ARTICLE Dimitrios Delibasis, *State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century*
Peace Conflict and Development: An Interdisciplinary Journal, Issue 8, February 2006, available from http://www.peacestudiesjournal.org.uk

ARTICLE

State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century

By Dimitrios Delibasis [1]

[1] Dimitrios Delibasis is an officer in the Greek Army Reserves and a NATO Reserve officer. He has an LLB degree from the National Capodistrian University in Athens, Greece, where he specialized in national security law. He is presently is a Visiting part time lecturer at the University of Westminster, UK, where he is also a doctoral candidate.

ABSTRACT

This article begins with a short overview of the various aspects of cyberspace warfare in an attempt to make clear the potential threat this new form of war represents to international peace and security. It then moves on to examine cyberspace warfare within the context of currently existing international legal norms on the use of force and to determine if these norms can be applied to this new form of warfare and if so, to what extent. Finally, the essay attempts to make apparent a twofold fact: first, that current legal norms on the use of force can only be applied to cyberspace by analogy and up to a certain point, hence there is a need to develop a regulatory framework specifically tailored for this purpose; second that the cause behind this need is the 'special' nature of cyberspace warfare.

"To guess at the intention of the enemy; to divine his opinion of yourself; to hide from both your intentions and opinion; to mislead him by feigned manoeuvres; to invoke ruses, as well as digested schemes, so as to fight under the best conditions – this is and always was the art of war".
Napoleon[2]

INTRODUCTION

Throughout the course of human history knowledge and information have always been considered to be tantamount to power[3]. In contrast with the past where the notion of power was thought to comprise solely military, economic and diplomatic factors, the current advent of the "Information Revolution" has made it evident that another vital, and perhaps the most vital element of power is, and has always been,

[2] Department of the Army – Headquarters, United States Army Training and Doctrine Command, 'Enabling Operations: Information Superiority', *Field Manual – FM3-0* 1 (Washington DC: Department of the Army, 2004).

[3] D. Kuehl, *Information Operations: The Hard Reality of Soft Power* 118 (Washington DC: Department of Defense, 2004).

information. Information has always historically been a force multiplier, as well as a major and extremely precise decision tool, and if its full potential is to be appreciated as well as exploited it must be regulated, and above all understood, for what it truly is – a weapon, which if it is utilised in the wrong way can backfire exactly like any other kinetic weapon in one's inventory[4].

Modern rapid advances in computer technology and especially in networking have instigated a major as well as fundamental shift in national security affairs and have irreversibly ushered the world community into a new era in which information warfare is the most prominent of powers[5]. As a direct consequence, the ability offered by modern technology to States to incorporate the full spectrum of information warfare tools and techniques in their respective arsenals, is currently affecting to an ever growing degree the means by which they would be going about their military as well as their civilian affairs in the new millennium[6].

Even more important is the fact that information warfare along with global networking has currently allowed any and all members of the international community to be in a position to benefit from the advantages of the information revolution by being able to utilise it in order to directly interact with one another irrespective of their relative state of technological, economic or military development. As an immediate result, there is nowadays not a single world State that is not in a position from which it can have a significant effect to both the maintenance of international peace and security as well as the world's economic development, provided it is capable of appreciating what a potent weapon information warfare can be and it also possesses the necessary political will to put such a potent weapon to good use[7].

Currently there are quite a few indications that potentially aggressive State sponsored as well as non State sponsored actors are showing a continuously and dangerously

[4] Ibid.
[5] Joint Command, Control and Information Warfare School, *Joint Information Operations Planning Handbook* 118 (Washington DC: Joint Command, Control and Information Warfare School, 2003).
[6] Ibid.
[7] See generally, FM3-0 Chapter 11, 'Characteristics of Information Superiority', *Enabling Operations – Information Superiority* (2004) via http://www.iwar.org.uk/iwar/recources/fm3-0/chapter11.htm.

increasing appreciation for the employment of information warfare as the best means of achieving their specific goals[8].

Within the past year, the Love Bug and Sasser Viruses managed to spread to over one and a half million computers respectively in less than four hours, far more quickly than any State's defence or law enforcement agencies could even begin to respond. information warfare attacks perpetrated by trusted insiders, individual hackers, organised groups and most importantly, various States have also dramatically increased and they continually appear to explore new approaches that make them extremely hard to identify and be traced back to their source.

More than twenty members of the international community-most prominent among them the United States, the Russian Federation, China, Israel, Australia as well as several members of the European Union-have made clear their intention to fully integrate information warfare as an asymmetric response in any future conflict they may have to be party to. Various elements of information warfare, including psychological operations, computer network attack, as well as computer network defence were extensively used in the 1998 Kosovo conflict; in 2001 during the course of "Operation Enduring Freedom" in Afghanistan; in the limited 2002 crisis between the People's Republic of China and Taiwan; in 2003 during "Operation Iraqi Freedom"; in 2001 during the international peacekeeping "Operation Belisi" spearheaded by the Australian defence Forces; and finally in the recently heated up Israeli-Palestinian conflict.

It is currently extremely hard to make an accurate prediction as to how much of an actual threat Information Warfare will eventually pose to international peace and security and what exact response the world will choose to give to it, especially in the regulatory field. Much will depend on the actual events that will eventually force the international community to turn its full attention to information warfare and whether it

[8] Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, 'Protecting the Homeland', *Report of the Defense Science Board Task Force on Defensive Information Operations: Memorandum for the Chairman, Defense Science Board* 1 (Washington DC: Department of Defense, 2001).

will eventually come to be viewed as a potent threat or just as a peaceful and purely scientific achievement.

However, there is already reason for concern[9]. Over twenty States are currently engaged, and extremely aggressively so, in developing information warfare attack capabilities. High speed interconnected information networks with a continuously increasing real time ability to identify targets, create and transmit plans, disseminate and analyse data and finally make decisions and take the necessary actions in minutes, if not seconds, have now become an integral part of the war-fighting capability of many modern States, due to the advent of the "Information Revolution". These same high speed interconnected information networks also form the backbone of all modern civilian national critical infrastructures, which are more vulnerable than ever before to a well coordinated information warfare attack. Such an attack could also rely for its success as well as anonymity for its perpetrators on sub-State actors, which during the first stages of an attack, will be extremely hard to identify.

The local as well as global interconnectivity of modern high speed information systems is the greatest advantage and also the greatest potential vulnerability of such systems because it provides the gate through which all unauthorised entries can, and usually do take place[10]. Prudence requires that States consider all existing viruses and "hacker attacks" as real information warfare operations and take the necessary steps to neutralise them as soon as such attacks are identified and traced. As a result, currently existing legal norms conceived with regard to the use of force in its traditional forms may not prove adequate in regulating such unique and potentially extremely volatile situations.

[9] Ibid.
[10] Ibid.

INFORMATION WARFARE AND EXISTING LEGAL NORMS ON SELF-DEFENSE

The first such set of legal principles which come into play with regard to the regulation of cyberspace warfare is premised in modern international legal norms as well as in general international customary law[11].

Modern international legal norms on self-defence are mainly rooted in the UN Charter which is applicable to all attacks perpetrated by State sponsors of aggression as well as to attacks launched by non-State sponsors of aggression in cases where there is a proven agency between any given attack and one or more States[12]. As a result, even cyberwarfare attacks initiated by non-State actors of aggression, will fall under the regulatory boundaries of the Charter if any direct or indirect agency is proven between the perpetrators of such attacks and a given foreign government. Additionally, and according to Article 51, the regulatory framework of the Charter with regard to self-defence governs only forcible acts that could be classified as armed attacks[13]. Unauthorised computer intrusions of a magnitude that is not large enough to classify them as armed attacks are bound to fall under the jurisdiction of international treaty law or in that of general international and domestic criminal law.

The main UN Charter provision regulating the use of force on the interstate level is Article 2(4) which sets forth a general prohibition of State recourse to forcible action[14]. As held by the International Court of Justice in its 1996 Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons[15] and on the Corfu Channel case[16], the broad phrasing of the article at hand prohibits any use or threats of force without any exception whatsoever, including those that are of a lesser magnitude than full scale war as well as those that may fall outside the traditional definition of armed

[11] *Case Concerning the Military and Paramilitary Activities in and Against Nicaragua* (Merits), [1986] *I.C.J. Rep.* 14, 94-5 and 176.
[12] *Tadic Case* (The Verdict), [May 7, 1997] *I.T. Press Release* CC/PIO/190-E.
[13] Charter of the United Nations, 59 *Stat.* 1031 *T. S. No.* 993, 3 *Bevans* 1153, Art. 51 (1945).
[14] *Advisory Opinion on the Legality of Threat or Use of Nuclear Weapons* [1996] *I.C.J Rep*. 226, 244.
[15] Ibid.
[16] *Corfu Channel Case* (Merits), 1949 *I.C.J. Rep.* 4, 21-3.

attack. This particular scope of the provision of Article 2(4) has been further and unanimously clarified by the UN General Assembly in Resolutions 2625[17] and 3314[18].

The phraseology of Article 2(4) combined with the one incorporated in General Assembly Resolutions 2625 and 3314 establishes that the main features of the threshold that has to be breached so that a given act which constitutes a "threat or use of force" falls within its regulatory parameters, hence being considered as illegal, are linked to the consequences rather than the means employed by the perpetrators of the act in question[19]. It therefore stands to reason that no forcible action can be lawfully exempted from the regulatory regime of Article 2(4) just because of it being of an advanced technological nature, even one as technologically advanced as information warfare, irrespective of the potential consequences of such an act.

There are two specific exceptions to the general prohibition of interstate force contained in Article 2(4). The first is embodied in UN Charter Article 39 which permits members of the UN to have recourse to force whenever the UN Security Council determines the existence of a threat to the peace, breach to the peace, or act of aggression and authorises such forcible action in accordance with subsequent Articles 41 and 42[20]. As provided in extremely broad terms by the aforementioned articles, especially by Article 42, there are no constraints whatsoever with regard to the exact nature of the forcible measures that may be authorised by the Security Council[21]. Consequently, even forcible actions of a somewhat unconventional as well as previously unheard of nature, such as the ones falling within the realm of cyberspace warfare, could be deemed to fall within the boundaries of the action permitted by the relevant provision of Article 42[22].

---

[17] Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, *UN Doc. A*/8028, General Assembly Resolution 2625, *UN GAOR 25TH Session Supplement* 28, 121 (1970).
[18] Definition of Aggression, *UN Doc. A*/9631, General Assembly Resolution 3314, *UN GAOR 29TH Session Supplement* 31, 142 (1974).
[19] Y. Dinstein, *War, Aggression and Self-Defense* 170-173 and 174 (Cambridge: Cambridge University Press, 2001). Also, US Department of Defense, *Active Defense against Computer Intrusions* 5-8 (Washington DC: Department of Defense, December 2nd 1998).
[20] Supra note 12 Art. 39.
[21] Ibid Art. 42.

The second explicit exception of the UN Charter to the prohibitive rule set forth by Article 2(4) is the right to individual and collective self-defence as elaborated in Article 51, which specifies that nothing short of an armed attack can give rise to the right of States to have recourse to forcible defensive action[23]. The actual use of the term "armed attack" in the article's text should not be construed as restrictive since it is important to keep in mind that Article 51 did not introduce the right to self-defence for the first time, but instead recognised a long established right, which is actually much broader than the wording used by the article's drafters[24].

This conforms to actual real world armed attacks, which under most circumstances do not comprise only traditional military weapons and tactics. Information warfare operations are the textbook example of a form of armed attack which is newly developed and totally unconventional in its conception and even though it is quite capable of causing widespread devastation is not covered by the traditional definition of the term 'armed attack'.

Indeed, as far as cyberspace warfare is concerned, especially if seen through the scope of the language adopted in Article 51, the crucial question that needs to be answered is whether an information warfare attack could fall under the classification of an armed attack and as a result justify recourse to forcible defensive action[25]. By focusing just on the means utilised in a given information warfare attack, one might fail at first to reach the inevitable conclusion that electronic signals can easily resemble bombs, bullets, missiles or other traditional types of weapons since they can have the same effect, if used in the appropriate manner. However, the international community is far more likely to be concerned about the actual consequences of a future successful cyberspace warfare, or any other type of new unorthodox attack,

---

[22] W. G. Sharp Sr. (Lt. Col. United States Marine Corps Ret.), 'Cyberspace and the Use of Force' *International Peace and Security : Current Legal Problems* 6-9 (Washington DC: Georgetown University Press, 1998).
[23] Supra note 12 Art. 51.
[24] *Case Concerning the Military and Paramilitary Activities in and Against Nicaragua* (Merits), [1986] *I.C.J. Rep.* 14, 176-77.
[25] US Department of Defense – Office of the General Counsel, *Active Defense against Peacetime Computer Intrusions* 7 (Washington: Department of Defense, 1998).

rather than its specific mechanism, particularly if it succeeds in causing severe material and human casualties.

The UN Charter articles regulating the exact circumstances under which States are entitled to resort to the use of force appear to be ideally suited to regulate forcible actions relating to information warfare operations. The key factor when it comes to the Charter's applicability to cyberspace warfare is its extremely broad language which is indicative of the fact that the Chapter's regulatory framework with regard to the use of force should not be seen from a restrictive point of view, since no legal instrument can be capable of fully and directly regulating all aspects of a given situation[26].

As far as international customary law is concerned, the ultimate test for any lawful exercise of the right of States to take recourse to force for self-defence purposes has been established by the "Caroline Case"[27]. According to the individual elements of the "Caroline Test", potential forcible actions taken by States in self-defence may be considered to be lawful only if they are subject to the three conditions of immediacy, necessity and proportionality which are innate to the very notion of self-defence. The legal test set forth by the "Caroline case" is traditionally considered to be linked to the highly ambiguous legal norm of anticipatory self-defence with the consequence that its potential applicability to modern State forcible defensive actions is heavily debated among the international legal community[28].

However, in retrospect the whole controversy with regard to the issue at hand appears to be moot since the eventual applicability of the "Caroline" or any other legal test regulating forcible defensive actions in general and any such actions that may relate to information warfare in particular depends entirely on the existence of an actual armed attack and not a fictitious threat[29].

[26] Supra note 13.
[27] Ibid at 245.
[28] I. Brownlie, *International Law and the Use of Force by States* 274-78 (Oxford: Clarendon, 1963).
[29] Supra note 23.

The critical factor to bear in mind at least when dealing with armed attacks that take shape in the real world, is that the "Caroline test", or any other legal norm of self-defence for that matter, comes into play at the precise moment in time during which such attacks actually commence and hence they materialise. Under most real life circumstances, that decisive point does not coincide with the time during which a given attack reaches its intended target and produces the effect desired by its perpetrator, it rather precedes it. As provided by existing self-defence norms, this is the factor that makes all the difference between a lawful recourse to forcible defensive action and an unlawful one[30]. Nothing less than a full fledged and very real and present armed attack can satisfy the "Caroline test"[31].

All in all, there is only one vital condition, which needs to be satisfied in order to ascertain in a given real world crisis situation whether the "Caroline test" might be applicable as well as to establish the side which would be answerable for initiating an armed attack[32]: to determine whether there is enough evidence to suggest that the side in question has engaged irreversibly and decisively on a specific course of action, not amounting to mere threats or to purely fictitious danger, so that an actual armed attack has begun to materialise, even if it has not yet crossed the borders of the State targeted or pressed home at its intended target.

In reality, the "Caroline test" relates not to anticipatory or preventive self-defence, which simply embodies a preventive forcible action in response to a purely foreseeable or conceivable armed attack and as a result could never hope to satisfy the three conditions of necessity, immediacy and proportionality, or the legal requirements of any other currently existing legal norms of self-defence[33]. Instead, the "Caroline test" relates to forcible defensive action which is interceptive in nature and which comes into play only after a potential aggressor has committed itself to an

[30] Supra note 13.
[31] Supra note 13 at 245.
[32] See generally, C. H. M. Waldock, 'The Regulation of the Use of Force by Individual States in International Law', 81 *R. C. A. D. I.* 450 et seq. (1952). Also, see generally, Cf. C. C. Joyner and M. A. Grimaldi, 'The United States and Nicaragua: Reflections on the Lawfulness of Contemporary Intervention', 25 *V. J. I. L.* 621 et seq. (1985).
[33] Y. Dinstein, *War, Aggression and Self-Defense* 172 (Cambridge: Cambridge University Press, 2001).

armed attack in a truly irreversible way, in other words when an attack has already been launched and is under way but has not yet reached its intended target[34].

To put it more simply, if in a hypothetical scenario, a State's defence establishment manages to successfully intercept and destroy an intercontinental ballistic missile launched from within the territory of another State against one of its cities then the action taken would be interceptive in nature. As a result, it would fly in the face of reason to hold the State which would appear to be the first to have opened fire answerable for inflicting an armed attack when in reality it would have acted in self-defence.

A similar scenario could arise in relation to a computer network attack. An unauthorised intruder may be positively identified while in the process of gaining unauthorised access to an information network which is of vital importance to a State's national critical infrastructure, either civilian or military, and unauthorised tampering with which would be bound to cause damage and potentially great loss of life. Under such circumstances it would be absurd to call for the attacked State's defence establishment to wait for the attack's full effects to take place and as a result run the risk of suffering severe damage before it starts taking the necessary forcible steps to neutralise it. Within the aforementioned context, the international customary legal paradigm established by the "Caroline case" is likely to be not simply adequate, but in fact rather significant for the potential regulation of State forcible actions in cyberspace[35].

The first two requirements of necessity and immediacy would be met with relative ease by any State which opts for taking forcible defensive action in cyberspace. This is due to the fact that the very nature of information warfare precludes any form of "anticipatory or preventive" computer network attacks[36], which might be launched in

[34] Supra note 16.
[35] A. D'Amato, 'International Law Cybernetics and Cyberspace', *U. S. Naval War College Int'l Law Studies – Blue Book 7*, 2 (Annapolis VA: US Naval War College, 2000).
[36] Author's Note: Cyberwarfare attacks can only be identified only after they are actually launched and they are well on their way. For details, US Department of Defense – Office of the General Council, *Active Defense against Peacetime Computer Intrusions* 8-9 (Washington DC: Department of Defense, 1998).

order to counter a hypothetical or purely fictitious threat and as a result would be rendered illegal[37]. As a consequence, all forcible defensive actions relating to cyberspace warfare are bound to take place only as a response to an actual armed attack as a direct consequence of which there is a necessity to seek recourse to force because all other avenues of redress are exhausted[38]. Additionally, the condition of immediacy would be inherent in any defensive cyberwarfare operation launched in response to a given computer network attack, since all such attacks call for immediate counteraction if there is any chance for their extremely destructive potential to be contained[39].

However, the most significant application of the "Caroline test" to cyberspace warfare activities is most likely to be with regard to the test's third legal condition of proportionality. Due to the high level of interconnectivity which characterises every aspect of cyberspace there is a very high potential for all information warfare operations to cause effects that might be gravely disproportionate to those originally intended[40]. Consequently, the hardest as well as most vital requirement for any State that has fallen victim to an information warfare attack to comply with, if it decides to exercise its right to self-defence by replying in kind, would be to ensure that the effects of any forcible defensive action taken would be proportionate to those caused by the attack suffered. Strict adherence to the principle of proportionality, as set forth by the "Caroline case", is likely to ensure that States contemplating a forceful response to a given cyberwarfare attack would weigh very carefully the actual extent of the damage they may cause if they eventually choose to "cross the Rubicon"[41].

[37] Supra note 13.
[38] O. Schachter, 'The Right of States to Use Armed Force', 82 *Mich. L. R.* 1620, 1635 (1984).
[39] A. K. Cebrowski (Vice Admiral US Navy, Ret.), *Sea, Space, Cyberspace: Borderless Domains* 5 (1999) via http://www.navy.mil/press/speeches/borderless.htm.
[40] *Advisory Opinion on the Legality of Threat or Use of Nuclear Weapons*, [1996] *I. C. J Rep*. 226, 225 and 263.
[41] Supra note 23.

ADDITIONAL INTERNATIONAL LEGAL INSTRUMENTS SUPPORTING THE RIGHT OF STATES TO USE FORCE IN CYBERSPACE

The second set of legal principles which are of major importance with regard to the regulation of cyberspace warfare is centred on the various international legal instruments containing legal norms supporting the right of States to use force in cyberspace.

Information Warfare and the "jus in bello"

One branch of international law containing a basic set of principles which could be applicable to even futuristic methods and means of waging war such as information warfare is the *"jus in bello"*. The *"jus in bello"* comes into effect as soon as hostilities commence between two or more belligerents[42] with the primary aim of setting some minimum standards of protection in order to prevent unnecessary suffering and destruction[43].

As provided by the law of war principles of military necessity and proportionality, potential cyberwarfare techniques may lawfully target only military targets and related critical national infrastructures[44]. Targets not of a military nature could be legitimately attacked during any information warfare operation only if the attacking State manages to show the military advantage from such an attack[45].

An additional principle of the *"jus in bello"* directly applicable to cyberspace warfare is the distinction between combatants and non-combatants which actually imposes a strict requirement with regard to information warfare operations. This requirement provides that only members belonging to a State's regular armed forces are legitimately authorised to conduct forcible actions during the course of an

[42] See generally, Y. Dinstein, War, *Aggression and Self-Defense* 207-13 (Cambridge: Cambridge University Press, 2001).
[43] The Annotated Supplement to the Commander's Handbook on the Law of Naval Operations', *U. S. Naval War College – Int'l Law Studies – Volume 73* 290-92 (Annapolis VA: US Naval War College, 1997).
[44] *Case Concerning United States Diplomatic and Consular Staff in Tehran,* [1980] *I. C. J. Rep.* 3, 43.
[45] Supra note 41.

international conflict[46]. In case of a cyberwarfare attack carried out by individuals falling outside the definition of a lawful combatant the perpetrators of the attack will both become legitimate military targets and they will also be liable to criminal prosecution, while the State sponsoring them will be in violation of the law of war[47].

An additional law of war principle with applicability to cyberwarfare is the one prohibiting weapons techniques and means of war that could cause superfluous injury, unnecessary suffering and long term damage to the environment[48]. The applicability of this particular principle to cyberwarfare operations is of particular significance, since due to their almost total interconnectivity modern information networks are very vulnerable to collateral damage, which may be caused by cyberwarfare weapons that are employed indiscriminately[49].

Furthermore and as provided by the relevant requirement of the *"jus in bello"*[50], States engaged in the study, development, acquisition, or adoption of new weapons and means of information warfare are under a legal obligation to determine that none of these means is prohibited in any way by international law.

Information warfare operations also need to comply with the *"jus in bello"* principle of chivalry according to which no war fighting techniques and tools whatsoever should be employed if they may rely on perfidy[51].

The final principle of the *"jus in bello"* applicable to information warfare operations is the principle of neutrality[52] which provides that: first, potential belligerents are

[46] Protocol (I), Additional to the Geneva Conventions of August 12th 1949 Relating to the Protection of Victims of International Armed Conflicts, *U. N. J. Y.* 95-117 Art. 4 and 43-51(1977).
[47] L. C. Green, *The Contemporary Law of Armed Conflict* 105-08 and 114-18 (Manchester: Manchester University Press, 2000).
[48] Supra note 45 Art. 35-42.
[49] Author's Note: An Information Warfare attack targeting a large civilian bio-chemical installation or a hydroelectric dam in complete disregard of the principles laid down by the *"jus in bello"* would fall within the aforementioned parameters by causing long term as well as serious damage to the environment.
[50] L. C. Green, *The Contemporary Law of Armed Conflict* 268-72 and 274 (Manchester: Manchester University Press, 2000).
[51] Author's Note: once again, perfidy relates to the use of electronic or visual symbols used to identify persons and property protected from attack in order to make a lawful military target immune to attack as well.

legally obliged to respect the territory and rights of States neutral to a given conflict; second, neutral States prevent by all necessary means, including the use of force, their territory from being used by a belligerent; third, neutral States abstain from assisting in any way the war effort of any of the belligerents. The significance of this particular legal norm with regard to cyberwarfare becomes evident if one keeps in mind that potential cyberwarfare aggressors are always likely to attempt to obscure the true origin of their attack by routing it through the information networks of one or more neutral States without the consent or knowledge of such States[53].

Information Warfare and the Law of Space

A further branch of international law comprising quite a few legal norms with applicability to cyberwarfare is the Law of Space. This applicability mainly stems from the fact that global networking, the key aspect of modern information technology, is dependent on the multiple space platforms orbiting Earth and on their relevant ground based supporting installations[54]. Moreover, space platforms are extremely important to information warfare operations for two additional reasons: one, they are by far the most vulnerable component of any information system as they are practically impossible to shield against attack; two, they represent the most vital force multiplier in any State's ability to successfully conduct information warfare operations; consequently, they are bound to be at the centre of any major contemporary defensive or offensive information warfare operation[55].

Information warfare operations involving space platforms fall under the legal norms regulating activities in space which are mostly articulated in the Outer Space Treaty

---

[52] See generally, A. Roberts and R. Guelff, *Documents on the Laws of War* 59 et seq. (Oxford: Oxford University Press, 2000).
[53] J. Adams, *The Next World War: The Warriors and Weapons of the New Battlefields in Cyberspace* 206-07 (London: Hutchinson, 1998).
[54] J. P. Terry, (Colonel United States Marine Corps Ret.), 'Responding to Attacks on Critical Computer Infrastructure' XLVI *Naval Law Review* 170 et seq. (1999). Also, see generally, T. C. Wingfield, *Legal Aspects of Offensive Information Operations in Space* 2 et seq. (2003) via http://www.usafa.mil/dfl/documents/wingfield.doc.
[55] T. C. Wingfield, *Legal Aspects of Offensive Information Operations in Space* 1-4 (2003) via http://www.usafa.mil/dfl/documents/wingfield.doc.

of 1967[56] and are considered by the international community as binding principles of international customary law[57].

First of all, information warfare activities in outer space continue to be subject to the currently existing legal framework regulating the use of force[58]. Secondly, all States engaged in information warfare activities in outer space must abstain from causing any potentially harmful interference with the activities of other States[59]. Thirdly, States involved in information warfare activities in outer Space shall bear international responsibility for all such activities, irrespective of whether these activities are being conducted by governmental or non-governmental entities[60].

The two further examples of specialised international space law regulatory instruments with direct applicability to information warfare operations are the INTELSAT agreement[61] and the INMARSAT agreement[62]. The INTELSAT agreement set up the regulatory framework for the establishment and functioning of the INTELSAT Organisation which is in charge of establishing and controlling a constellation of communications satellites linking various fixed terrestrial communications installations. INTELSAT comprises two independent segments one responsible for providing public telecommunications services and one responsible for providing specialised telecommunications services. As provided by the INTELSAT agreement only the segment providing public telecommunications services may be utilised for military purposes, including information warfare operations[63].

The INMARSAT agreement regulates the establishment as well as functioning of an international organisation controlling a large number of satellites providing

[56] See generally, Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 610 *U.N.T.S.* 205 (1967).
[57] P. A. Johnson (Colonel USAF/JAG Ret.), *An Assessment of International Legal Issues in Information Operations* 27. (Washington DC: Department of Defense, 1999).
[58] Supra note 54 at 5 (2003).
[59] Supra note 55 Art. 9.
[60] Supra note 55 Art. 6.
[61] See generally, Agreement Relating to the International Telecommunications Satellite Organization, 23 *U. S. T.* 3813 (1971).
[62] See generally, Convention of the International Maritime Satellite Organization 31 *U. S. T.* 1 *T. I. A. S. No*. 9605 (1976).
[63] Supra note 60 Art. 3.

telecommunications links between mobile terrestrial installations. As provided by the relevant articles of the agreement, the resources of INMARSAT may be employed for all legitimate military uses and that includes information warfare operations.

Information Warfare and the Law of the Sea

An additional international legal instrument putting forth several legal norms which are applicable to information warfare activities is the 1982 United Nations Convention on the Law of the Sea[64]. First, the Convention provides that all naval vessels exercising the right of innocent passage through a State's territorial waters must abstain from engaging in activities prejudicial to the peace, good order and security of the coastal State[65]. The Convention lists a series of several "prejudicial activities" every one of which could be a major integral part of a cyberwarfare operation[66]. Furthermore, the Convention calls for all States to co-operate in suppressing unauthorised broadcasting from the high seas[67], while it also takes several steps to guarantee the prosecution of the perpetrators of any potential unauthorised broadcasting from the high seas[68]. Lastly, the Convention provides for the protection of submarine cables[69].

Information Warfare and Communications Law

The branch of international communications law is also an area whose primary legal norms can be applicable to information warfare operations. These legal norms are being set forth in the International Telecommunications Convention[70]. The

[64] See generally, United Nations Conventions on the Law of the Sea". *UN Doc. A/CONF*.62/122, 21 *I. L. M.* 1261 (1982).
[65] Ibid Art. 19.
[66] Author's Note: The prejudicial activities referred to in Art. 19 are: a) any threat or use of force against the sovereignty, territorial integrity or political independence of the coastal State, or in any other manner inconsistent with the principles embodied in the Charter of the United Nations; b) any act aimed at collecting information to the prejudice of the defense or security of the coastal State; c) any act of propaganda aimed at affecting the defense or security of the coastal State; and d) any act aimed at interfering with any systems of communication or any other facilities of the coastal State.
[67] Supra note 63 Art. 109.
[68] Supra note 63 Art. 109.
[69] Supra note 63 Art. 113.
[70] See generally, International Telecommunications Convention, with Annexes and Protocols, Nov. 6th 1982 *US Senate Treaty Document* 99-6 (1982).

Convention allows for the cutting off of any private telecommunications which may appear to be dangerous to the security of a State party to the Convention[71]. Moreover, States have the right to suspend all international telecommunications service for an indefinite time for reasons of national security, provided they immediately notify the UN Secretary General. Additionally, all radio transmitting stations should be established and operated in such a manner so as not to cause harmful interference[72]. Eventually, and as provided by the last provision which is relevant to information warfare, States parties to the Convention retain absolute freedom with regard to the potential use of their military communications installations as long as they take all necessary steps to prevent any harmful interference[73].

Information Warfare and the Law of Treaties

Probably the most important branch of international law with regard to its potential applicability to information warfare operations is the law of treaties. This is due to the fact that treaty law represents the basic means through which members of the international community conduct their various transactions with one another[74]. A key issue relating to treaty law with regard to all kinds of forcible action is the question of whether a given treaty would continue to apply during wartime. When treaties fail to provide themselves a specific answer to this crucial question they are considered to be suspended between the belligerents in the events of hostilities[75], with the consequence that any forcible action involving the actual belligerents themselves would be subject to the *"jus in bello"*[76].

Quite a few aspects of the law of international agreements can have a direct applicability on the conduct of information warfare operations[77]. Extradition treaties as well as judicial assistance agreements are the most essential, if not the only lawful,

[71] Ibid Art. 19 (109-110).
[72] Supra note 69 Art. 20.
[73] Supra note 69 Art. 38 (164).
[74] See generally, D. J. Harris, *Cases and Materials in International Law* 765-70 (London: Thomson-Sweet and Maxwell, 2005).
[75] The Fisheries Jurisdiction Case, [1973] *I. C. J. Rep.* 3, 20.
[76] L. C. Green, *The Contemporary Law of Armed Conflict* 57-8. (Manchester: Manchester University Press, 2000).
[77] A. D. McNair, 'The Functions and Differing Legal Character of Treaties', 11 *B. Y. I. L.* 100 (1930).

means available for States to clamp down on the perpetrators of the overwhelming majority of unauthorised computer intrusions which appear as non State sponsored ones[78]. Consequently, it is of major importance that both the aforementioned types of treaties are conceived in such a way as that they cover information warfare activities, either through them being broad enough or through the inclusion of specific provisions designed to regulate cyberwarfare.

International agreements regulating civil aviation also include provisions regulating the conduct of information warfare. First, all States are under the obligation to show, under all circumstances, due regard for the safety of navigation of civil aircraft and are not to interfere in any way with that safety[79]. Second, States are prohibited from resorting to the use of all types of weaponry against civil aviation[80]. Furthermore, and as provided by treaties regulating diplomatic relations, members of the international community contemplating or engaged in any form of information warfare activities involving diplomatic personnel, premises or equipment must take into account the fact that diplomatic personnel, premises and equipment can neither be lawfully an integral segment nor a legitimate target of any such activities, since they are only to be utilised in strict accordance with their official purpose[81].

Status of Forces and Stationing Agreements represent the final type of international agreements which bear direct relevance to the regulation of information warfare operations[82]. Such agreements make all information warfare operations initiated by military forces stationed overseas subject to the following legal requirements: a) Whether the host State has to be notified before the commencement of any information warfare operation; b) whether the actual equipment involved in any given information warfare operation will be in breach of any legal obligation specified by a given stationing agreement; c) whether a given information warfare operation would require the use of a host State's own information systems; d) and finally, whether the

[78] Ibid.
[79] The Chicago Convention "Chicago International Air Services Transit Agreement, *U. K. T. S.* 8 1953 *Cmd.* 8742 – 171 *U.N. T. S.* 387 Art. 3(d), 28 and 37 (1944).
[80] Ibid Art. 3bis.
[81] Vienna Convention on Diplomatic Relations, 500 *U. N. T. S.* 95 – 55 *A. J. I. L.* 1064 Art. 2 and 24-30 (1961).
[82] Ibid Art. 41.

launching of an information warfare operation from a host State will make that particular host State subject to possible retaliation.

Even though the vast majority of modern international legal instruments do contain quite a few provisions which are applicable to the broader aspects of information warfare operations there is still a lack of an international legal framework specifically conceived to regulate this just emerging phenomenon. The potential establishment, in part of the international community, of any kind of legal regime for the particular regulation of a newly emerged situation, especially one of a highly technological and rapidly evolving as well as "dual purpose"[83] nature has historically been directly related to the seriousness of the actual events which will eventually draw the world's attention to the existence of such a situation[84]. If events in the future show unauthorised computer intrusions to be a serious menace to international peace and security, members of the world community will be more likely to pursue the establishment of a strict legal framework with regard to the regulation of information warfare tools and techniques. On the other hand, the opposite could be the case if no future actor of aggression aspires to take advantage of the ability of modern information technology to be used as a particularly effective and potentially very destructive force multiplier.

However, and irrespective of how much of a threat information warfare proves to be in the coming years, the continued absence of a universally adopted international legal framework which will oblige States to join forces in cutting down on unlawful information warfare activities emanating from their soil will almost literally render any attempt to indict the perpetrators of such activities pointless and entirely dependent on the good will of the individual governments of the world. In cases where a given unauthorised computer intrusion is either not defined as criminal or it actually is, yet the local government shows unwillingness to provide judicial

[83] Author's Note: The term "dual purpose" is being used here in its classical national security law meaning which is commonly used in order to denote technologies which can be used with equal effectiveness for both peaceful as well as for non peaceful purposes.
[84] See generally, C. H. Morgan II (Colonel USAF/JAG – Senior Judge Advocate/Air Force Office of Special Investigations), *Cyberspace Intrusion Investigations* 3 et seq. (Colorado Springs CO: Unites States Air Force/Office of Special Investigations, 2001).

assistance to the country finding itself on the unhappy receiving end of any such activity, the State victim will be practically left with little recourse, unless it decides to consider forcible defensive action, if the intrusion in question is serious enough so as to justify such action.

The seriousness as well as potential volatility of such acts becomes even more apparent when one considers that actors of aggression relying on unauthorised computer intrusions are in a position to start causing damage immediately upon gaining access to a given information system and as a consequence their actions must be interdicted immediately upon their apprehension[85]. Such a potentially critical situation for the long term maintenance of international peace and security calls for some serious means to be dealt with, with the most effective among them passing through a concerted effort to strengthen international cooperation which could comprise several aspects.

INFORMATION WARFARE AND THE NEED FOR CREATING A "JUS NOVUM"

The first such aspect would be to cover any gaps in currently existing legislation as well as ensure the modernisation of existing legal norms already applicable to information warfare activities both on the domestic level, through the adoption of the necessary criminal statutes, and on the international level, through the adoption of international legal instruments guaranteeing the provision of mutual judicial assistance.

The second would be to take advantage of the already existing regulatory framework comprising all international legal instruments which contain specific provisions applicable to information warfare operations. All these legal instruments, in their specific sections, outlaw both unauthorised gaining of access as well as interference with information systems and in general call upon States to cooperate in curtailing

[85] See generally, J. Adams, *The Next World War: The Warriors and Weapons in the New Battlefields in Cyberspace* 199 et seq. (London: Hutchinson, 1998). Also, J. F. Dunnigan, *The Next War Zone: Confronting the Global Threat of Cyberterrorism* 1 et seq. (New York NY: Osborne/McGraw-Hill, 2002).

such activities in all their forms[86]. All international legal instruments falling into the aforementioned category are generally being considered to express customary international law and consequently are equally binding on all States even if they are not parties to these particular instruments[87]. Governments in the avant-garde of modern information technology would have every interest in pushing towards strict adherence to currently existing legal norms which are applicable to cyberwarfare activities.

However, and despite the fact that there are quite a few aspects of the international legal framework which can be applied to the issue at hand, its very own nature marks it as a totally new, highly specialised and full of different heavily conflicting national interests. As a consequence, there is a necessity for the world's States to move in the direction of adopting an international legal instrument specifically tailored to regulate cyberlaw in general and information warfare in particular. In fact, there is a strong precedent in the international community for creating a *"jus novum"* as the best possible means of regulating a special and newly emerged situation the specific features of which appear to be both in defiance of traditional national borders as well as situated in the centre of a host of important national interests heavily opposed to one another[88]. This precedent comprises two of the most important legal instruments in the history of international law, the 1982 United Nations Convention on the Law of the Sea and the 1967 Treaty on Outer Space. A process similar to the one that led to the implementation of the two aforementioned treaties could lead to the adoption of an international legal instrument which should meet successfully several challenges.

The first and foremost challenge that should be met is a detailed outlining of the specific characteristics which are unique to information warfare. These are: a) attackers start causing serious damage immediately upon gaining unauthorised access to a given information system; b) it's extremely stealthy nature makes it very hard to

[86] Author's Note: Once again there is no need to analyze in detail the various international legal instruments referred to here since this has already been done in the relevant section of this work and it would be redundant.
[87] See generally, H. Thirlway, *International Customary Law and Codification* 4 et seq. (Lieden: A. W. Sijthoff, 1972).
[88] UNESCO Resolution 29/C via http://www.i_forum.unesco.or.kr/data/fuentes.doc

identify the exact location of a given information warfare attack, thus complicating a victim's potential recourse to forcible defensive action; c) information warfare is a textbook example of a field in which no State can hope to achieve superiority or make itself impervious to attack. A full understanding of these features would ensure that any regulatory norms established strike the correct balance between the offensive as well as defensive interests the world's States may have with regard to information warfare, thus guaranteeing that they would both be effective and enjoy the maximum possible support amongst the international community.

The second challenge to be dealt with is the conforming of any new international legal instrument adopted with regard to regulating information warfare to currently existing legal norms of self-defence. Moreover, the provisions of any future Convention conceived for the potential regulation of information warfare must incorporate in their text the *"jus in bello"* norms relating to targeting, as well as to the distinction between combatants and non combatants and to mercenaries. Additionally, any future convention designed to regulate information warfare activities should take every possible step in order not only to avoid jeopardising in any way the world community's free access to cyberspace but also to guarantee it to the fullest possible degree.

The final challenge the potential drafters of any future information warfare regulatory regime would have to live up to is probably the most important: it is imperative that they include in the text guarantees for the provision of full judicial assistance from one government to another in cases of information warfare attacks whose location of origin has been positively identified. Furthermore, the relevant legal regime must leave no doubt whatsoever that in cases where a given State has been identified beyond any reasonable doubt as the source of a serious information warfare attack, and despite the fact that its government refuses to provide any judicial assistance so that the attack's perpetrators are brought to justice, then there would be a presumption of guilty involvement and the possibility of forcible defensive action.

This final challenge in particular is indicative more than any other of the international legal community's need for a new paradigm with regard to the effective regulation of information warfare and to all potential forcible actions relating to it. This is solely due to the fact that the advent of modern cyberwarfare tools and techniques which has provided potentially aggressive actors with an extremely simple yet effective weapon represents nothing less than a totally unprecedented concept of armed force which is still in the initial stages of its evolutionary process.

INFORMATION WARFARE AND ITS UNIQUE CHARACTERISTICS

Even though any attempt to foresee in an accurate way, whether information warfare will eventually manage to live up to its potential for becoming a major threat to international peace and security would be extremely difficult as well as premature for the time being, the risks involved in such an eventuality are too high to be ignored. The simple fact of the matter is that the same vast expanse of global information networks which is responsible for leading the way to prosperity for all members of the international community, renders all those who try to make the most of it susceptible to information warfare attacks by practically anyone with access to those same information networks[89]. What country having found itself at the wrong end of a world or even regional superpower's political, military, or economic might could resist utilising the ability offered by this characteristic of "global networking" to even the score and to take on even a vastly superior opponent with the high probability of inflicting a large amount of damage to it[90]? Additionally, relying on Information Warfare instead of employing more traditional methods of armed force carries quite a few advantages which make it an even more tempting form of waging war[91].

State sponsored cyberwarfare attacks are extremely hard to track back to their source. Furthermore, they have a tendency of appearing (especially in their initial stages) as isolated events and therefore it is even harder to establish whether they are State

[89] See Office of the Undersecretary of Defense – for Acquisition, Technology and Logistics, *Protecting the Homeland: Report of the Defense Science Board on Defensive Information Operations* 85 (Washington DC: Department of Defense, 2001).
[90] Ibid.
[91] Ibid.

sponsored or not. Moreover, even if a given cyberwarfare attack is State sponsored and that sponsorship is finally established, the State which organised and launched the attack can still have plausible deniability. Last, but certainly not least, information warfare allows a potential aggressor to wage war on its own terms by avoiding coming face to face with the strengths of a given opponent and instead turning that opponent's strength of being advanced enough so as to depend on modern information networking into a crucial and easily exploitable weakness.

An additional unique characteristic of information warfare is that the channels as well as the means through which it materialises are military as well as civilian and the same goes for its potential targets. Accordingly, if there can be any chance for adequate defensive steps to be taken against it, that chance can only exist through the very close and constant co-operation of both the government and the private sector. This is in direct contrast with more traditional forms of warfare responsibility for which falls almost exclusively under the jurisdiction of a given government[92].

Above all, information warfare attacks can only be identified after they are well on their way and have already caused significant damage. As a direct consequence, States that find themselves under any form of cyberwarfare attack have to take action in order to counter the attack at hand and neutralise its harmful effects as soon as they identify it. Also, a successful defence against the looming threat of information warfare is bound to require a reproduction in cyberspace of all the traditional defensive techniques of war specifically tailored as well as regulated to suit the new operational environment in which they will be called to function[93].

The final and perhaps most controversial characteristic that is inherent to information warfare is that computer network attacks have a national security as well as a law enforcement aspect[94]. Computer network attacks mounted against a given country call for the involvement of that country's defence establishment because it is the responsibility of that particular establishment to defend the country in question and

[92] Ibid at 85-6.
[93] Ibid.
[94] Ibid at 89-90.

because its assets are more likely to be the objectives of such an attack, partly due to the fact that they rely heavily on civilian critical infrastructure and partly because they represent the most logical targets of choice for a State's enemies. At the same time, in the overwhelming majority of information warfare attacks, especially during their initial phase, it is not possible to positively identify the actual intent of the perpetrator involved thus classifying them as simple criminal or terrorist activity, as an act of war or something in between[95]. In cyberspace, the same "hacking tools" can be employed with equal effectiveness by both an ordinary criminal and by a hostile State. The situation becomes even more complicated by the fact that information warfare is also virtually anonymous and under any circumstances deniable and easily so. As a result, any successful defence against it, calls for traditional law enforcement to be able to form as close and effective working relationship as possible with defence and national security agencies.

CONCLUSION

All in all, information warfare represents a totally new concept of taking recourse to forcible action, which even though is still in the first phase of its evolutionary process, has already reached the point where it needs to be subjected to a regulatory regime specifically tailored to meet the specific challenges it sets. Currently existing international legal norms on the use of force in general, and on self-defence in particular, can only marginally regulate cyberwarfare, since they were conceived to deal with more traditional and certainly less complicated forms of forcible action. They can only hope to achieve that regulation, in the form of the ubiquitous "Caroline Principle" which if it is eventually applied as the main regulatory regime in information warfare operations is bound to complicate things, rather than make them simpler, as it is far from capable of answering the various overlapping political, legal, economic and military challenges introduced by a revolutionary concept such as cyberwarfare.

[95] Ibid.

The challenges these currently existing norms of self-defence fail to address are several and they all require as precise a regulatory answer as possible if international peace and security is to be secured in the decades to come and the threat of cyber attacks is to be contained[96].

The first such challenge which fails to be dealt with by traditional international legal norms of self-defence is the question of a common and homogeneous terminology. Every new concept inevitably carries along with it the need for new terminology[97]. This need becomes even more urgent when the new concept involves complex legal and technological issues that have reached the point of requiring regulation. How one defines a concept and all its relevant aspects has a direct bearing on what actual legal framework will be applied to it or whether a new regime needs to be created in order to specifically regulate it[98]. Furthermore, devising the correct terminology and definitions for a newly evolved concept, such as cyberspace warfare, will impact other issues that may be directly affecting the concept at hand such as issues of political constraint, of providing adequate funding to develop the necessary defences, or of resolving matters of closer and more adequate co-operation between all those government agencies legally responsible for dealing with the new situation not only at the intra-State but also at the inter-State level.

The problem is even bigger with regard to forcible actions in cyberspace due to several complications that are inherent to this particular form of forcible action. Firstly, as it is rather difficult to distinguish computer network attacks attributed to ordinary criminal activity or even terrorist activity from large scale State sponsored attacks, there is the need for precisely defining the notion of armed attack in cyberspace. As things stand today there is a lack in the international legal community in general, and in the current legal doctrine of self defence in particular, not only of an adequate definition of the actual action that could be termed a 'cyber attack' but also of a consensus on whether computer network attacks pose a danger sufficient to

[96] See generally, Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, *Protecting the Homeland: Report of the Defense Science Board Task Force on Defensive Information Operations* 85 et seq. (Washington DC: Department of Defense, 2001).
[97] Ibid.
[98] Ibid.

justify a concerted defensive effort against such attacks[99]. Moreover, there are quite a few existing terms and definitions relating to cyberspace warfare which may be interpreted in many different ways depending on who is actually using them. For example, the term "monitoring" may have a specific meaning to the defence establishment of a given country, but it may have a totally different meaning if seen from a law enforcement or judicial point of view, and it certainly has a different meaning when seen from a civil liberties point of view[100].

A second issue, which is integral to any potentially successful concerted effort to regulate computer network attacks and that is not being addressed by existing legal norms of self-defence, is the fact of cyberspace warfare having a military as well as a civilian aspect[101]. Offensive as well as defensive information warfare requires, at an almost equal level, a very close working relationship between a State's private and public sectors, since information technology is one of the few fields were the civilian sector is technically ahead of the military. If such a relationship is to be successful it will have to be regulated by a legal framework specifically tailored to bridge the traditional gap between the private sector, which is usually reluctant to fundamentally change its ways, especially when it comes to free enterprise and to the yielding of control to government agencies, and the public sector which is organised around central control, especially in matters relating to defence and national security.

A third challenge set forth by information warfare activity which has a direct bearing on any regulatory attempt relating to cyberspace warfare activities, and which is not taken on by existing self-defence norms, is that any serious defensive attempt in containing forcible actions in cyberspace would be to a great extent dependant, for its supposed success, on previously unprecedented co-operation on the inter-State

[99] Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, *Protecting the Homeland: Report on the Defense Science Board Task Force on Defensive Information Operations* 86 (Washington DC: Department of Defense, 2001).
[100] Ibid.
[101] Ibid.
.

level[102]. This is due not only to the fact that global networking allows for computer network attacks to be routed through the borders of multiple countries, but also as a result of cyberwarfare's extremely stealthy nature, which makes it extremely hard for those under attack to tell whether they are being targeted by ordinary hackers or are the victims of a more serious State sponsored information warfare attack. The addressing of this particular issue would be of extreme importance from a regulatory point of view, for the additional reason that it would most likely set the legal threshold beyond which States might be lawfully justified in taking forcible action in response to information warfare activity directed against them.

If the potential threat posed by information warfare is to be contained in any effective manner at all, it is imperative that all currently existing law enforcement information sharing as well as cooperation roadblocks are resolved, not only at the domestic, but also at the international level[103]. As a direct result of cyberwarfare's stealthy nature which makes even large scale State-sponsored attacks indistinguishable during their initial stages from ordinary criminal activity, the complicated task of mounting an effective defensive effort against any given large scale computer network attacks, as well as organising a recovery effort after any such attacks are over, will be inevitably dependent for its success on one thing, and one thing alone: the willingness of all States whose territory or information networks appear to be related in any way with the cyberwarfare activity to provide intelligence sharing, as well as law enforcement and judicial cooperation, to the fullest of their abilities and as promptly as possible. This kind of close and absolutely essential inter-State cooperation will have to be sought on a previously unheard of and legally obligatory level in the history of international peace and security since that is exactly what is being called for by the unique nature of the problem at hand.

At the same time, living up to this particular regulatory challenge set by the advent of information warfare is of paramount importance for an additional reason. The

[102] Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, *Protecting the Homeland: Report of the Defense Science Task Board Task Force on Defensive Information Operations* 89 (Washington DC: Department of Defense, 2001).

[103] Ibid.

agreement or refusal on the part of any given State to offer, with all the means at its disposal, the close judicial, technical, or even military assistance necessary to contain a cyberwarfare attack emanating or being routed from within its territory, would eventually offer the only realistic legal threshold the violation of which would be tantamount to a presumption of guilty involvement and could lead to sanctions or even a lawful recourse to military action.

Once again, there is nothing in the currently existing doctrine on the use of force that would make it a legal obligation for the members of the international community to close ranks in offering such full and prompt assistance with regard to matters overlapping not only traditional law enforcement but national security as well. Furthermore, the legal norms relating to the lawful undertaking of forcible action in response to armed attacks not involving traditional means and methods of war are sketchy and highly controversial and they are bound to be tested to their limits by a concept as nebulous as the one represented by information warfare. The situation could only be resolved by the creation of a specific regulatory framework which would be purposely tailored to address all these critical issues, fully and in detail.

A further regulatory challenge set forth by cyberspace warfare and not being addressed by existing legal norms on self-defence, is the absence of any precise rules of engagement for States that might find themselves under cyber attack. The need for the adoption of such rules of engagement stems again from the purely technical nature of computer network attacks which allows for them to be identified only after they are well underway[104]. As a result, it is imperative that States finding their critical information infrastructures under cyberwarfare attack be able to take the necessary steps in order to contain such attacks at almost literally a moment's notice and without the need for too much deliberation. In a more practical sense this makes traditional law enforcement and national security procedures, both at the domestic and international levels too lengthy as to be of any real value in containing a given information warfare attack before it can cause severe damage.

[104] See generally, US Department of Defense, *Directive 3600.1 – Revision 1: Information Operations-ASD (C3I)* 2 et seq. (Washington DC: Department of Defense, 2001).

This regulatory issue could, if not dealt with, have very serious consequences for the maintenance of international peace and security in the future since it could tempt countries targeted by future cyberwarfare attacks to hastily reach the conclusion that their only available recourse would be to take refuge in forcible action without taking into consideration the legal issues involved, especially if they suffer major damage from cyber attacks. Such a problematic and potentially explosive situation could be avoided by the creation of specific procedures to ensure close inter-State judicial as well as technical and military co-operation with regard to information warfare attacks streamlined so that they are as least time-consuming as possible. Furthermore, it would be essential to precisely define the information warfare actions that would fall within the legal boundaries of the term 'armed attack' and to finally create a detailed set of relevant rules of engagement which would leave no doubt whatsoever to those responsible for the defence of each State's critical information infrastructure about the various and specific steps they are lawfully allowed to undertake during a given crisis-situation. Such a course of action would mean going beyond traditional legal norms on the use of force which have never been conceived in order to take on a complex, highly technical and above all asymmetric form of warfare such as represented by cyberwarfare and are therefore too general to be able to cover its multiple aspects.

In the coming decades, and in a highly unstable world environment, international peace and security will come face to face with a multitude of threats and challenges. However, none will be so likely to pose such a dramatic challenge, for both the best and the worst, as the one posed by the advent of the information revolution and especially by information warfare. The only way for the members of the international community to stand up successfully to this enormous challenge is by the adoption of an international legal network specifically designed to regulate all its potential aspects and therefore minimise the risks accompanying it.

This work was conceived and eventually put together with a very specific purpose in mind. To explore the challenges set by the advent of information warfare which is a completely new and mostly untried concept and as such is inevitably going to reach a

point where it will require being subject to a regulatory framework. Currently existing legal norms on the use of force appear to be marginally capable of being that regulatory framework and only because of the absence of a legal regime specifically tailored to deal with the issue at hand.

Time can only tell how much of a threat information warfare will eventually prove to be. However, it has undoubtedly given a completely new meaning to the term 'warfare' and nullified traditional borders between States. In essence, it has set forth, for the first time in the history of the law on the use of force, several new regulatory challenges the successful answering of which calls for the creation of a new paradigm with regard to the legal norms relating to forcible action. This is an issue which sooner or later the international legal community will have no choice but to face. And before it finally does so, perhaps it should remember the words of James Thurbur[105]: *"In times of change, learners shall inherit the earth, while the learned are beautifully equipped for a world that no longer exists"*.

BIBLIOGRAPHY

ACLU v. Reno, 929 F. Supp. 824, E.D. Pa. 1996, aff'd, 521 US 844 (1997).

J Adams, The Next World War: The Warriors and Weapons of the New Battlefields in Cyberspace, London; Hutchinson (1998).

Air Force Investigative Office deemed Incompetent during Rome Labs "Info-War" Break in, Crypt Newsl. (Jan. 1998). Available at http://sun.soci.niu.edu/~crypt/other/crpt46.htm

Col. J B Alexander (US Army Retired), Future Non Lethal Weapons in Twenty First Century Warfare, New York; St. Martin's Press (1999).

R W Aldrich, How Do You Know You Are at War in the Information Age, 22 Hous. J. Int'l Law (2000).

Y Alexander and M S Swetnam, Cyber Terrorism and Information Warfare, Oceana Publications, Dobbs Ferry; Oceana (1999).

Andem, International Legal Problems in the Peaceful Exploration and use of Outer Space, Rovaniemi; University of Lapland, Faculty of Law (1992).

[105] Reproduced in the US Department of Defense's *Protecting the Homeland* 85 (Washington DC: Department of Defense, 2001).

R H Anderson et al., Securing the US Defense Information Infrastructure: A Proposed Approach, Santa Monica CA; Rand Organization Publications (1999). Available at http://www.rand.org/publications/MR/MR 933.

R H Anderson and A C Hearn, An Exploration of Cyberspace Security R&D Investment Strategies for DARPA, Santa Monica CA, Rand Organization Publications (1997). Available at http://www.rand.org/publications/MR/MR 880.

D Amor, The e-business Revolution: Living and Working in an Interconnected World, Upper Saddle River, NJ; London-Prentice Hall PTR.

J E De Arechaga, International Law in the Past Third of the Century, 159 R.C.A.D.I. (1978).

A C Arend and R J Beck, International Law and the Use of Force: Beyond the UN Charter Paradigm, London; Routledge (1993).

Arrian (edited by Goold G P, as part of the Loeb Classical Library in 1976), Anabasis of Alexander, Harvard MA; Harvard University Press (1976).

Saint T Aquinas (edited by Blackfriars), Summa Theologiae – Secunda Secundae, Oxford; Blackfriars (1972).

Aristotle (edited by E Barker), The Politics, Oxford; Clarendon (1961).

J Arquilla and D Ronfeldt Eds, In Athena's Camp: Preparing for Conflict in the Information Age, Santa Monica CA; Rand Organization Publications (1997). Available at http://www.rand.org/publications/MR/MR 880.

J Arquilla and D Ronfeldt, The Advent of Netware, Santa Monica CA; Rand Organization Publications (2001).

J Arquilla et al., Cyberwar and Netwar: New Modes, Santa Monica CA; Rand Organization Publications (1995).

Available at http://www.rand.org/publications/randreview/issues/RRR.fal95.cyber/.

J Arquilla and D Ronfeldt, The Emergence of Noopolitik: Toward an American Information Strategy, Santa Monica CA; Rand Organization Publications (1999). Available at http://www.rand.org/publications/MR/MR 1033.

Saint Augustine (edited by Loeb Classical), De Civitate Dei Contra Paganos, Harvard MA; Harvard University Press (1960).

K E Avtzigiannis, One Year After the Mother of All Battles: Desert Storm-The First War Won From the Air, Athens; Technical Editions Ltd (1992).

Ayala (edited by Classics of International Law), De jure et Officiis Bellicis et Disciplina Militari, S.I; Carnegie Endowment for International Peace (1912).

J Barboza, Necessity in International Law, Hague; Recuil de Cours (1984).

C Barnett, Engage the Enemy More Closely, London; Penguin (2001).

D Bernstein, Industry Survey, Infosecurity News (May 1997), Reuters, Sabotage Suspect Charged, CNET News.com (1998). Available at http://www.news.com/News/Item/0,4,19245,00.html

H Bicheno, Midway, London; Cassel (2001).

D Bowett, Reprisals Including Recourse to Armed Force, 66 American Journal of International Law Vol.1 (1972).

D Bowett, Self-Defense in International Law, Manchester; Manchester University Press (1958).

D Bowett, The Use of Force for the Protection of Nationals Abroad; in A Cassese's: The Current Legal Regulation of the Use of Force, Dordrecht-Lancaster; Nijhoff M. (1985).

M E Bowman, Is International law ready for the Information age? 19 Fordham Int'l L. J. 1935 (1996).

G Bradley, Authorities Struggle with Cyberspace Rules, Washington Post, A1 (July 8th, 1998).

O'Brien, Reprisals, Deterrence and Self-Defense in Counterterror Operations, 30 V.J.I.L. 2-421 (1990).

J Brierly, The Law of Nations, S.I; Oxford University Press (1942).

J L Brierly, International Law and Resort to Armed Force, 4 Cambridge Law Journal (1932).

J L Brierly, Some Implications of the Pact of Paris, 10 B.Y.B. I.L. (1929).

H W Briggs, The Law of Nations: Cases, Documents, Notes; New York; Appleton-Century-Crofts (1952).

British and Foreign State Papers, London; Public Record Office (1857).

B Broms, The Definition of Aggression, 154 R.C.A.D.I. (1980).

I Brownlie, International Law and the Use of Force by States, Oxford; Clarendon (1981).

I Brownlie, Principles of Public International Law, Oxford; Oxford University Press (2003).

I Brownlie, The Use of Force in Self-Defense, 37 B. Y. I. L. (1961).

I Brownlie, The Rule of Law in International Affairs, The Hague-London; Nijhoff M. (1998).

I Brownlie, Humanitarian Intervention; in J N Moore's Law and Civil War in the Modern World 3- reprinted in J N Moore's National Security Law, Durham, N Carolina; Carolina Academic Press (1990).

G Bunn, International Law and the Use of Force in Peacetime: Do US Ships Have to Take the First Hit? Naval War College Review, Newport RI; Naval War College Press (May-June 1986).

A Campen, D Dearth and R T Gooden Eds, Cyberwar: Security, Strategy and Conflict in the Information Age, Fairfax VA; AFCEA Press (1996).

R Cartier, A History of the Second World War, Athens-Paris; Papyrous-Larousse (1987).

V ADM A K Cebrowski, Sea, Space, Cyberspace: Borderless Domains (1999). Available at http://www.nwc.navy.mil/press/speeches/borderless.htm.

Centre for Infrastructural Warfare Studies, Information Operations: Information Warfare Tutorial (2003).

At http://www.iwar.org.uk/iwar/resources/carlisle/iw-tutorial/ececsum.htm.

D J DiCenso, Information Warfare Cyberlaw (2003). Available at http://www.airpower.maxwell.af/mil/airchronicles/apj/apj99/sum99/dicenso.html.

CERT/CC Statistics 1988-2003 at http://www.cert.org.

CERT Coordination Centre Annual Reports at http://www.cert.org.

A Chayes, The legal Case for the US Action on Cuba, Dept. of St. Bull. 46 (1962).

D Chereshekin, V Tsygichko and G Smolyan, A Weapon That May Be More Dangerous than A Nuclear Weapon: The Realities of Information Warfare (1995). Available at

http://www.iwar.org.uk/iwar/resources/parameters/iw-deterrence.htm.

Cicero (edited by Loeb Classical), De Re Publica, Harvard MA; Harvard University Press (1928).

CIWARS Intelligence Report at http://www.iwar.org.

I Claude, Swords into Plowshares, London-New York; University of London Press (1971).

A Coll, The Limits of Global Consciousness and Legal Absolutism: Protecting International Law from some of its best friends, Harv. J. Int'l Law 27 (1986).

A Coll et al., Legal and Moral Constraints on Low Intensity Conflict, US Naval War College International Law Studies, Volume 67, Newport RI; Naval War College Press (1995).

Communiqué of the Meeting of Justice and Interior Ministers of the Eight (Dec. 10, 1997). Available at http://www.qlinks.net/comdocs/washcomm.htm

C O'Connell, The Prospects for Enforcing Monetary Judgments of the International Court of Justice: A Study of Nicaragua's Judgment against the United States, 30 V.J.I.L. (1990).

Covenant of the League of Nations, 1 International Legislation 1, (1919).

CJCSI S-3210, Joint Information Warfare Policy, Washington DC; Joint Chiefs of Staff (1996).

CJCSI 6510.01, Defensive Information Warfare Implementation, Washington DC; Joint Chiefs of Staff (1996).

CJCSI Instruction 3121.01, Standing Rules of Engagement for US Armed Forces, Washington DC; Joint Chiefs of Staff (1994).

CSIS, A Washington Think Tank Has Issued A Report.

Available at http://www.Infowar.com/mil_C4I_122298A_jshmtl. (1999).

CSIS Global Organized Crime Project, Cybercrime… Cyberterrorism… Cyberwarfare: Averting an electronic Waterloo, Washington DC; The Centre for Strategic International Studies Press (1998).

A D'Amato, International Law, Dobbs Ferry NY; Transnational Publishers (1987).

A D'Amato, The Concept of Custom in International Law, Ithaca-London; Cornell University Press (1971).

A D'Amato, International Law Cybernetics and Cyberspace, Naval War College Int'l Law Studies Blue Book-Volume 7, Newport RI; Naval War College Press (1999).

K W Dam and H S Lin, Cryptography's Role in Securing the Information Society, Washington DC; National Academy Press (1996).

J Deane, Digital Dragnet: The Hacking Crackdown. Available at http://www.zdnet.com/zdtv/thesite/0597w3/life/life550_051297

Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States, UN G. A. Res. 2131 (1965).

D Denning, Information Warfare and Security, New York NY; ACM Press (2003).

Y Dinstein, War Aggression and Self-Defense, Cambridge; Cambridge University Press (2001).

Y Dinstein, The Right of Self-Defense against Armed Attacks, Lund; Juristforlaget i Lund (1987).

Duke Journal of Comparative and International Law, Symposium: International Information Infrastructure, Protection and National Security, vol. 9 383-490 (1999).

J F Dunnigan, The Next War Zone: Confronting the Global Threat of Cyberterrorism, New York NY; Osborne/McGraw-Hill (2002).

C J Dunlap, Jr., Taming Shiva: Applying International Law to Nuclear Operations, 42 Air Force Law Review 157 (1997).

Von Elbe, The Evolution of the Concept of the Just War in International Law, 33 American Journal of International Law (1939).

J Elliston, The CIA and Cyberwar at http://www.Parascope.com/ds/cyber1.htm (1999).

P Emmett, "Information Mania – A New Manifestation of Gulf War Syndrome?" RUSU Journal 19-26 (February 1996).

J E S Fawcett, Outer Space: New Challenges to Law and Policy, Oxford; Clarendon (1984).

J E S Fawcett, International Law and the Uses of Outer Space, Dobbs Ferry NY; Oceana (1968).

J E S Fawcett, Intervention in International Law: A Study of SOME Recent Cases, 103 R.C.A.D.I. (1961).

H Foley, Woodrow Wilson's Case for the League of Nations, Princeton NJ; Princeton University Press (1923).

J Fonteyne, The Customary International Law Doctrine of Humanitarian Intervention: Its Current Validity under the UN Charter, 4 C.W.I.L.J. (1973).

T M Frank, Who Killed Art. 2(4)? Or Changing the Norms Governing the Use of Force by States, 64 American Journal of International Law (1970).

L Freedman, Information Warfare: Will Battle ever be joined? Lecture given at the launch of the International Centre for Security Analysis in London (October 1996). Available at http://www.kcl.ac.uk/orgs/icsa/larry.htm

L J Freeh, Director of the FBI speech at the 1997 International Computer Crime Conference (March 4, 1997). Available at http://www.fbi.gov/dirspch/compcrim.htm

D A Fulghum and R Wall, US Shifts Cyberwar to Combat Commands at http://www.dia.smil.mil/admin/EARLYBIRD/010226/e20010226usshifts.htm (2001).

GAO Report, Information Security: Computer Attacks at Department of Defense pose Increasing Risks (1996). See http://nsi.org/Library/Compsec/infosec.txt

The Geneva Protocol on the Pacific Settlement of International Disputes, International Legislation 1378-1381 (1924).

G Von Glan, Law among Nations, Boston-London; Allyn and Bacon (1996).

L Gomes, The Internet under Siege: Digital Forensics' Sleuths Focus on Routers, Hope for Some Luck, Wall Street Journal A3 (February 11, 2000).

D C Gompert, Right Makes Might: Freedom and Power in the Information Age, Institute for National Strategic Studies National Defense University Washington, DC, McNair Paper 59 (May 1998).

D C Gompert, National Security in the Information Age, Naval War College Review (Autumn 1998). Newport RI; Naval War College Press.

Goodrich, Hambro and Simmons, The Charter of the United Nations, New York-London; Columbia University Press (1969).

R E Gorelick, Wars of National Liberation: Jus ad Bellum, 11 C.W.R.J.I.L. (1979).

L C Green, The Contemporary Law of Armed Conflict, Manchester; Manchester University Press (2000).

Greenberg, Goodman and Soo Hoo, Information Warfare and International Law (1988). Available at http://www.dodccrp.org/.

M Greenspan, The Modern Law of Land Warfare, Berkeley-Los Angeles CA; University of California Press (1959).

C Greenwood, International Law and the United States Air Operation against Libya, 89 W.V.L.R. (1987).

C Greenwood, Self-Defense and the Conduct of International Armed Conflict; in Y Dinstein's Int'l Law at a Time of Perplexity: Essays in Honor of Sabtai Rosenne, Dordrecht; Nijhoff M. (1989).

L Gross, The Peace of Westphalia, 42 American Journal of International Law (1948).

H Grotius (edited by J B Scott), De Jure Belli ac Pacis, S.I; Oxford University Press (1925).

H Guomo, On Meeting the Challenge of The New Military Revolution, FBIS-CHI-96-130 (2003).

G Hackworth, 6 Digest of International Law (1943).

K Hafner and M Lyon, Where Wizards Stay Up Late: The Origins of The Internet, New York NY; Simon and Schuster (1996).

F J Hampson, Belligerent Reprisals and the 1977 Protocols to the Geneva Conventions of 1949, 37 I.C.L.Q. (1988).

J Hamre, DoD is Very Interested – Statement by the Deputy Secretary of Defense in the US Senate's Subcommittee on Technology, Terrorism and Government Information (1997). Available at http://www.fas.org/irp/congress/1988_hr/98-06-11.htm.

E Harshberger and D Ochmanek, Information in Warfare: New Opportunities for US Military Forces, Santa Monica CA; Rand Organization Publications (1999). Available at http://www.rand.org/publications.MR/MR1016.

D J Harris, Text Cases and Materials on International Law, London; Sweet and Maxwell (1998).

M A Harry, The Right of Self-Defense and the Use of Armed Forces against States Aiding Insurgency, 11 S.I.U.L.J. (1987).

L Henkin, How Nations Behave, New York NY; Columbia University Press (1979).

L Henkin, R C Pugh, O Schachter and H Smith, International Law: Cases and Materials, St. Paul MINN; West Publishing Co. (1993).

Hirota et al, International Military Tribunal for the Far East, 1948 A.D. (1948).

K Holsti, Peace and War, Cambridge; Cambridge University Press (1991).

S T Hosmer, The Information Revolution and Psychological Effects, Santa Monica CA; Rand Organization Publications (1999). Available at http://www.rand.org/publications/MR/MR1016.

M Howard, Temperamenta Belli: Can War be Controlled; in M Howard's Restraints on War: Studies in the Limitation of Armed Conflict, Oxford; Oxford University (Lecture Course Papers) (1979).

R Hundley et al., Security in Cyberspace: Challenges for Society, Santa Monica CA; Rand Organization Publications (1996). Available at

http://www.rand.org/publications/MR/MR880/MR880.ch10.htm.

P. Hughes (Lt. Gen. US Army), Global Threats and Challenges: The Decades Ahead, Statement for the Senate Select Committee on Intelligence, January 28th 1998. Available at http://www.globalsecurity.org/intell/library/congress/1999_hr/99020208_tlt.htm.

ICJ Reports 3, The Fisheries Jurisdiction Case (1973).

ICJ Reports 4, The Corfu Channel Case (1949).

ICJ Reports 14, Nicaragua v. USA (merits 1986).

ICJ Reports 226, Advisory Opinion on the Lethality of the Use or Threat of Nuclear Weapons (1996).

ICJ Reports 3, Case Concerning the Barcelona Traction, Light and Power Company, Limited (1970).

ILC Report, Report of the International Law Commission (32nd session) (1980).

ILC Report, Third Report on State Responsibility (1991).

International Information Systems Security Certification Consortium. Available at http://www.isc2.org.

1996 Information Systems Security Survey conducted by WarRoom Research, LC. At http://www.infowar.com.

Information Warfare Tutorial at http://www.iwar.org.uk/iwar/resources/carlisle/iw-tutorial/execsum.htm (2003).

IWS Information Operations, IWAR Chapter at http://www.iwar.org.uk/iwar/ (2004).

Jane's Geopolitical Intelligence Foreign Report (various issues).

See http://www.janes.com/janes.html

P C Jessup, A Modern Law of Nations, New York NY; Macmillan Co. (1956).

Joint Forces Staff College – Joint Command, Control and Information Warfare School, Joint Information Operations Planning Handbook, Washington DC; Joint Forces Staff College (2003).

Joint Pub. 3-13, Joint Doctrine for Information Operations, Washington DC; Joint Chiefs of Staff. Available at http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf.

G Johnson, From Two Small Nodes a Mighty Web has Grown, N.Y. TIMES, October 12, A1 et seq. (1999).

Cf C C Joyner and M A Grimaldi, The United States and Nicaragua: Reflections on the Lawfulness of Contemporary Intervention, 25 V.J.I.L. (1985).

Japan Wages "Cyber War" against Hackers, London Daily Telegraph A4 (October 24, 2000).

M E Kabay, ISCA White Paper on Computer Crime Statistics. Available at http://www.ncsa.com/knowledge/research/comp_crime.htm

B Kahin and C Nesson, Borders in Cyberspace: Information Policy and the Global Information Infrastructure, Cambridge MA; MIT Press (1997).

K H Kaikobad, Self-Defense Enforcement Action and the Gulf Wars 1984-88 and 1990-91, 63 B.Y.B.I.L. (1992).

P G Karaiosifidis, The Air Operations of NATO in Yugoslavia, Athens; Technical Editions Ltd (1999).

PG Karaiosifidis, Operation Enduring Freedom – The War in Afghanistan, Athens; Technical Editions Ltd (2001).

R D Kearny and R E Dalton, The Treaty on Treaties, 64 American Journal of International Law (1970).

The Kellogg-Briand Pact, Stat. 46: 2343, T.S. No. 796, L.N.T.S. 94 (1928).

H Kelsen, Principles of International Law, New York NY; Holt-Rinehart and Winston (1967).

H Kelsen, The Law of the United Nations, London; Stevens and Sons (1950).

H Kelsen, General Theory of Law and State, Cambridge MA; Harvard University Press (1946).

H Kelsen, US Naval War College Int'l Law Studies-Collective Security Under International Law, Newport RI; Naval War College Press (1998).

Z M Khalizad and J P White Eds, Strategic Appraisal: The Changing Role of Information in Warfare, Santa Monica CA; Rand Organization Publications (1999). Available at http://www.rand.org/publications/MR/MR1016.

S P Kanuck, Information Warfare: New Challenges for public international law, Harvard Int'l L. J. 272 (winter 1996).

J Kish, International Law and Espionage, The Hague-London; Nijhoff M. (1995).

D Kuehl, Information Operations: The Hard Reality of Soft Power, Washington DC; Department of Defense (2004).

J L Kunz, Individual and Collective Self-Defense in Art. 51 of the Charter of the United Nations, 41 American Journal of International Law (1947).

Cf M Lachs, The Developments and General Trends of International Law in our Time, 169 R.C.A.D.I.9 (1980).

I O Lesser et al., Countering the New Terrorism, Santa Monica CA; Rand Organization Publications (1999).

Z Li, and B Lihong, Information Warfare Poses Problems, FBIS-CHI-96-014 (2003).

O Lissitzyn, Treaties and Changed Circumstances, 61 American Journal of International Law (1967).

M C Libicki, What is Information Warfare? Centre for Advanced Concepts and Technology Institute for National Strategic Studies, Washington DC; National Defense University (August 1995).

R B Lillich, Economic Coercion and the New International Economic Order, Charlottesville, VA; The Michie Company (1976).

R b Lillich, Forcible Self-Help by States to Protect Human Rights, 53 Io.L.R. (1968).

D K Linnan, Self Defense, Necessity and UN Collective Security: United States and Other Views, Duke Journal of Comparative and International Law 57 (1991).

Livy (edited by Loeb Classical), Ab Urbe Condita, Harvard MA; Harvard University Press (1919).

Y Lobel, The Use of Force to Terrorist Attacks, 24 Yale Journal of International Law (1999).

M Maclachlan, Security Market is maturing but needs Standards, TechWeb News (March 9, 1998). Available at http://www.techweb.com/wire/story/0398iwld/TWB19980309S0015

W Masden et al., Cryptography and Liberty: An International Survey of Encryption Policy, Washington DC; Electronic Privacy Information Centre (1998). Available at http://www.epic.org/alert/EPIC_alert_8.05.html.

MCI, Information on DoSTracker (Oct. 9, 1997). Available at

http://www.security.mci.net/dostracker/prelease.html.

T L H McCormack, Self-Defense in International Law: The Israeli Raid on the Iraqi Nuclear Reactor, New York NY; St. Martin's Press (1996).

M McDougal and F Feliciano, Law and Minimum World Public Order, New Haven CT; Yale University Press (1961).

J McHugh, Forcible Self Help in International Law, Naval War College Review (November-December 1972).

T D McNeeley, Hackers, Crackers and Trackers, The American Legion Magazine (Feb. 1997) at 34. Available at http://www.legion.org/pubs/1997/hackers.htm

L Meeker, Defensive Quarantine and the Law, American Journal of International Law 57 (1963).

R Molander, A Riddile and P Wilson, Strategic Information Warfare: A New Face of War, Santa Monica CA; Rand Organization Publications (1996).

R Molander et al., Strategic Information Warfare Rising, Santa Monica CA; Rand Organization Publications (1998).

A Moller, International Law in Peace and War, London; Stevens and Sons (1935).

J Moore, The Caroline, Digest of International Law 2 (1903).

J N Moore, National Security Law 47, Durham N Carolina; Carolina Academic Press (1990).

J N Moore, Strengthening World Order: Reversing the Slide to Anarchy, 4 A.U.J.I.L.P. (1989).

JN Moore, Development of the International Law of Conflict Management; in National Security Law 47, Durham N Carolina; Carolina Academic Press (1990).

C H Morgan, Why Computer Crime is so Tough, Colorado Springs CO; United States Air Force-Air Force Office of Special Investigations (2002).

T A Morth, Considering our position: Viewing Information Warfare as a Use of Force prohibited by Art. 2(4) of the UN Charter, Case Western Reserve Journal of International Law (1998).

Lt. Col. E F Murphy, Maj. G C Bender, Maj. L J Schaefer, Maj. M M Shepard, and Maj. C W Williamson III (US Air Force), Information Operations: Wisdom Warfare for 2025, Washington DC; Department of the Air Force (2003).

B Nichiporuk and C H Builder, Information Technologies and the Future of Land Warfare, Santa Monica CA; Rand Organization Publications (1995).

B Nichiporuk, US Military Opportunities: Information Warfare Concepts of Operation, in Strategic Appraisal: The Changing Role of Information in Warfare, Santa Monica CA; Rand Organization Publications (1999).

Identic Notes of the United States to Other Governments in Relation to the Pact along With all the Relevant Replies, 22 American Journal of International Law Supp (1929).

A Nussbaum, A Concise History of the law of Nations, New York NY; Macmillan Co (1954).

Oceans Law and Policy Department, Naval War College Centre for Naval Warfare Studies, Annotated Supplement to the Commander's Handbook on the Law of Naval Operations, NWP 1-14M/ MCWP 5-2.1/ COMDTPUB P5800.1, Newport RI; Naval War College Press (1997).

R Oppenhaim, International Law, London; Longmans-Green and Co (1955).

J Parker, Introduction in George Chapman's Homer, Ware; Woodsworth Ed. (2000).

J Paust and A Blaustein, The Arab Oil Weapon, Dobbs Ferry NY; Oceana (1977).

PC Gamer-The World's Best Selling Games Magazine, Brisbane CA; Imagine Media (December 2001).

A Pearce, The Hague Conference and other International Conferences concerning the Laws and Usages of War: Text of Conventions with Notes, London; Stevens and Sons (1904).

C Phillipson, The International Law and Custom of Ancient Greece and Rome, S.I; Macmillan (1919).

E J Pollock and A Petersen, Serbs Take Offensive in the First Cyber War, Wall Street Journal A8 (1999).

President of the United States Memorandum to Secretary of Defense, Washington DC; White House Printing Office (September 29, 1999).

The Public Record Office, The Enigma Papers, London; Public Record Office (2003).

K W Quigley, A Framework for Evaluating the Legality of the United States Intervention in Nicaragua, 17 N.Y.U.J.I.L.P. (1985).

A Randelzhofer, The Charter of the United Nations: A Commentary, Oxford; Oxford University Press (1995).

A Rathmell, Cyber-Terrorism: The Shape of Future Conflict, RUSI Journal 40-45 (October 1997).

A Rathmell, Strategic Information Warfare: Responding to the Threat, Centre for Defense studies, Brassey's Defense Yearbook (1998).

A Rathmell, R Overill, L Valeri and J Gearson, The IW Threat from Sub-State Groups: An Interdisciplinary Approach, presented at the Third International Symposium on Command and Control Research and Technology, June 17-20 1997 at http://www.kcl.ac.uk/orgs/icsa/terrori.htm.

W M Reisman, Coercion and Self-Determination: Construing Charter Art. 2(4), 78 American Journal of International Law (1984).

Report on the President's Commission on Critical Infrastructure Protection (a series of 12 reports). See http://www.pccip.gov/report_index.html

Restatement (Third) of Foreign Relations

2 R.I.A.A. 1012, Portugal v. Germany (1982).

2 R.I.A.A. 1011, Naulilaa Case (1928).

A Roberts and R Guelff, Documents on the Laws of War, Oxford; Oxford University Press (2000).

H B Robertson Jr., Contemporary International Law: Relevant to Today's World? Naval War College Review (Summer-1992).

A P V Rogers, Law on the Battlefield, Manchester; Manchester University Press (1996).

N Ronziti, Resort to Force by States to Protect Nationals, Va. J. Int'l. Law 21 (1981).

N Ronziti, Rescuing Nationals Abroad Trough Military Coercion and Intervention on Grounds of Humanity, Dordrecht; Nijhoff M. (1985)

R Rosenstock, The Declaration of Principles of International Law Concerning Friendly Nations: A Survey, Am. J. Int'l Law 53 (1971).

AW Rovine, Contemporary Practice of the United States Relating to International Law, Am. J. Int'l Law 65 (1974).

R Russell and J Muther, A History of the United Nations Charter: The Role of the United States 1940-1945, Washington DC; Brooking Institution (1958).

R Saduska, Threats of Force, 82 American Journal of International Law (1988).

J Shapiro, Information and War: Is it a Revolution? Santa Monica CA; Rand Organization Publications (1999). Available at http://www.rand.org/publications/MR/MR1016/MR1016.chap5.pdf.

N M Shaw, International Law, Cambridge; Grotius (1997).

O Schachter, The Right of States to use Armed Force, Mich. L. Review (1998).

O Schachter, In Defense of International Rules on the Use of Force, University of Chicago Law Review 53 (1986).

O Schachter, International Law in Theory and Practice (1991).

O Schachter, The Enforcement of International Judicial and Arbitral Decisions, 54 American Journal of International Law (1960).

O Schachter, Just War and Human Rights, 1 P.Y.I.L. (1989).

O Schachter, The Legality of Pro-Democratic Invasion, 78 American Journal of International Law (1984).

O Schachter International Law in the Hostage Crisis: Implications for Future Cases, New Haven CT-London; Yale University Press (1985).

O Schachter, The Lawful Use of Force by A State against Terrorists in Another Country, 19 I.Y.H.R. (1989).

O Schachter and C C Joyner, United Nations Legal Order, Cambridge; Grotius (1995).

M N Schmitt, Computer Network Attack and the Use of Force in international law: Thoughts on a normative framework, 37 Columbia J. Int'l L 885 (1999).

M N Schmitt and B T O'Donnell, Computer Network Attack and International Law (US Naval War College International Law Studies Volume 76 (2001).

MN Schmitt, Bellum Americanum: The US View of Twenty First Century War and its Possible Implications for the Law of Armed Conflict 19 Michigan Journal of International Law (1998).

R D Scott, Legal Aspects of Information Warfare: Military Disruption of communications, 45 Naval L. Rev. 57 (1998).

WG Sharp, International Peace and Security: Current Legal Problems, Washington DC; Georgetown University Law Centre (Course Lecture Materials) (1998).

B Simma, NATO the UN and the Use of Force – Legal Aspects, 10 E.J.I.L. (1999).

A Sofaer, Sixth Annual Waldemar A. Solf Lecture: International Terrorism, the Law and the National Defense, Military Law Review (1989).

A Sofaer and S E Goodman, A Proposal for an International Convention on Cyber crime and Terrorism, Stanford CA; Stanford University Centre for International Security and Cooperation (2000).

G Shultz, Low Intensity Warfare: The Challenge of Ambiguity, Washington DC; Address to the Low Intensity Warfare Conference-Department of State (1986).

T Spangler, Rapid Consolidation in Security Market, Webweek (Dec 8, 1997). Available at http://www.internetworld.com/print/1997/12/08/news/19971208-rapid.html

M Stephen, Sea Battles in Close Up: World War II, Annapolis, Naval Institute Press (1988).

J Stone, Aggression and World Order, London; Stevens and Sons (1958).

W Schwartau, Information Warfare, New York: Thunder's Mouth Press 2nd edition (1996).

Suarez (edited by Classics of International Law), De Triplici Virtute Theologica Charitate, S.I; Carnegie Endowment for International Peace (1944).

M Sussmann, The Critical Challenges from International High-Tech and Computer Related Crime at the Millennium, 9 Duke Journal of Comparative and International Law (1999).

H Taylor, A Treatise on International Public Law, Chicago IL; Callaghan and Company (1901).

J P Terry, Responding to Attacks on Critical Computer Infrastructure: What Targets?
What Rules of Engagement? Naval Law Review XLVI 170-187 (1999).

Textor (edited by Classics of International Law), Synopsis Juris Gentium, S.I; Carnegie Endowment for International Peace (1925).

H Thirlway, International Customary Law and Codification, Leiden; A. W. Sijthoff (1972).

Thomas and Duncan, The Annotated Supplement to the Commander's Handbook on the Law of Naval Operations, Newport RI; Naval War College Press (1997).

A V W Thomas and A J Thomas, The Concept of Aggression in International Law, Dallas; Southern Methodist University Press (1972).

R D Thomas, The Nation's Cutting Edge Cyber detective-A kind of Private Eye. Available at http://www.pimall.com/nais/n.seanor.html

A Toffler and H. Toffler, Foreword to In Athena's Camp: Preparing for Conflict in the Information Age, Santa Monica CA; Rand Organization Publications (1997).

Cf G Townsend, State Responsibility for Acts of De Facto Agents, 14 A.J.I.C.L. (1997).

R W Tucker, Reprisals and Self-Defense: The Customary Law, 66 American Journal of International Law (1972).

US Department of the Army, Field Manual No. 100-6 Information Operations, Washington DC; Department of the Army (2003).

US Department of the Army, United States Operational Law Handbook, Washington DC; Department of the Army (1996).

US Department of the Air Force, Cornerstones of Information Warfare 2, Washington DC; Department of the Air Force (1995).

US Department of the Air Force, International Law: The Conduct of Armed Conflict and Air Operations, Washington DC; Department of the Air Force (1999).

US Department of the Air Force, Air Force Doctrine Document 2-5 Information Operations, Washington DC; Department of the Air Force (2003).

US Department of Defense, Active Defense against Peacetime Computer Intrusions, Washington DC; Department of Defense (1998).

US Department of Defense, Directive S-3600.1, Information Operations, Washington DC; Department of Defense (1996).

US Department of Defense, Joint Chiefs of Staff, Information Assurance: Legal, Regulatory, Policy and Organizational Considerations 3rd edition, Washington DC; Joint Chiefs of Staff (September 17th 1997).

US Department of Defense, Joint Chiefs of Staff, Joint Publication 3-13 Joint Doctrine for Information Operations, Washington DC; Joint Chiefs of Staff (2000).

US Department of Defense, Joint Publication 3-13, Joint Doctrine for Information Operations, Washington DC; Department of Defense (1998).

US Department of Defense, Instruction 5000.1, Defense Acquisition, Washington DC; Department of Defense (1996).

US Department of Defense, Dictionary of Military and Associated Terms, Washington DC; Department of Defense (1999).
Available at http://www.dtic.mil/doctrine/jel/c_pubs.html

US Department of Defense, Instruction 5000.2, Defense Acquisition Management Policies and Procedures, Washington DC; Department of Defense (1991).

US Department of Defense, Joint Vision 2010, Washington DC; Department of Defense (1999).

US Department of Defense, Joint Vision 2020, Washington DC; Department of Defense (2004).

US Department of Defense, Office of the General Counsel: An Assessment of International Legal Issues in Information Operations, Washington DC; Department of Defense (1999).

US Department of Defense-TRADOC Pamphlet 525-69 – The Force XXI Army: Concept for Information Operations, Washington DC; Department of the Army (1995).

US Department of Defense, Protecting the Homeland: Report of the Defense Science Board Task Force on Defensive Information Operations, Washington DC; Department of Defense (2004).

US Department of Justice, Computer Crime and Intellectual Property Section, International Aspects of Computer Crime, Washington DC; Department of Justice (2000).
Available at http://www.usdoj.gov/criminal/cybercrime/intl.html

US National Research Council, Communiqué to Review Department of Defense C4I Plans and Programs, Realizing the Potential of C4I: Fundamental Challenges, Washington DC; National Research Council (1999).

US Naval War College, International Law Studies, Collective Security under International Law, Newport RI; Naval War College Press (1997).

US Naval War College, International Law Studies, Volume 72, The Law of Military Operations, Newport RI; Naval War College Press (1998).

US Navy (USCINCLANT), Legal Aspects of Offensive information Warfare: Information Memorandum 1 – US Commander in Chief Atlantic Memorandum 5800 J20L, Norfolk VA; USCINCLANT (1996).

US Navy, Tentative Instructions Governing Maritime and Aerial Warfare, Washington DC; Department of the Navy (May 1941).

US Executive Order no. 13.010, 61 Fed. Reg. 37347.

US Presidential Decision Directive 62, Combating Terrorism, Washington DC; White House Printing Office (1998).

US Presidential Decision Directive 63, Critical Infrastructure Protection, Washington DC; White House Printing Office (1998).

United Nations Manual on the Prevention and Control of Computer Related Crime (2000). Available at http://www.ifs.univie.ac.at/~pr2gq1/rev434.html

C Vulcan, L' Execution des Decisions de la Court Internationale de Justice d' après la Charte des Nations Unies, 51 R.G.D.I.P. (1947).

L Valeri, Guarding against a New Digital Enemy, Jane's Intelligence Review 379-382, (August 1997). Available at http://www.janes.com/janes.htm

Victoria (edited by Classics of International Law), De Indis et Jure Belli Relectiones, S.I; Carnegie International Endowment for Int'l Peace (1917).

C H M Waldock, The Regulation of the Use of Force by Individual in International Law, 81 R.C.A.D.I. (1952).

G K Walker, Anticipatory Collective Self-Defense in the Charter Era: What the Treaties Have Said, Cornell International Law Journal 321 (1998).

G K Walker, Information Warfare and Neutrality, 33 Vanderbilt Journal of Transnational Law 1082 (2000).

F P A Walters, A History of the League of Nations, London; Oxford University Press (1952).

War Room Research, LLC, 1996 Information Systems Security Survey (1996).
Available at
http://www.warroomresearch.com/wrr/SurveysStudies/1996ISS_Survey_SummaryResults.htm.

W H Ware, The Cyber Posture of the National Information Infrastructure, Santa Monica CA; Rand Organization Publications (1998).

R Wedgwood, Responding to Terrorism: The Strikes against Bin Laden, 24 Y.J.I.L. (1999).

H Wehberg, The Outlawry of War, S.N; Washington DC; Carnegie Endowment for Int'l Peace (1931).

W Wengler, L' Interdiction de Recourir a` la Force-Problemes et Tendances, 1971 R.B.D.I. (1971).

M Wertheim, The Pearly Gates of Cyberspace: A History of Space from Dante to the Internet, New York NY; Norton (1999).

The White House, Office of the Press Secretary, Fact Sheet: Summary of Presidential Decision Directives 62 and 63. Available at http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1998/5/22/6.text.1

M Whiteman, Digest of International Law V (1965).

T C Wingfield, Cyberspace and the Use of Force, Washington DC; Aegis Group (2004).

T C Wingfield, Legal Aspects of Offensive Information Operations in Space (2003). Available at http://www.usafa.af.mil/dfl/documents/wingfield.doc

T C Wingfield, An Introduction to Legal Aspects of Operations in Cyberspace, Monterey CA; Naval Postgraduate School (2004).

J L Woodward, Statement to the House Armed Services Committee (2001). Available at http://www.globalsecurity.org/military/library/congress/2001_hr/01-05-17woodward.htm

K Wolfke, Custom in Present International Law, Dodrecht-London; Nijhoff M. (1993).

W Wong, Security Software Companies continue Consolidation, Techweb News (Feb. 24, 1998). Available at http://www.techweb.com/wire/story/TWB19980224S0011

B Yeltsin, The Russian Federation President's Inauguration Speech for the Official Installment of the New Minister of Defense (1996). Available at http://lgi.osi.hu/publications/

H Yeo and H Killo, The Evolution of Military Information Warfare, http://www.geocities.com/collegePark/Quad/8813/main.html.

P L Zanardi, Indirect Military Aggression, Dordrecht-London; Nijhoff M. (1986).

L Zhoumin, Information Warfare and Training of Skilled Commanders, FBIS-CHI-96-036 (2003).

J Zourek, Enfin une Definition de l'Agression, 20 A.F.D.I. (1974).

Also http://www.dia.smil.mil/admin/EARLYBIRD/010226/e20010226usshifts.htm

Also http://www.dtic.mil/defense link

Also http://www.Infowar.Com/mil_c4I_071098c_j.html-ssi.

Also http://www.ndu.edu/

Also http://www.nwc.navy.mil/

Also http://www.google.com.

LIST OF ABBREVIATIONS

A.C.	Appeal Cases
A.D.	Annual Digest and Reports of Public International Law
A.F.D.I.	Annuaire Francais de Droit International
A.I.D.I.	Annuaire de L'Institute de Droit International
A.J.I.C.L.	Arizona Journal of International and Comparative Law
A.J.I.L.	American Journal of International Law
A.L.R.	Alberta Law Review
A.P.S.R.	American Political Science Review

A.S.J.G.	Acta Scandinavica Juris Gentium
A.U.I.L.R.	American University International Law Review
A.U.J.I.L.P.	American University Journal of International Law and Policy
A.Y.B.I.L.	Australian Yearbook of International Law
A.U.L.R.	American University Law Review
Auck.U.L.R.	Auckland University Law Review
B.F.S.P.	British and Foreign State Papers
B.J.I.L.	Brooklyn Journal of International Law
B.Y.B.I.L.	British Yearbook of International Law
C.J.T.L.	Columbia Journal of International Law
C.T.S.	Consolidated Treaty Series
C.W.I.L.J.	California Western International Law Journal
C.W.R.J.I.L.	Case Western Reserve Journal of International Law
C.Y.I.L.	Canadian Yearbook of International Law
Cam.L.J.	Cambridge Law Journal
Col.L.R.	Columbia Law Review
Cor.L.R.	Cornell Law Review
D.J.C.I.L.	Duke Journal of Comparative and International Law
D.J.I.L.P.	Denver Journal of International Law
D.L.J.	Denver Law Journal
D.S.B.	Department of State Bulletin
E.J.I.L.	European Journal of International Law
E.P.I.L.	Encyclopedia of Public International Law
F.	Federal
For. Aff.	Foreign Affairs
G.J.I.C.L.	Georgia Journal of International and Comparative Law
G.Y.I.L.	German Yearbook of International Law
H.I.C.I.L.	Hastings International and Comparative Law Review
H.I.L.J.	Harvard International Law Journal
Har.L.R.	Harvard Law Review
Hof.l.r.	Hofstra Law Review
I.C.J.Rep.	International Court of Justice Reports
I.C.L.Q.	International and Comparative Law Quarterly
I.J.I.L.	Indian Journal of International Law
I.L.C. Ybk	International Law Commission Yearbook
I.L.M.	International Legal Materials
I.L.Q.	International Law Quarterly
I.L.R.	International Law Reports
I.M.T.	Trial of Major War Criminals before the International Military Tribunal

I.R.R.C. International Review of the Red Cross
I.Y.H.R. Israel Yearbook of Human Rights
I.Y.I.L. Italian Yearbook of International Law
Int.Aff. International Affairs
Int.Con. International Conciliation
Int.Leg. International Legislation
Int.Rel. International Relations
Io.L.R. Iowa Law Review
Is.L.R. Israel Law Review
J.I.L.E. Journal of International Law and Economics
J.Y.I.L. Jewish Yearbook of International Law
Jur.R. Juridical Review
Ken.L.J. Kentucky Law Journal
L.C.P. Law and Contemporary Problems
L.J.I.L. Leiden Journal of International Law
L.N.T.S. League of Nations Treaty Series
L.Q.R. Law Quarterly Review
L.R.T.W.C. Law Reports of Trials of War Criminals
M.P.Y.U.N.L. Max Planck Yearbook of United Nations Law
Mar.J.I.L.T. Maryland Journal of International Law and Trade
Mer.L.R. Mercer Law Review
Mich.J.I.L. Michigan Journal of International Law
Mich.L.R. Michigan Law Review
Mil.L.R. Military Law Review
Mod.L.R. Modern Law Review
N.I.L.R. Netherlands International Law Review
N.M.T. Trials of War Criminals before the Nuremberg Military Tribunals under Control Council Law No. 10
N.W.C.R. Naval War College Review
N.Y.I.L. Netherlands Yearbook of International Law
N.Y.L.S.J.I.C.L. New York University Journal of International and Comparative Law
N.Y.U.J.I.L.P. New York University Journal of International Law and Politics
P.A.S.I.L. Proceedings of the American Society of International Law.
P.S.Q. Political Science Quarterly
P.Y.I.L. Pace Yearbook of International Law
R.B.D.I Revue Belge de Droit International
R.C.A.D.I. Recueil des Cours de l'Academie de Droit International
R.D.S.C. Resolutions and Decisions of the Security Council
R.E.D.I. Revue Egyptienne de Droit International

R.G.A. Resolutions adopted by the General Assembly
R.G.D.I.P. Revue Generale de Droit International Public
R.I.A.A. Reports of International Arbitral Awards
R.I.D.P. Revue Internationale de Droit Penal
R.S.I.D.M.D.G. Recueils de la Societe Internationale de Droit Militaire et de Droit de la Guerre
S.D.L.R. San Diego Law Review
S.I.U.L.J. Southern Illinois University Law Journal
S.J.I.L. Stanford Journal of International Law
S.J.I.L.C. Syracuse Journal of International Law and Commerce
S.J.L.R. Saint John's Law Review
Sp. Special
Supp. Supplement
T.G.S. Transactions of the Grotius Society
T.I.L.J. Texas International Law Journal
Tul.L.R. Tulane Law Review
U.C.L.R. University of Chicago Law Review
U.L.R. Utah Law Review
U.N.J.Y. United Nations Juridical Yearbook
U.N.T.S. United Nations Treaty Series
U.T.L.R. University of Toledo Law Review
V.J.I.L. Virginia Journal of International Law
V.J.T.L. Vanderbilt Journal of Transnational Law
Vill.L.R. Villanova Law Review
Vir.L.R. Virginia Law Review
W.C.R. World Court Reports
W.L.L.R. Washington and Lee Law Review
W.U.L.Q. Washington University Law Quarterly
W.V.L.R. West Virginia Law Review
Y.B.W.A. Year Book of World Affairs
Y.J.I.L. Yale Journal of International Law
Y.L.J. Yale Law Journal
Z.A.O.R.V. Zeitschrift fur Auslandisches Offentliches Recht und Volkerrecht