[4] This reason, as well as the lack of widespread experience in Cyberspace warfare among the international community suggests that commanders and their lawyers must resort to drawing analogies from custom, treaties, and principles applied in the law of land, sea, air and space law. As will be seen, the law of the sea, the law of naval warfare, and the law of aerial warfare offer the most comprehensive analogies for information warfare situations.[5] Moreover, since commanders and their lawyers are most familiar with the laws and principles that govern the use of force in physical space, it is likely that those same principles will be applied in future information warfare.

If the realm of Cyberspace has a strong conceptual parallel to the realm of physical space, then the navigational regimes applied to physical space under the 1982 United Nations Convention on the Law of the Sea[6] (hereinafter referred to as "1982 LOS Convention," or "LOS Convention") can be a useful and familiar conceptual framework when applied by analogy to planning and conducting operations in Cyberspace. This paper will explore how the LOS concepts of national and international waters can be applied to information operations, discuss the rights of transit through Cyberspace under those regimes, evaluate the advantages and disadvantages of applying the LOS concepts to information operations, and suggest how these LOS-based information operations concepts could impact the rights and obligations of neutral States.

The discussion of the legal implications of computer network attack begins with a scenario. It is 2005. In response to an unprovoked hostile act against citizens of State A by the armed forces of State Z, the national command authorities of State A authorize the use of force in national self-defense citing Article 51[7] of the Charter of the United

---

[4] George K. Walker, "Information Warfare and Neutrality", Vanderbilt Journal of Transnational Law, 33, 5 (November 2000), 1187

[5] Walker, 1175. See also, An Assessment of International Legal Issues in Information Operations, 47.

[6] The 1982 United Nations Convention on the Law of the Sea opened for signature 10 December, 1982. It came into force November 16, 1994. Annotated Supplement to the Commander's Handbook on the Law of Naval Operations, NWP 1-14M (1997), 1.1, p. 1-2, 3.

[7] Article 51 recognizes the "inherent right of individual or collective self defence" if an armed attack occurs against a Member of the United Nations.

Nations. Because there remains a continuing threat from State Z military forces, the State A Joint Task Force commander is authorized by superiors to launch a computer network attack[8] (CNA) on a State Z *military* computer system. State A military forces launch the computer network attack from a military-owned computer system in the territory of State A. Nearly instantaneously, the attack travels in electronic "packets" through the Internet, through communications networks in States B, C, D, E, F, and G before reaching the desired target in State Z. (Figure 1) As a result of the CNA, State Z military commanders are denied the use of their computer networks to communicate with units in the field. We will further assume the use of force in self defense by State A was lawful under the attendant circumstances, that disrupting State Z's computer network achieved a definite military advantage, and the use of force did not exceed what was necessary to prevent further attacks.

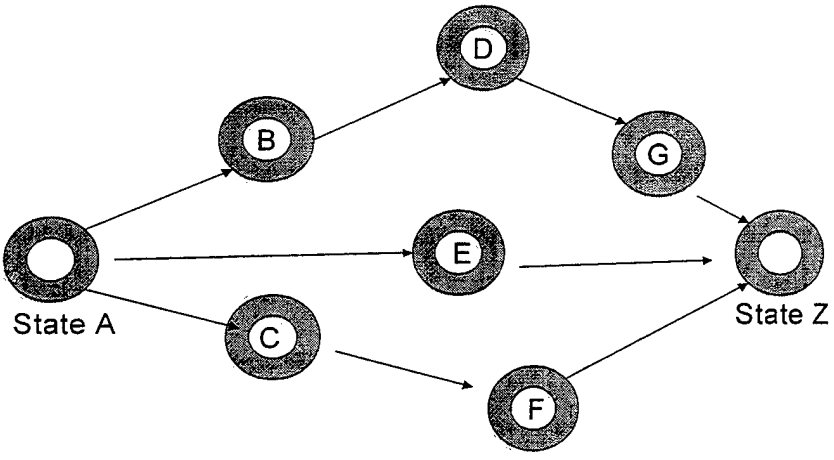


Figure 1: Hypothetical CNA Attack

[8] Joint Doctrine for Information Operations, GL-5. A Computer Network Attack is "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."

Under international law, did State A have the right to use the international telecommunications infrastructure to launch a CNA attack on State Z? Was the territorial sovereignty of those intermediate States violated by the mere passage of the CNA attack through their national telecommunications infrastructure? Did an act of force take place within their territory? If those States were neutral in the armed conflict, was that neutrality violated? May State Z insist those neutral States take affirmative steps to prevent further computer network attacks from being routed through the neutral State's telecommunications infrastructure? If the neutral States are willing but technologically unable to prevent further computer network attacks without shutting down their entire telecommunications infrastructure are the telecommunications nodes in those neutral states subject to attack by State Z? Finally, what distinction under international law, if any, would there be if State A had destroyed State Z's C2 computer system using a conventionally armed cruise missile launched from international waters instead of a CNA attack? Discussion of these questions begins by examining how the purposes and language of the LOS Convention can be adapted to operations in Cyberspace.

Purposes of the 1982 LOS Convention

The State Parties to the LOS Convention desired to settle issues related to the law of the sea "in a spirit of mutual understanding and cooperation [as an] important contribution to the maintenance of peace, justice, and progress for all peoples of the world."[9] The State Parties sought to resolve "problems of ocean space" through a regime that provides "due regard for the sovereignty of all States, a legal order for the seas and oceans which will facilitate international communication, and will promote the peaceful uses of the seas and oceans, the equitable and efficient utilization of their resources, the conservation of their living resources, and the study, protection and preservation of the marine environment."[10] Significantly, the State Parties expressly intended the

[9]UN Convention on the Law of the Sea, Preamble
[10]id.

Convention benefit not only coastal States but also land-locked States and "contribute to the realization of a just and equitable international economic order which takes into account the interests and needs of mankind as a whole and, in particular, the special interests and needs of developing countries."[11] The principles set forth in the Convention were premised on a United Nations (UN) General Assembly resolution which "solemnly declared *inter alia* that the area of the seabed and the ocean floor and the subsoil thereof, beyond the limits of national jurisdiction, as well as its resources are the common heritage of mankind, the exploration and exploitation of which shall be carried out for the benefit of mankind as a whole, irrespective of the geographical location of States[...]."[12]

Therefore, from these oceans policy principles the LOS Convention created an international framework to reaffirm the sovereignty of coastal States where necessary for safety and security while declaring international waters not subject to the sovereignty of any State but free for the use of all States. This notion of high seas freedom of navigation strikes a resounding chord with advocates of similar rights to users of the Internet. But that freedom must be balanced against important national interests:

> Techno-purists feel that Cyberspace is borderless; there are no national or regional boundaries to inhibit anyone from communicating with anyone by phone, across the network, or across the universe. And from one perspective we must agree: If Cyberspace is "that place in between" the phones or the computers, then there are no borders. As we electronically project our essences across the network, we become temporary citizens of Cyberspace, just like our fellow cybernauts. By exclusively accepting this view, however, we limit our ability to create effective national information policies and to define the economic security interests of our country.[13]

A sound policy that balances international freedoms in Cyberspace with legitimate concerns about national security may be achieved by applying the language

---

[11]id.
[12]id.
[13]Winn Schwartau, *Information Warfare: Chaos on the Electronic Super Highway*, Thunder's Mouth Press (New York, 1994), 327.

and terminology found in the LOS convention to the medium of Cyberspace. Fairly applied, such global Cyberspace policies could be as successful as the LOS Convention. Applying the underlying policies and purposes of the LOS Convention could, borrowing from the language of the Convention,

- be an important contribution to the maintenance of peace, justice, progress;
- resolve problems of Cyberspace;
- provide due regard for the sovereignty of all States;
- facilitate international communication;
- promote peaceful uses of Cyberspace and the equitable and efficient utilization of its resources;
- aid the study, protection, and preservation of the Cyberspace environment;
- contribute to the realization of a just and equitable economic order which takes into account the interests and needs of mankind as a whole and, in particular, the special interests and needs of developing countries;
- establish international Cyberspace as beyond the limits of national jurisdiction, as a common heritage of mankind, the exploration and exploitation of which shall be carried out for the benefit of mankind as a whole irrespective of the geographical location of States.

From the foregoing it is suggested that the underlying purposes of the LOS Convention, if applied to the Cyberspace medium, could have a desirable effect on international development of Cyberspace. If so, then one test of the usefulness of this analogy to preserving national sovereignty is how well two of the most important access rights under the LOS Convention, "innocent passage"[14] and "transit passage,"[15] might be applied to military operations in Cyberspace. Before we apply LOS transit rights to Cyberspace by analogy it is helpful to first identify LOS-unique regimes used to divide

[14]id., Part II, Section 3, generally.
[15]id., Part III, Section 2, generally.

land, sea, and air space and adapt those regimes to the unique medium of Cyberspace. To be useful to the Cyberspace analogy the regimes must support a realistic model for operations in Cyberspace and be consistent with current practice among States.

Dividing Cyberspace

Constructing a Cyberspace analogy begins by identifying Cyberspace navigational regimes based on the maritime navigational regimes from the 1982 LOS Convention. To be a valid analogy, the Cyberspace application of the traditional LOS concepts must be consistent with the underlying policy embodied in the LOS Convention and be applied fairly, neither creating new rights for States nor infringing on preexisting ones. The analogy must use a balanced, rational approach to divide the intangible medium of Cyberspace into areas where sovereign rights of the individual State are preserved, and yet which recognizes that the Internet is part of an international telecommunication system where freedom of access promotes the welfare of all States, and to which any artificially drawn boundaries would have to be consistent with legitimate issues of national sovereignty and customary international law.

With those goals in mind, the proposed analogy will divide Cyberspace into regimes called national Cyberspace (Figure 2)--consisting of internal Cyberspace and territorial Cyberspace--and international Cyberspace. Those terms are easily recognized for their similarity to terms used in the 1982 LOS Convention. The advantage of appropriating familiar LOS terms for the Cyberspace analogy is it will aid conceptualization of how the familiar maritime navigational regimes can be applied to Cyberspace.

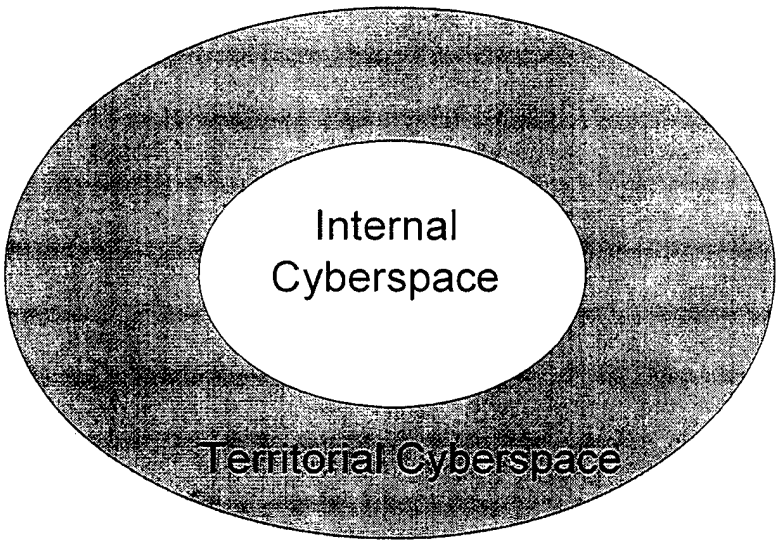


Figure 2. National Cyberspace

National Cyberspace.

National Cyberspace is the region of Cyberspace in which individual States require substantial sovereign rights to preserve the political and economic security of the State. National Cyberspace encompasses all of internal Cyberspace, with the addition of territorial Cyberspace. Understanding the distinction between internal and territorial Cyberspace is necessary to frame the overall rights and interests of national sovereignty that a State may exercise in national Cyberspace.

Internal Cyberspace

Internal Cyberspace is that region of Cyberspace where a State may exercise complete sovereignty; it is the Cyberspace equivalent to the land space, internal waters, and the air space above a State.[16] Internal Cyberspace is that medium serviced by the State's national telecommunications infrastructure[17] that is normally only accessible to

[16]The 1982 LOS Convention declares the national airspace to extend seaward from the land to the limit of the territorial sea.

[17]The term, "national telecommunications infrastructure" should be understood, in this context, to include both government and private telecommunications systems and not solely systems administered by and for the exclusive use of the State.

authorized users (that is, persons with the specific permission of the computer system administrator). It is further understood that the owner/operator of the computer system may use appropriate measures to deny unauthorized access and prevent intrusion. Internal Cyberspace includes the internal telecommunications systems of businesses and institutions of all kinds that are linked into the international telecommunications infrastructure by a combination of connections including cables, wires, microwave transmitters, and satellite ground stations. An example of the internal Cyberspace of the United States would include sensitive government telecommunication infrastructure and computer networks (e.g., the Department of Defense SIPRNET--Secret Internet Protocol Router Network--a computer network used for classified communications within the Department of Defense), and the equivalent internal communication networks used by businesses and organizations. Such networks, described as "critical infrastructure" by President Clinton in Executive Order 13010, include infrastructures so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.[18] The President acknowledged that because so many of these critical infrastructures are owned and operated by the private sector "it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation."[19] For this reason States can, and in most cases will, establish laws to prohibit unauthorized intrusions into internal Cyberspace by unauthorized users. Moreover, the protection of internal Cyberspace becomes a matter that requires the combined efforts of military and civil authorities to establish a robust defense.[20]

---

[18]Signed on 15 July 1996, EO 13010 identified the critical infrastructure into eight categories: telecommunications; electrical power systems; gas and oil storage and transportation; banking and finance; transportation; water supply systems; including medical, police, fire and rescue; and continuity of government.

[19]Sharp, 198.

[20]For an extensive discussion of operational considerations for computer network defense see, Colonel James P. Terry, USMC (Ret), *Responding To Attacks On Critical Computer Infrastructure: What Targets? What Rules of Engagement?* 46 Naval Law Review, 1999.

Because States have interests in protecting their critical information infrastructure, the commander must evaluate the political and military risks associated with information operations that intrude into the internal Cyberspace of another State. Lawyers may provide guidance to the commander using analyses similar to that used when an intrusion of internal waters, land space, national airspace, or the territorial sea is contemplated. Depending on the circumstances of the operation, those lawyers would likely recommend that the commander consult with superiors and seek permission, if appropriate, before intruding into another State's internal Cyberspace.[21] An intrusion into another State's internal Cyberspace for the purpose of conducting military operations, including a use of force against that State to degrade neutralize or destroy a computer network, will be considered lawful if the underlying use of force is authorized under Article 2 (4) of the Charter of the United Nations.[22] However, if the States are not lawfully engaged in armed conflict under Article 2 (4), then the intrusion of the internal Cyberspace of another State would not be lawful.

Responding to the discovery of an intrusion for the sole purpose of collecting intelligence is more difficult from the standpoint of the State desiring to defend against the intrusion. An intrusion for the limited purpose of collecting intelligence, without more, is probably not a "use of force" that would immediately entitle the aggrieved State to respond with force in self-defense. In such a case the most appropriate response by the aggrieved State would be to lodge a diplomatic protest of the unauthorized intrusion with the offending State as is frequently done by nations in response to discovering another State conducting espionage within its sovereign territory. However, if a State determines the intrusion constitutes a grave breach of the States national security, then use of force may be among the range of response options. An example of such a grave breach of

[21]For guidance on the use of force, see, generally, U.S. Joint Chiefs of Staff, Chairman of the Joint Chiefs of Staff Standing Rules of Engagement For US Forces. CJCSI 3121.01A (15 January 2000).

[22]Article 2 (4) expressly prohibits the use of force in international relations except as authorized by the United Nations Security Council under Chapter VII, or in national or collective self-defense under Article 51.

national security would be the act of inserting a computer virus into a military command and control computer network and not simply an intrusion for the purpose collecting intelligence information. Assuming the intruder could be identified, then any response involving the use of force by the aggrieved state must be premised on self-defense, and limited in scope to what is necessary and proportional to negate the danger posed by the intrusion.[23]

Without clear demarcation of borders or boundaries it may be difficult to determine when an information operation is at the point of intruding into internal Cyberspace. However, the practice among Internet users has begun to indicate virtual boundaries that may be adequate for the purposes of avoiding unintentional intrusions of internal Cyberspace. For example, some Internet sites are restricted to authorized users who register, obtain a password, or pay a fee to view materials or buy products or services on the site. Commanders conducting information operations should probably consider these types of owner/operator restrictions, by password or otherwise, as *prima facie* evidence that the site is within the internal Cyberspace of a State. The decision to intrude upon the site without authorization should be subjected to the risk analysis described above. The mere use of a warning screen "banner,"[24] indicating access to the site is limited to authorized users, is probably not sufficient to indicate the site is within a States' internal Cyberspace. However the Department of Defense Office of General Counsel suggests it may be possible to specify certain information systems or Internet sites as "vital to national security," both to give those systems high priority for security measures or to warn an intruder that an attack on the system could trigger an active defense in response that could damage the intruders' computer.[25] A prudent commander will conduct a risk analysis based on the specific warning language on the site and

---

[23]Sharp, p. 100.
[24]U.S. government web sites normally include a banner screen both greeting and alerting users and intruders that they are entering a government web site and advising of the penalties for unauthorized access.
[25]An Assessment of International Legal Issues in Information Operations, 47.

consult with qualified counsel before authorizing the intrusion to determine whether an unauthorized intrusion might trigger a defensive response or diplomatic protest, if detected.

Territorial Cyberspace

Territorial Cyberspace is that portion of national Cyberspace *through which and to which*, governments, commercial enterprises, or private organizations allow generally unrestricted access. An example of territorial Cyberspace of the United States government is the new Internet site, http://WWW.FirstGov.gov.[26] Developed as a single point of access to literally hundreds of web sites, FirstGov enables anyone with access to the World Wide Web to "surf" for information about agencies of the United States Government. Using this web site a potential adversary could lawfully use its national intelligence capabilities to collect open-source intelligence (OSINT) information about the United States government. Similarly, hundreds of thousands of businesses and non-commercial organizations maintain web sites on the World Wide Web and provide access to users from all over the world. There are currently no restrictions on agents or employees of government agencies, corporations, noncommercial organizations and individual persons to "surf" those web sites, send electronic mail, transfer files and funds "through and to" the territorial Cyberspace of a State.[27] For our analogy, this right of unrestricted access to territorial Cyberspace in the manner described above is discussed below as Cyber-innocent passage.

Taken together, internal Cyberspace and territorial Cyberspace comprise the national Cyberspace of a State. Within this area, States may promulgate laws to govern

[26]http://WWW.FirstGov.gov. Visitors to the site are welcomed with the following: "Welcome to FirstGov — the first-ever government website to provide the public with easy, one-stop access to all online U.S. Federal Government resources. This cutting-edge site gives the American people the "Information Age" government they deserve. By using the wonders of information technology to bring government closer to the American people, we can expand the reach of democracy and make government more responsive to citizens."

[27]The possible economic restriction, that a user must first have a computer with a connection to the Internet, does not change the underlying fact that once connected to the Internet the user is free to go anywhere.

access to national Cyberspace and exercise police power, including the power to initiate criminal prosecution against individuals who violate State laws and who are subject to personal jurisdiction of the State.[28] States may exercise judicial authority over activities in national Cyberspace, including laws concerning criminal acts (such as threats to harm the person or property of another), consumer protection, and require enforcement of contracts (again, subject to the requirement of having jurisdiction over a party).[29] Unlike OSINT activities in territorial Cyberspace, which are entirely lawful, a person who conducts intelligence collection activities that involve an unauthorized intrusion into internal Cyberspace is subject to criminal jurisdiction in the State where the penetration occurred.[30]

International Cyberspace

The regime of international Cyberspace is more difficult to define because there is no physical space counterpart specifically defined in the 1982 LOS Convention. The U.S. Navy *Commander's Handbook on the Law of Naval Operations* defines international waters "for operational purposes...[as] all ocean areas *not* subject to the territorial sovereignty of any nation."[31] Similarly, the 1982 LOS Convention identifies the high seas as comprising "all parts of the sea that are *not included* in the exclusive economic zone, in the territorial sea, or in the internal waters of a State."[32] The "not

---

[28]Under criminal law, for a person to be tried by a court they must be physically present within the jurisdiction of the court. This concept is called *in personam*, or personal jurisdiction.

[29]The question of personal jurisdiction for activity in Cyberspace is beyond the scope of this paper. The discussion of jurisdiction is merely intended to show the extent of national sovereignty that a State may exercise over activities conducted in national Cyberspace.

[30]While international law does not prohibit States from conducting espionage, it is well settled that State's may prosecute individual persons who conduct espionage if they are found within the physical territorial jurisdiction of the State. See, generally, Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law,* 68 U.S. Naval War College International Law Studies, 1978-1994 (1995).

[31] Commander's Handbook, at 1.5. For the purposes of this paper the term "nation" in the Commander's Handbook is the equivalent of "State." Italics in original.

[32]1982 LOS Convention, Part VII, Section 1, Art. 86. Italics added. The regime of exclusive economic zones (EEZ) is unique to physical space. Although coastal States retain specific rights over the resources found within the water column in the EEZ, those rights do not otherwise restrict the freedom of all States within the international waters, provided those freedoms are exercised with due regard to the rights of the Coastal State. See, id., Art. 58.

subject" and "not included" language in both definitions is significant in several respects. First, it underlines the primary approach taken in the LOS Convention to dividing maritime navigational regimes: the Convention defines with specificity those waters subject to the national jurisdiction of coastal States and leaves all other waters outside the jurisdiction of any State. Second, by defining international waters and the high seas in the negative--"not subject" and "not included," in coastal State jurisdiction, respectively--it reinforces the notion that, except for areas of the ocean in which coastal States have clearly identifiable and protected interests, no State has the right to declare jurisdiction over the areas of international waters. Finally, the approach suggested in this paper for defining regimes in Cyberspace is consistent with the intent of the LOS Convention because it reinforces the underlying LOS principle that outside national Cyberspace, commanders may move Cyber Forces with freedom from restrictions by other States, giving due regard for the rights of others.[33] In other words, international Cyberspace is not a place. It is that *characteristic* of Cyberspace by which something is not present anywhere but is merely in transit within the international telecommunications infrastructure and therefore not subject to the territorial sovereignty of any State.[34]

Under our analogy, since States would have authority to exercise jurisdiction over national Cyberspace it may be possible that a State could close national Cyberspace to information operations. While possible, it is not probable because one of the characteristics of the Internet is that no single organization controls access to the World Wide Web, "nor is there any centralized point from which individual Web sites or services can be blocked from the web."[35] To close national Cyberspace would require the State to cut off virtually all access to its own domestic telecommunications network, a measure that would be extremely disruptive and unsuitable except in the most grave

[33] Sharp, 15.
[34] Walker, 1104.
[35] Walker, 1099.

threats to national security. However, in cases where only the most critical national infrastructure is threatened and access to national Cyberspace is merely restricted, if telecommunication nodes are still accessible from outside the State the LOS Convention analogy provides two exceptions to the sovereignty of coastal States over national waters: innocent passage and transit passage.[36] These transit rights could be exercised to "move" Cyber Forces through national Cyberspace without the obligation to notify the State or any intermediate States, as suggested in the hypothetical scenario at the beginning of this paper.

Innocent Passage and Transit Passage in Cyberspace

The rights of innocent passage and transit passage under the LOS Convention are exceptions to the general rule that Coastal States may limit access by ships of all kinds to national waters. While both innocent passage and transit passage may be exercised by warships, both passage rights have specific limitations which must be considered by the operational planner seeking to employ either or both passage rights as a legal basis to move forces through physical space. Applied to Cyberspace navigation, it will be seen that Cyberspace transit passage is the preferred, though not the exclusive, mode that could be employed. From the following brief analysis it will be seen that the right of transit passage gives the commander superior flexibility as compared to the right of innocent passage.

Generally, the right of innocent passage gives the ships of all States, whether coastal or land-locked, the right to traverse the territorial sea in a continuous and expeditious manner, so long as that passage is not prejudicial to the peace, good order, or

---

[36]Horace B. Robertson, "The New Law of the Sea and the Law of Armed Conflict at Sea." 68 U.S. Naval War College International Law Studies, 1978-1994 (1995), 286. Discussing the EEZ, quoting Ambassador Elliott Richardson, "In the group which negotiated this language it was understood that the freedoms in question...must be *qualitatively* and *quantitatively* the same as the traditional high-seas freedoms recognized by international law: they must be qualitatively the same in the sense that the nature and extent of the right is the same as the traditional high-seas freedoms; they must be quantitatively the same in the sense that the included uses of the sea must embrace a range no less complete--and allow for the future uses no less inclusive--than traditional high-seas freedoms.[119]"

security of the coastal State. Certain actions by a warship or State vessel may be considered "not innocent" and thus inconsistent with the right of innocent passage through the territorial sea of a coastal State under Article 19 of the Convention. Those limitations, coupled with the right of coastal States to temporarily suspend the right of innocent passage when necessary for the security of the coastal State, reduce the value of innocent passage to the operational planner. Applying those same limitations to the right of innocent passage through the territorial Cyberspace (Figure 3), an operational planner may be unable to use Cyberspace innocent passage if the Cyber Force could be characterized as violating any of the following categories of activities extracted from the Convention:

> (a) any threat or use of force against the sovereignty, territorial integrity, or political independence of the coastal state, or in any other manner in violation of the principles of international law embodied in the Charter of the United Nations;
>
> (b) any exercise or practice with weapons of any kind;
>
> (c) any act aimed at collecting information to the prejudice of the defence or security of the coastal State;
>
> (d) any act of propaganda aimed at affecting the defence or security of the coastal State;
>
> (f) the launching, landing or taking on board of any military device;
>
> (g) the loading or unloading of any commodity, currency or person contrary to the customs, fiscal, immigration or sanitary laws and regulations of the coastal State;
>
> (h) the act of willful and serious pollution contrary to this Convention, (...)
>
> (j) the carrying out of research or survey activities;
>
> (k) any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State;
>
> (l) any other activity not having a direct bearing on passage.[37]

[37]id., Part II, Section 3, Subsection A, Article 19.

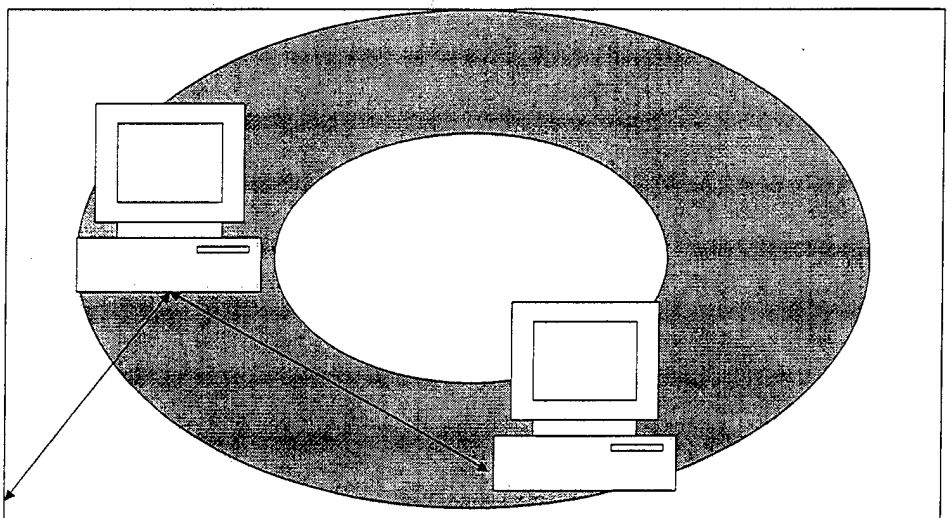


Figure 3: Cyberspace Innocent Passage, State B

A brief review of the factors expressed in the Convention as "prejudicial to the peace, good order or security of the coastal State" if conducted in the territorial sea suggests that any right of innocent passage through territorial Cyberspace would be at least as limited as that enjoyed by physical ships. In particular, restrictions under Article 19(2)(a) and (k) could directly impact a military operation involving CNA if the effect of the use of force actually interferes with communications, facilities, or installations of the transited state.[38] However, if no action or use of force is intended to be used against the

[38]It may be argued that the remainder of the limitations under Article 19(2) could further limit the right of innocent passage in Cyberspace, but a complete discussion of those limitations is beyond the scope of this article. Some problem areas include the following sub articles: (a) the question of when a military operation in Cyberspace constitutes a use of force requires applying the legal restraints on the use of force imposed by Article 2(4) of the Charter of the United Nations [See, Sharp, "What constitutes a prohibited 'threat or use of force' in Cyberspace and elsewhere is a question of fact that must be subjectively analyzed in each and every case in the context or all relevant law and circumstances." p.137] (c) the ordinary use of the Internet to collect open-source intelligence (OSINT); (g) the loading or unloading of a computer sniffer program, virus, logic bomb, or Trojan horse as a "commodity" contrary to the laws and regulations of the coastal State; (h) any action, willfully targeted toward another State which results in serious pollution contrary to the Convention, affecting the coastal State; (j) research or survey activities intended to identify features and vulnerabilities of the telecommunications infrastructure of the State; (k) the broad proscription on interfering with "any systems of communication" of the coastal State may be invoked if actions directed against a third State have a foreseeable collateral effect on the Coastal State; (l) the "other activity not having a direct bearing on passage" language points to the underlying assumption of innocent passage, being specifically a limited waiver of territorial sovereignty only when passing through the territorial sea or Cyberspace.

transited State, it may be argued that these issues are of limited effect unless they violate the sovereignty of the transited State. The more significant problem with using innocent passage for movement of force through Cyberspace may be the proscription against "any threat or use of force against the sovereignty, territorial integrity, or political independence of the coastal State, or in any other manner in violation of the principles of international law embodied in the Charter of the United Nations." Assuming no threat or use of force is directed against the *transited* State, there still remains the issue of whether innocent passage through Cyberspace may be limited if the use of force is targeted against a *third* State. However, the U.S. view of military use of innocent passage is that "cargo, destination, or purpose of the voyage can not be used as a criterion for determining that the passage is not innocent," and that "possession of passive characteristics, such as the innate combat capabilities of a warship, do not constitute 'activity'" within the territorial sea in regard to the enumerated list.[39] Therefore, applying that policy to Cyberspace innocent passage, the fact that a Cyberspace transmission contains an information "weapon" with destructive capability does not render passage "non-innocent."

In contrast, the maritime navigational regime of transit passage provides significantly greater flexibility to the commander and when applied by analogy to Cyberspace operations more closely matches how the international telecommunications infrastructure supports information operations (Figure 4).

In maritime navigation, the right of transit passage allows all ships and aircraft freedom of navigation and overflight solely for the purpose of continuous and expeditious transit of the international strait between one part of the high seas or an exclusive economic zone and another part of the high seas or an exclusive economic zone. Ships

---

[39]*Commander's Handbook (Annotated Supplement)*, Section 2.3.2.1, p. 2-8, footnote 27, summarizing testimony of Professor (Admiral) H.B. Robertson, House Merchant Marine & Fisheries Comm. , 97th Cong., hearing on the status of the law of the sea treaty negotiations, 27 July 1982, Ser. 97-29, at 413-14, and Professor B. Oxman, paragraph 2.1.1, note 2 (p. 2-1), at 853, respectively.

and aircraft exercising the right of transit passage may proceed without delay through or over the strait, in their normal mode of operations, and must refrain from the threat or use of force against the sovereignty, territorial integrity or independence of States bordering

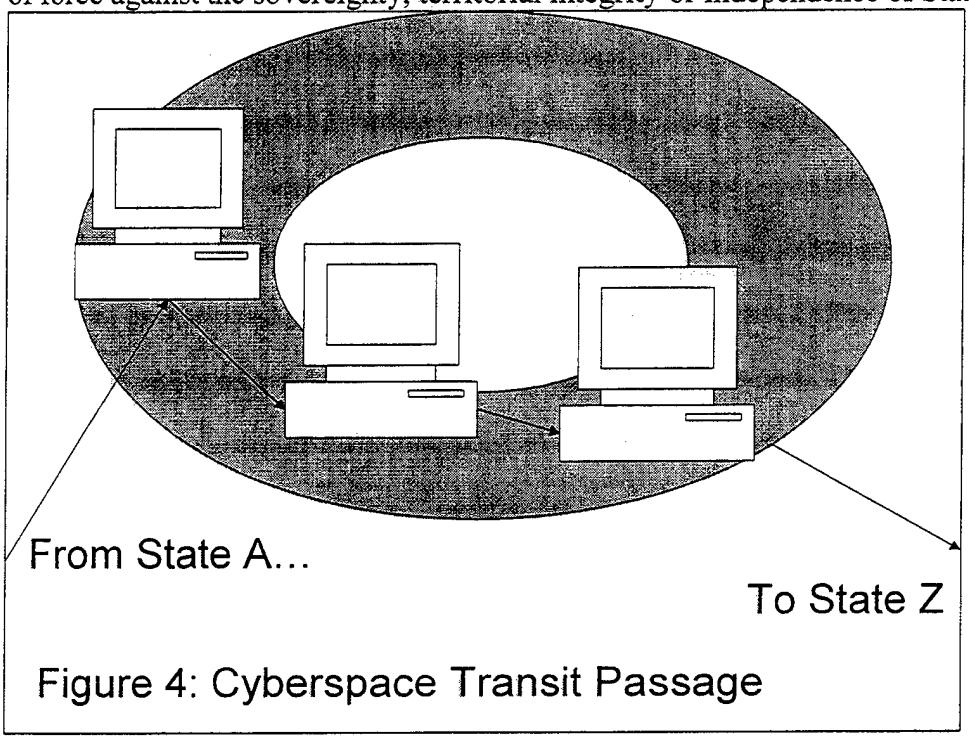


Figure 4: Cyberspace Transit Passage

the strait.[40] Therefore it would violate the rights of all States to exercise transit passage if, for example, Spain or Morocco closed the Straits of Gibraltar to ships and aircraft transiting between the Atlantic Ocean and the Mediterranean Sea, or if Iran or Oman closed the Straits of Hormuz to transit between the Persian Gulf and the Gulf of Oman. The right of transit passage through these international straits is important to the international economy, communication, and to national and collective self-defense.

In a similar manner, States and their people must use the national telecommunications infrastructure to gain access to international Cyberspace. Therefore the State's national telecommunications infrastructure is the Cyberspace equivalent of an international strait. When navigating these Cyberspace international straits, users behave much like ships and aircraft engaged in transit passage: they proceed without delay, in the

[40]1982 LOS Convention, Part III, Section 1, Articles 34-39.

normal mode of continuous and expeditious transit, and refrain from any threat or use of force against the national Cyberspace through which their communication is routed. The nature of telecommunications means Cyber Forces transit Cyberspace almost instantaneously and without delay except as limited by system bandwidth during periods of peak demand. The high speed of transmission is valuable to the commander as well as the State through which the Cyber Force is transmitted. The combination of speed and volume of Internet traffic means most States have limited capability to intercept and monitor Cyberspace communications. This limited ability to intercept and monitor traffic through Cyberspace is important to maintaining the neutrality of states that are mere intermediaries in information warfare, as in our opening scenario, because the transited State can plausibly deny knowledge of the transmission.

Transit passage provides the commander two major advantages over innocent passage: forces may transit in their normal mode of operations[41] and bordering States may not suspend the right of transit passage through international straits. When applied to navigation through Cyberspace the nonsuspendability characteristic of transit passage is a strong argument for applying the LOS Convention by analogy to Cyberspace. While governments, corporations and private organizations may choose to suspend access to their internal Cyberspace for various reasons, as global economies become more dependent on the international telecommunications infrastructure, it is much less likely that States could or would entirely close national Cyberspace. Even if a State tried to close national Cyberspace it would have little effect on other States ability to transfer CNA packets through international Cyberspace because an essential characteristic of the Internet is that if intermediate routers are not available the packet will be automatically rerouted through other servers. Finally, if a belligerent State, like State A in the opening scenario, were able to specifically route a CNA attack through the Cyberspace of a

[41]For submarines, submerged; for aircraft carriers, while conducting flight operations; for aircraft, while flying defensive cover for transiting surface ships,

neutral intermediate state that act alone would not be sufficient to violate the neutrality of the transited State if the Cyberspace transit passage analogy is used.

Neutrality in the Era of CyberWarfare

Codification of the navigational regimes in the LOS Convention had an immediate impact on the application of customary international law of armed conflict to the maritime environment. In his article, *"The New Law of the Sea and the Law of Armed Conflict at Sea,"* Rear Admiral Horace B. Robertson, JAGC, USN (Retired) discussed how the navigational regimes of the LOS Convention impacted the rights of neutral States. Admiral Robertson noted, "One of the advantages of the new transit passage concept is that it keeps the littoral States bordering straits with great strategic value out of the vicious circle of escalation in times of tension and crisis. If transit through such straits were subject to the discretion of the coastal States, they would unavoidably become involved even if the discretionary power were to be exercised evenhandedly[...]. The escalation preventing quality of transit passage in times of tension and crisis--i.e. in time of fragile peace---are even more important for neutral States in times of armed conflict.[42]" This is a particular advantage to States that are neutral in international armed conflict and is equally applicable to both traditional military operations and information operations.

The right of states to remain neutral in international armed conflict is well established under international law. The Hague Convention No. XIII, Concerning the Rights and Duties of Neutral Powers in Naval War (Hague XIII),[43] has not received universal ratification, but most of its provisions are considered to be a statement of customary international law. Hague XIII comprises the latest expression in treaty form of the respective rights and duties of neutrals and belligerents with respect to hostile

[42]Robertson, 282, Quoting Rauch, The Protocol Additional To The Geneva Conventions For The Protection Of Victims Of International Armed Conflicts And The United Nations Convention On The Law Of The Sea: Repercussions On The Law Of Naval Warfare 32, (1984)

[43]Hague Convention No. XIII, The Hague, 18 October 1907, 36 Stat. 2415, 2 Am. J. Int'l L.. (Supp) 202.

activities within neutral "maritime territory" (that is, internal waters and the territorial sea) and may be used as a starting point for discussion of these issues for our Cyberspace LOS analogy.[44]

Admiral Robertson described how the 1982 LOS Convention and the international law of armed conflict created special challenges for neutral States that must be reconciled with Hague XIII.[45] Hague XIII uses the terms "neutral waters" or waters "within its jurisdiction," or similar terms to refer "either to the internal waters or the territorial waters (territorial sea) of the neutral State", since those were the only areas of the oceans recognized at that time as being within the jurisdiction or sovereignty of the coastal State.[46] The cardinal principle of the law of neutrality is that belligerents may not conduct hostilities in neutral territory, land, or sea. Neutral states have an obligation to use the means at their disposal to conduct surveillance of their waters to ensure that belligerents do not violate their neutrality and to take preventive or corrective action if they detect such violations.[47] As the application of the law of neutrals has evolved through state practice over time, so too the changes in technology, including information

---

[44]Robertson, 276. Footnote omitted.

[45]. "The significant provisions of the Hague Convention No. XIII are as follows:

Belligerents are required to respect the sovereign rights of neutral States and to abstain from acts that would constitute a violation of neutrality (article 1);

[...]

Belligerents cannot use neutral ports or waters as a base of operations nor erect any apparatus to communicate with belligerent forces at sea (article 5);

A neutral Government must employ the "means at its disposal" to prevent the fitting out or arming of vessels within its jurisdiction which it believes are intended for cruising or engaging in hostile operations and to prevent departure from its jurisdiction of such vessels (article 8);

A Neutral State must apply its rules and restrictions impartially to the belligerents and may forbid the entry of vessels which have violated its rules or its neutrality (article 9);

The "mere passage" of belligerent warships or prizes through a neutral's territorial sea does not affect the neutral's neutrality (article 10);

Unless the neutral's regulations provide otherwise, belligerent warships may remain in neutral ports, roadsteads or territorial waters no more than 24 hours (article 12);

A neutral State must exercise such surveillance "as the means at its disposal allow" to prevent violation of its territorial waters (article 25); and

The exercise of its rights under the Convention by a neutral cannot be considered an unfriendly act by a belligerent (article 26).

[46]id.

[47]id., 278, footnote omitted.

warfare, do not cause states to discard those aspects of international law concerning neutrals which have become customary.

Citing Dr. Elmar Rauch, Admiral Robertson concluded that since the same rules apply to the post-1982 LOS Convention territorial sea that formerly applied in the narrow territorial sea, "...as a matter of principle belligerents are bound to respect the sovereignty of neutral powers and to abstain, in neutral territory or neutral waters from any act of warfare. Any act of hostility, including capture and the exercise of the right of search, committed by belligerent warships in the territorial waters of a neutral power, constitutes a violation of neutrality and is strictly forbidden."[48]

Counterbalancing this requirement for belligerents to refrain from violating neutrality is the obligation of the neutral State to conduct surveillance in their territorial waters to ensure belligerents comply. In an observation that immediate illustrates the difficulty of conducting surveillance of national Cyberspace, Admiral Robertson makes this observation concerning the perils created for the neutral under the 1982 LOS Convention:

> The emergence of a "new" peacetime regime for the oceans, with its expansion of existing zones subject to national jurisdiction and the creation of new zones also subject to the same or similar forms of jurisdiction, has created problems of adaptation of the traditional rules of armed conflict at sea to these new developments.... As has been suggested by the foregoing analysis, however, the geographic and operational factors that determine the nature and scope of naval operations in time of armed conflict, and, in particular, the relationships between belligerent and neutral forces, render it uncertain as to whether such mechanical application of prior rules to new or expanded areas of national jurisdiction serves the best interests of either neutrals or belligerents or the humanitarian objectives of the rules. Massive expanses of waters that are denied to belligerents for hostile operations and for which neutral States have burdensome duties of surveillance and control are likely to increase beyond belligerents' power to resist the temptation to violate such waters and to overtax the capabilities of neutral States to enforce their duties within them. The result may well be increased tension between neutral and belligerent States with the consequent danger of widening the

[48]Id., 279.

area of conflict and drawing neutral States into it.[49]

Admiral Robertson's recommendations for reformulating the rules of naval warfare that are affected by the emergence of new zones in the "new" law of the sea may be readily adapted by commanders and their lawyers, to the emerging requirements for the new zones of Cyberspace proposed in this paper. Those recommendations, found in pertinent part[50] at Appendix A, could serve as a useful policy to protect the rights of neutrals by guaranteeing that the mere transit of a computer network attack through a neutral States' national Cyberspace would not result in the loss of neutral status.

Conclusion

This paper has proposed that the navigational regimes under the 1982 UN Law of the Sea Convention could be applied by analogy to information operations involving a computer network attack. It was suggested that the CNA described in the scenario at the beginning of the paper might be lawfully transmitted through the international telecommunications infrastructure, including Internet routers physically located in neutral States, by applying the analogy of innocent passage and transit passage. The concept of Cyberspace transit passage gives commanders greater flexibility for information operations than does Cyberspace innocent passage, because under the LOS Convention states have the right to temporarily suspend innocent passage. During the near instantaneous transmission of the CNA to the intended target in the opening hypothetical, the CNA passed through international Cyberspace. The territorial sovereignty of those intermediate States was therefore not violated, nor did an act of force take place within

[49]id., 302.

[50]The author has substituted the Cyberspace terminology developed in this paper for the traditional LOS Convention maritime terms, and eliminated those sections of Admiral Robertson's analysis that do not

their territory. For that reason, and because most States lack the technological means to detect, intercept, and identify the CNA as it passes through the Internet, those neutral States had no obligation to prevent the transit of their national Cyberspace and their status as neutrals was not violated. Perhaps this analogy will provide a future Joint Task Force Commander with the conceptual tools needed to more effectively plan and conduct operations in and through Cyberspace with greater certainty that the courses of action involving the use of force in Cyberspace will comply with international law.[51]

---

apply to our analogy, such as maritime zones of archipelagic waters and exclusive economic zones.

[51] A prudent commander will seek and obtain the assistance of qualified legal counsel at the earliest planning stages. Qualified counsel must be consulted to determine whether, if at all, the analogy proposed in this paper comport with customary international law under the specific circumstances.

Appendix A

A Proposal To Adopt Selected Principles From The Hague Convention No. XIII, Concerning the Rights and Duties of Neutral Powers in Naval War to Information Operations

"3. Neutral [Cyberspace] consist of the internal [Cyberspace], territorial [Cyberspace], and where applicable, the [national Cyberspace], of a State which is not a party to the armed conflict.

"4. Within neutral Cyberspace, hostile acts by belligerent forces are forbidden. A neutral State must exercise such surveillance and enforcement measures as the means at its disposal allow to prevent violation of its neutral Cyberspace by belligerent forces.

"5. Hostile acts within the meaning of paragraph 4 include [.... e.] Use [of neutral Cyberspace] as a base of operations.

"6. Subject to the duty of impartiality, and under such regulation as it may establish, a neutral State may, without jeopardizing its neutrality, permit the following acts within its neutral [Cyberspace]:

a. Innocent passage [...]

"7. A belligerent [may not cause a transmission with offensive information operation capability to] extend its stay in neutral [Cyberspace] [....]

"8. Belligerent [States] may exercise the right of transit passage through neutral international straits [in Cyberspace]. While within neutral [Cyberspace] comprising an international strait [...] belligerent [...] forces are forbidden to carry out any hostile act.

"9. Should a neutral State be unable or unwilling to enforce its neutral obligations with respect to hostile military activities by belligerent [...] forces within its neutral [Cyberspace], the opposing belligerent may use such fore as is necessary within such neutral [Cyberspace] to protect its own forces and to terminate the violation of neutral [Cyberspace].

"10. A neutral State shall not be considered to have jeopardized its neutral status by exercising any of the foregoing neutral rights nor by allowing a belligerent State to exercise any of the privileges permitted to a belligerent State."[52]

[52] Robertson, 302.

Bibliography

Graham, Bradley. "Military Cyber Warfare Rules." The Washington Post. November 09, 1999
URL: http://www.computeruser.com/news/99/11/09/news9.html

Greenberg, Lawrence T., Seymour E. Goodman, Kevin J. Soo Hoo. Information Warfare and International Law. National Defense University Press. http://www.dodccrp.org/iwilindex.htm

Hague Convention No. XIII, The Hague, 18 October 1907, 36 Stat. 2415, 2 Am. J. Int'l L.(Supp) 202.

Lisitzyn, Oliver J. "Electronic Reconnaissance from the High Seas and International Law." 61 U.S. Naval War College International Law Studies, 1947-1977 (1995).

Robertson, Horace B. "The New Law of the Sea and the Law of Armed Conflict at Sea." 68 U.S. Naval War College International Law Studies, 1978-1994 (1995), 263.

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

Sharp, Walter Gary, Sr. Cyberspace and the Use of Force. Falls Church: Aegis Research Corporation, 1999.

Smith, George. How I Learned To Stop Worrying And Love The Virus. Time. February 3, 1997 Vol. 149 No. 5 TIME Digital - August 7, 1997
URL:http://www.time.com/time/digital/yourtech/0,2936,0,00.html

Terry, Colonel James P., USMC (Ret). "Responding To Attacks On Critical Computer Infrastructure: What Targets? What Rules of Engagement?" 46 Naval Law Review, 1999, 170.

Thompson, Mark. "If War Comes Home." TIME. August 21, 1995 Volume 146, No. 8.

Toffler, Alvin and Heidi Toffler. War and Anti-War. Boston: Little, Brown, 1993.

United Nations, Charter of the United Nations, New York: n.p.

United Nations Conference on the Law of the Sea, 3d. United Nations Convention on the Law of the Sea, A/CONF. 62/122. n.p.: 1982.

U.S. Department of Defense. Office of General Counsel. An Assessment of International Legal Issues in Information Operations. Second Edition. Washington, DC: November, 1999.

U.S. Joint Chiefs of Staff. Joint Doctrine for Information Operations, Joint Pub 3-13, (Washington, DC: 9 October 1998).

_____. Chairman of the Joint Chiefs of Staff Standing Rules of Engagement For US Forces.
CJCSI 3121.01A (15 January 2000).

U.S. Naval War College. Oceans Law and Policy Department. Annotated Supplement to the Commander's Handbook on the Law of Naval Operations. Naval Warfare Pub. 1-14M. Newport, RI: 1997.

Walker, George K. "Information Warfare and Neutrality" 33 Vanderbilt Journal of Transnational Law, Vol. 33. No. 5. (November 2000), 1079.

Waller, Douglas. "Onward Cyber Soldiers" TIME. August 21, 1995 Volume 146, No. 8.

Wolf, Jim. "U.S. Spy Chief: Cyberspace Is Potential Battlefield." TIME, August 21, 1995 Volume 146, No. 8.