Cyber Warfare: The Effects of Technological Advancements in Expanding the Concept of War and the Role of Non-state Actors and Individuals

Ira Paulo A. Pozon[★]
Anthony Edsel Conrad F. Tupaz[★★]

> *We shall go on to the end. We shall fight in France, we shall fight on the seas and oceans, we shall fight with growing confidence and growing strength in the air, we shall defend our island, whatever the cost may be.*
>
> *We shall fight on the beaches, we shall fight on the landing grounds,*
>
> *We shall fight in the fields and in the streets; we shall fight in the hills;*
>
> *We shall never surrender.*
>
> — Winston Churchill[1]

★ '09 J.D., Far Eastern University; '08 M.B.A., De La Salle University. The Author serves as Legal Counsel to the Vice President of the Republic of the Philippines, Hon. Jejomar C. Binay. He was also appointed by the Vice President to head the Special Concerns Unit of the Office of the Vice President and to be deputy head of the Vice President's Office for Foreign Affairs (VPFA). He currently teaches at the Pamantasan ng Lungsod ng Maynila College of Law and the Universidad de Manila. His previous works in the *Journal* include: *Subjudice and Judicial Privilege in the Impeachment*, 57 ATENEO L.J. 706 (2013) & *Public Accountability: An Analysis of the Horizontal and Vertical Accountability Measures in Philippine Law*, 57 ATENEO L.J. 767 (2013).

★★ '08 L.L.M., Harvard Law School; '03 J.D., *with honors*, Ateneo de Manila University School of Law; Member, New York Bar. The Author was a private prosecutor for the House of Representatives Prosecution Panel during the Impeachment Trial of Chief Justice Corona. He was counsel of the Philippine Truth Commission prior to the Supreme Court's declaration of its unconstitutionality. He teaches subjects on comparative and international law at the De La Salle University-Far Eastern University Joint MBA-JD Program and the Philippine Christian University (PCU) College of Law. He is also a bar review lecturer on public

I. INTRODUCTION

Traditionally, international law characterizes warfare as both an action and a state of conflict between sovereigns (or at least *de facto* sovereigns) through the use of armaments and soldiers to enforce the demands of one such combatant state over another.[2] These definitions limit the frontiers of war to merely land, sea, and air, and apparently negate the possibility of individuals or non-state actors (such as corporations) from having direct legal personality in the conduct of war.

However, the advent of technology, the creation of the Internet, and the rise of the current digital age, have brought about the evolution of a new species of warfare, that of cyber warfare.[3] Cyber warfare has gained military significance over the past few years, with armed forces and intelligence agencies focusing on securing classified information and military computer systems. Most recently, as part of its military exercises, the Iranian Navy

---

international law and constitutional law at the PCU College of Law. He also taught at the New England School of Law, Boston, Massachusetts. He was Managing Technical Editor of the Harvard Human Rights Journal. He is the owner and managing partner of Tupaz & Associates, a public interest law firm. He was previously an Editor and Staff of the *Ateneo Law Journal*. His past works published in the *Journal* include: *Subjudice and Judicial Privilege in the Impeachment*, 57 ATENEO L.J. 706 (2013); *Public Accountability: An Analysis of the Horizontal and Vertical Accountability Measures in Philippine Law*, 57 ATENEO L.J. 767 (2013); *Expatriates and Retirees Coming to the Philippines: Giving Up U.S. Citizenship and the U.S. Exit Tax*, 56 ATENEO L.J. 1 (2011); *The Mindanao Question: Constitutional Dialogue in Southern Philippines*, 54 ATENEO L.J. 1 (2009); *Constitutional Courts in Divided Societies: A Call for Scholarship on International Intervention in Constitutional Law and Politics*, 53 ATENEO L.J. 324 (2008); *Deliberative Democracy and Weak Courts: Constitutional Design in Nascent Democracies*, 53 ATENEO L.J. 343 (2008); *Self-Determination as "Defined" Under the United Nations Draft Declaration on the Rights of Indigenous Peoples: Secession or Autonomy?*, 51 ATENEO L.J. 1039 (2007); *Ruiz v. Court of Appeals: A Moral Hazard*, 49 ATENEO L.J. 982 (2004); *A Synthesis on the Colloquium on Indigenous Peoples*, 47 ATENEO L.J. 775 (2002); & *The People Power and the Supreme Court in Estrada v. Arroyo*, 47 ATENEO L.J. 8 (2002).

Cite as 57 ATENEO L.J. 1065 (2013).

1. Winston Churchill, Prime Minister of Britain, We Shall Fight on the Beaches, Address at the House of Commons (June 4, 1940) (transcript *available at* http://www.winstonchurchill.org/learn/speeches/speeches-of-winston-churchill/128-we-shall-fight-on-the-beaches (last accessed Feb. 28, 2013)).
2. *See generally* ISAGANI A. CRUZ, INTERNATIONAL LAW 221 (2003 ed.).
3. *See* Channel News Asia, Iran stages cyber warfare drill: reports, *available at* http://www.channelnewsasia.com/stories/afp_world/view/1245314/1/.html (last accessed Feb. 28, 2013).

conducted cyber attacks on the computer systems of its defensive forces.[4] While the preparedness of Iran may appear to some as a case of technological paranoia, a report from The Economist[5] explains the back-and-forth use of cyber warfare tactics between states. In that report, cyber attacks were said to have been conducted by Iran in the release of the Shamoon virus that crippled numerous computer systems in Aramco and RasGas in the Kingdom of Saudi Arabia and Qatar, respectively.[6] Also alleged was that either the United States (U.S.), Israel, or both cooperatively, launched the Stuxnet worm and the Flame virus, the former designed to paralyze the centrifuges of the Iranian Natanz uranium-enrichment plant, while the latter's goal was to infect Iranian computers connected with oil production.[7]

Perhaps more alarming is the admission of the U.S. Defense Department that, in July 2011, its computer networks were hacked by a "foreign intelligence service" that gained access to 24 thousand highly confidential files on missile tracking systems and unmanned drones.[8]

It is these threats against U.S. domestic security that was the key issue in the speech of Secretary of Defense Leon Panetta. He warned of the possibility of a "cyber Pearl Harbor" and noted the significant susceptibility of key computer networks controlling power utilities, transportation systems, finance, and the government.[9] He declared that

> [t]he Internet is open. It [is] highly accessible, as it should be. But that *also presents a new terrain for warfare*. It is a battlefield of the future where adversaries can seek to do harm to our country, to our economy, and to our citizens.
>
> I know that when people think of cybersecurity today, they worry about hackers and criminals who prowl the Internet, steal people's identities, steal sensitive business information, steal even national security secrets. Those threats are real and they exist today.

---

4. *Id.*
5. *Hype and Fear*, ECONOMIST, Dec. 8, 2012, *available at* http://www.economist.com/news/international/21567886-america-leading-way-developing-doctrines-cyber-warfare-other-countries-may (last accessed Feb. 28, 2013).
6. *Id.*
7. *Id.*
8. Alfonso F. Serrano, *Cyber Crime Pays: A $114 Billion Industry*, THE FISCAL TIMES, Sep. 14, 2011, *available at* http://www.thefiscaltimes.com/Articles/2011/09/14/Cyber-Crime-Pays-A-114-Billion-Industry.aspx#page1 (last accessed Feb. 28, 2013).
9. Leon E. Panetta, Secretary of Defense of the United States, Remarks at a gathering of the Business Executives for National Security in New York City (Oct. 11, 2012) (transcript *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136 (last accessed Feb. 28, 2013)).

> But the even greater danger — the greater danger facing us in cyberspace goes beyond crime and it goes beyond harassment. A cyber attack perpetrated by nation states [or] violent extremists groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation.[10]

In describing the manner of cyber attacks against the U.S., Panetta cited that aggressor nations or extremists could potentially derail trains, contaminate water supplies, and shutdown power grids.[11] He also noted that cyber attacks could be utilized not only by states but also by non-state actors to compromise U.S. defensive capabilities in preparation for an actual physical attack, which collectively could result in "a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life."[12]

We argue that this new form of warfare allows for the direct participation of both individuals and other non-state actors, shifting the conflict to a digital battlefield, and is not governed by any treaty or convention establishing the rules of conduct. This revolutionary form of warfare completely deviates from traditional warfare on many aspects which we discuss in detail.

In the second part of this Article, we discuss the traditional form of warfare, its status under international law, and the corresponding roles of individuals and non-state actors. In the third part, we discuss the legal and technological aspects of cyber warfare and how cyber warfare has increasingly expanded not just the concept of war and but also the roles of non-state actors. Finally, in the fourth part we discuss various recommendations for the legal framework to govern the conduct of cyber warfare.

II. TRADITIONAL DEFINITION OF WAR

Warfare has traditionally been considered as an armed contention through the use of armaments between the public forces of states or belligerent communities and implies the use of violence as a necessary means of enforcing their respective demands.[13]

War in the legal sense has been traditionally thought of as the recognized status of hostilities between nation-states.[14]

---

10. *Id.* (emphasis supplied).

11. *Id.*

12. *Id.*

13. CRUZ, *supra* note 2, at 221.

14. JAMES FOX, DICTIONARY OF INTERNATIONAL AND COMPARATIVE LAW 356 (3d ed. 2003).

This traditional and arguably antiquated concept of war is explained by Justice Stukes in *West v. Palmetto State Life Insurance*.[15] He writes:

> *War* in the legal sense is the *state of nations* among whom there is an interruption of all pacific relations and *a general contestation of arms by authority of the several sovereigns*; it is not a mere contest of force, but must be an armed struggle *carried on between two political bodies* each of which exercises de facto authority over persons within a determinate territory, and its existence is determined by the authorized political department of the government. *So, lawful war can never exist without the actual concurrence of the war-making power*, but may exist prior to any contest of the armed forces.[16]

Subsequently, Justice Hays in *Pan American World Airways, Inc v. Aetna Casualty & Surety Co*.[17] reiterated a similar legal sentiment:

> *War* has been defined *almost always as the employment of force between governments or entities essentially like governments*, at least de facto.
>
> ...
>
> The cases establish that *war is a course of hostility engaged in by entities that have at least significant attributes of sovereignty*. Under international law[,] *war* is waged by states or state-like entities.[18]

As to the viewpoint of war in international law, two branches are dominant, namely *jus ad bellum* and *jus in bello*.[19] As described by the International Law of War Association, the former refers for the rules or conditions when war or other forms of force may be justified, while the latter refers to the manner and conduct to be observed by the party-combatants in the performance of war or armed conflict.[20]

Historically the codes of conduct comprising *jus ad bellum* were codified through treaties and conventions. Among the more prevalent rules of conduct include those regulating sea warfare,[21] the use of expanding bullets,

15. West v. Palmetto State Life Insurance, 25 S.E. 2d 475 (S.C. 1943) (U.S.).

16. *Id.* at 477 (citing 93 C.J.S. *War & National Defense* § 1) (emphases supplied).

17. Pan American World Airways, Inc v. Aetna Casualty & Surety Co., 505 F.2d 989 (2d Circ. 1974) (U.S.).

18. *Id.* at 1012 (emphases supplied).

19. International Law of War Association, Chapter ONE: Introduction to the Law of War, *available at* http://lawofwar.org/introduction.htm (last accessed Feb. 28, 2013).

20. *Id.*

21. *See generally* SIR FRANCIS PIGGOT, THE DECLARATION OF PARIS, 1856: A STUDY 189-97 (1919 ed.).

asphyxiating and poisonous gases, and bacteriological warfare,[22] the regulation of submarine warfare,[23] the treatment of wounded, sick, and prisoners of war,[24] and the non-proliferation and disarmament of nuclear weapons.[25]

Perhaps most glaring is the prohibition contained in the Charter of the United Nations (Charter) from the use or threat of force by states as a means of resolving political and territorial conflicts between themselves.[26] This provision of the constituent treaty states that "*All members shall refrain* in their international relations *from the threat or use of force against the territorial integrity or political independence of any state*, or in any other manner inconsistent with the [p]urposes of the United Nations."[27]

This provision is clearly in line with the outright declaration of commitment to the proscription of war contained in the very Preamble of the Charter, which states that the United Nations (U.N.) is determined "to save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind."[28]

Despite this, the same Charter has provided for certain exceptions, namely self-defense and Security Council authorization.[29] On self-defense, the Charter provides that

> [n]othing in the present Charter shall impair *the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations*, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at

22. *See generally* Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare pmbl., *opened for signature* June 17, 1925, 94 L.N.T.S 65.

23. *See generally* Treaty for the Limitation of Naval Armament, *adopted* Apr. 22, 1930, 112 L.N.T.S. 65.

24. *See generally* Convention relative to the Treatment of Prisoners of War, *opened for signature* July 27, 1929, 118 L.N.T.S. 2734.

25. *See generally* Treaty on the Non-Proliferation of Nuclear Weapons, *opened for signature* July 1, 1968, 729 U.N.T.S. 161.

26. U.N. Charter art. 2, ¶ 4.

27. *Id.* (emphasis supplied).

28. *Id.* pmbl.

29. *Id.* arts. 39-51.

> any time such action as it deems necessary in order to maintain or restore international peace and security.[30]

This Proviso recognizes a state's right to self-defense against any armed attack by another state, albeit in a temporary manner until the Security Council is able to enforce security measures. The exercise of this right was expounded and critiqued heavily in the case of *Nicaragua v. United States*,[31] involving the alleged activities of the U.S. in attacks on Nicaraguan facilities and naval vessels, the mining of Nicaraguan ports, invasion of Nicaraguan air space, and the training, arming, equipping, financing, and supplying of revolutionary forces seeking to overthrow the Sandinista government. The International Court of Justice (I.C.J.) ruled that these activities constituted an unlawful use of force, that the U.S. had breached its obligations under international law, and that it violated Article 51 of the Charter because the use of force was not prompted by an armed attack by Nicaragua against the political and territorial integrity of the U.S.[32]

Nicaragua also clarified further that the use of force must be necessary to defend the state against an external act of aggression by another state, and that this use of force must have immediately succeeded the external armed attack or act of aggression.[33] Finally, the I.C.J. also added the proportionality requirement, necessitating the force in retaliation to be proportionate to the damage caused by the external aggression or attack.[34]

An additional exception under the Charter is found under Chapter VII, allowing the use of force upon authorization from the Security Council. The U.N. Charter states that "[t]he Security Council shall *determine the existence of any threat* to the peace, breach of the peace, or act of aggression and *shall make recommendations, or decide what measures shall be taken* in accordance with Articles 41 and 42, to maintain or restore international peace and security."[35]

Following this provision and further provisions in the Charter, it is clear that the Security Council is authorized to determine any threats or acts of aggression in international disputes, and is empowered to decide the appropriate measures to resolve the conflict between two competing states.[36]

---

30. *Id.* art. 51 (emphasis supplied).

31. Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14 (June 27).

32. *Id.* at 60–75.

33. *Id.* at 103–25

34. *Id.*

35. U.N. Charter art. 39 (emphasis supplied).

36. *Id.* arts. 39, 41, & 42.

Also, it is expressly provided that the Security Council itself may engage in the use of armed forces in order to resolve the conflict.[37]

Internationally accepted customs are also the source of exceptions to the general prohibition on recourse to war, justifying incursion into a sovereign territory and engagement of armed conflict in cases of humanitarian intervention, peacekeeping operations, and wars of national liberation.[38]

A. Role of Individuals and Non-State Actors

In centuries past, the role of individuals in the conduct of war was limited mainly to the focus on humanitarian considerations.[39] Care was usually, albeit belatedly, placed on condemning war due to its ill effects on the civilian populace.[40] Whether as unfortunate victims considered merely as collateral damage[41] or as active participants acting outside of the military,[42] civilian individuals have had a very small role to play in the traditional conduct of war.

It would appear that the actual participation of individuals in the conduct of war results in legal incongruities and challenges. We take cue from the article of George P. Fletcher in arguing that civilians engaged in combat and detained by the enemy must be treated in the same manner as prisoners of war,[43] the treatment of which is governed by the Geneva Convention.[44]

---

37. *Id.* arts. 44-51.

38. *See generally* Cornelia Sorabji, *Managing memories in post-war Sarajevo: individuals, bad memories, and new wars*, 12 J. ROYAL ANTHROPOLOGICAL INST. 1, 4-14 (2006). *See also* JOHUA S. GOLDSTEIN, WAR AND GENDER: HOW GENDER SHAPES THE WAR SYSTEM AND VICE VERSA 10-34 (2001 ed.).

39. Sorabji, *supra* note 38, at 4-14.

40. *Id.*

41. *Id.*

42. *See generally* STATHIS N. KALYVAS, THE LOGIC OF VIOLENCE IN CIVIL WAR 14-32 (2006). *See also* Stathis N. Kalyvas, The Logic of Violence in Civil War (An Unpublished Paper for the New York University Department of Politics) 5-18, *available at* http://humansecuritygateway.com/documents/KALYVAS_LogicOfViolence_CivilWar.pdf (last accessed Feb. 28, 2013) & DAVID KILCULLEN, THE ACCIDENTAL GUERRILLA: FIGHTING SMALL WARS IN THE MIDST OF A BIG ONE 28-38 (2009 ed.).

43. George P. Fletcher, *On Justice and War: Contradictions in the Proposed Military Tribunals*, 25 HARV. J. L. & PUB. POL'Y 635, 639 (2002) (citing *Ex parte* Quirin, 317 U.S. 1, 34 (1942)).

44. Convention relative to the Treatment of Prisoners of War, *supra* note 24, art. 2. This Article provides that "[p]risoners of war are in the power of the hostile Government, but not of the individuals or formation which captured them.

Indeed, if a civilian individual acts as a combatant and causes the death of the enemy, this same civilian cannot and should not be tried for the violence caused as such is what is expected of soldiers in combat. While they may be detained, the same rules of conduct in the treatment of prisoners of war must apply to them, and in the event that the conflict and hostilities end, their release should be an expected eventuality.

The manner by which terrorists conduct acts of violence and aggression in recent years has brought about the question as to whether individuals and non-state actors have become active participants in the conduct of war.[45] The manner by which states themselves react to acts of terror by non-state actors, perhaps best exemplified by the 10-year manhunt by the U.S. for Osama Bin Laden, raises the issue as to whether the traditional concept of war has evolved from state versus aggression to also cover state versus non-state conflicts.[46]

Even as to the question of whether a state may be held responsible for the actions of non-state actors, the international legal trend has shown a paradigm shift that tends to respond to this question in the affirmative. As earlier mentioned, the case of *Nicaragua* attempted to hold the U.S. responsible for actions of organizing, training, arming, and financing the Contra in its rebellion against the established Nicaraguan government.[47] The I.C.J. ruled that the U.S., despite having supported the rebels, could not be responsible for the acts of the Contras for lack of any effective control over the military or paramilitary operations of the latter.[48] This was later referred to as the "effective control" test in assessing state responsibility.[49]

This doctrine has since modified the standard of effective control in determining and imputing state responsibility for acts committed by non-state actors. In *Prosecutor v. Tadic*,[50] the International Criminal Tribunal for the former Yugoslavia ruled that a state may be responsible for actions of militarized non-state groups in instances where the state itself had coordinated or assisted in the planning of the military activity.[51] This, as

---

They shall at all times be humanely treated and protected, particularly against acts of violence, from insults[,] and from public curiosity. Measures of reprisal against them are forbidden." *Id.*

45. *See generally* Fletcher, *supra* note 43, at 635-39.

46. *Id.*

47. *Nicaragua*, 1986 I.C.J. at 4.

48. *Id.* at 103-25.

49. *Id.* at 64-65.

50. Prosecutor v. Tadic, Case No. IT-94-1-I, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

51. *Id.* ¶¶ 92-115.

argued by David E. Graham, marks the shift from "effective control" to "overall control."[52]

As we earlier intimated, the infamous 11 September 2001 attack by the Al Qaeda on the World Trade Center and the subsequent Bin Laden manhunt spawned the argument that war has now evolved to include state versus non-state actions. It was that attack, as argued by author Vincent-Joël Proulx, that further shifted the standard from the original "effective control" and the subsequent "overall control" to one of "indirect responsibility."[53] He argued further that while there were no indicia of Taliban exercise of effective or overall control over the Al Qaeda, the fact that the Taliban served as sanctuary for the Al Qaeda made the actions of the latter imputable to the former.[54]

The trend is now clearer in imputing responsibility upon a state for the actions of non-state actors as a failure of the state itself in preventing its territory from being used as a base from which the non-state actors plan, organize, and launch their attacks on other states.[55] This is furthered by the adoption of the Draft Articles on the Responsibility of States for Internationally Wrongful Acts,[56] widely accepted and recognized by the U.N. General Assembly and its member-states.

This, we argue, is a major step in establishing state responsibility for actions of non-state actors and will be useful in the drafting of similar conventions on state responsibility in cases of cyber warfare.

But this obligation imposed on states is hardly novel. As early as 1949, the I.C.J. ruled in the *Corfu Channel Case*[57] that states have a duty not to knowingly allow its territory to be used for acts contrary to the rights of other states.[58] In sum, this presents an affirmative duty on states to prevent non-state aggressors from committing armed attacks on other states.

52. David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SEC. L. & POL'Y 87, 95 (2010).

53. Vincent-Joël Proulx, *Babysitting Terrorists: Should States be Strictly Liable for Failing to Prevent Transborder Attacks?*, 23 BERKELEY J. INT'L. L. 615, 619-20 (2005).

54. *Id.* at 634-48.

55. *See* TAL BECKER, TERRORISM AND THE STATE: RETHINKING THE RULES OF STATE RESPONSIBILITY 62-65 (2006 ed.).

56. International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Supp. No. 10 (A/56/10), Ch. IV.E.1 (Nov. 2001).

57. Corfu Channel (U.K. v. Albania), 1949 I.C.J. 4 (Apr. 9).

58. *Id.* at 22.

III. CYBER WARFARE

Most authors and experts recognize that an exact definition of cyber warfare is highly debatable and is difficult to espouse.[59] It has been debated that there is a significant need for the governments of the world to develop and agree on an acceptable definition of cyber warfare in order for stronger multilateral policies and agreements to address the threats involved.[60]

Authors Jason Andress and Steve Winterfeld argue that in order to understand cyber warfare, one must first comprehend what cyberspace is as a potential theater of war.[61] The U.N. defines cyberspace as

> [t]he *global system* of systems of *internetted* computers, communications infrastructures, online conferencing entities, databases[,] and information utilities generally known as the Net. This mostly means the Internet; but the term may also be used to refer to *the specific, bounded electronic information environment of a corporation or of a military, government*[,] *or other organization.*[62]

In a similar light, the U.N. had occasion to define a "cyber attack" as "an act, usually through the Internet, that attempts to undermine the confidentiality, integrity, or availability of computers or computer networks, or the information that resides within the systems themselves."[63]

However, experts have also differed on the potential effects of cyber attacks. As earlier discussed, no less than the U.S. Secretary of Defense cited that numerous acts of cyber attacks may cause damage, loss of life, and the crippling of military, communications, and utility systems.[64] Law professor Hollis writes that a major economic downfall may occur in the event that a virus is successful in attacking the information servers of banks, financial institutions, and stocks and equities exchanges.[65] Also, Vida Antolin-Jenkins

---

59. *See generally* Oona A. Hathaway, et al., *The Law of Cyber Attack*, 100 CAL. L. REV. 817 (2012).

60. *Id.* at 823-33.

61. JASON ANDRESS & STEVE WINTERFELD, CYBER WARFARE: TECHNIQUES, TACTICS AND TOOLS FOR SECURITY PRACTITIONERS 2-4 (2011 ed.).

62. U.N. Term, Cyberspace, *available at* http://unterm.un.org/DGAACS/unterm.nsf/WebView/99B98BDBCBAB096185256E620052EFD3?OpenDocument (last accessed Feb. 28, 2013) (emphasis supplied).

63. U.N. Term, Cyber Attack, *available at* http://unterm.un.org/DGAACS/unterm.nsf/WebView/E43E07261A12A99D852572F00051585?OpenDocument (last accessed Feb. 28, 2013).

64. Panetta, *supra* note 9.

65. Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1042 (2007).

argues that such a major catastrophe is a possibility if terrorists gain access to the computer systems that control nuclear reactors.[66]

The use of cyber warfare tactics, specifically Distributed Denial of Service (DDOS) actions, has proven to have useful consequences for aggressor forces.[67] In April 2007, hackers were successful in disrupting public access to emergency lines for the dispatch of ambulances and firetrucks.[68] In 2008, the internet functionality of Georgia was interrupted at the most inopportune time when Russian forces were invading South Ossetia.[69]

Regardless of how cyber attacks are specifically used in cyber war or actual war, it has become indisputable that cyber attacks are not only necessary steps for cyber war, but are integral elements thereof. We are reminded by Oona A. Hathaway, et al.[70] that a cyber war is the collective of cyber attacks and the conduct of the former necessarily includes instances of the latter, with the goal of impairing the integrity of essential computer systems and the information contained therein.[71]

We find that the definition presented by Charles G. Billo and Welton Chang[72] as most adequate for purposes of this Study. In describing cyber warfare, they stated that

> [c]*yber warfare involves units organized along nation-state boundaries, in offensive and defensive operations, using computers to attack other computers or networks through electronic means.* Hackers and other individuals trained in software programming and exploiting the intricacies of computer networks *are the primary executors of these attacks.* These individuals *often operate under the auspices and possibly the support of nation-state actors.* In the future, if not already common practice, individual cyber warfare units will execute attacks against targets in a cooperative and simultaneous manner.[73]

66. Vida Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 NAVAL L. REV. 132, 138-40 (2008).

67. *Cyberwarfare: Newly Nasty*, ECONOMIST, May 24, 2007, *available at* http://www.economist.com/node/9228757 (last accessed Feb. 28, 2013).

68. *Id.*

69. *The Threat from the Internet: Cyberwar*, ECONOMIST, July 1, 2010, *available at* http://www.economist.com/node/16481504 (last accessed Feb. 28, 2013).

70. Hathaway, *supra* note 59.

71. *Id.* at 839-56.

72. Charles G. Billo & Welton Chang, Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States (A Study in Response to a Grant by the Department of Homeland Security) 3, *available at* http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf (last accessed Feb. 28, 2013).

73. *Id.* (emphasis supplied).

A. Individuals and Non-State Actors in Cyber Warfare

Andress and Winterfeld summarize the various personalities of non-state actors in cyber warfare as follows:

(1) *Script Kiddies* are often the least skilled, but most common, of non-state attackers. They usually use scripts and tools written by others in order to perpetrate their cyber attacks. Their threat level is considered as low, as their skill and success in attacking networks and computer systems are highly dependent on the quality of the tools used and the quality of the network security of their targets.[74]

(2) *Malware authors* are considered a very specialized type of cyber attacker, as a greater amount of programming skill is required for one to write the code. Lower level malware authors are likened to script kiddies in cases where the former utilize already existing codes and programs in developing their own malware.[75]

(3) *Scammers* are those who utilize the same tools as script kiddies for the purpose of fraudulently gaining access to a person's personal information, such as usernames and passwords, social security numbers, and bank and financial data. They are thought of as having little or no technical skill at all, and only utilize the Internet and network communications to fool their targets into revealing their personal information.[76]

(4) *Blackhats* are among the most highly skilled of individuals, thought of as having "no care for the rule of law, the systems they disrupt[,] or the ill effects that they cause."[77] Blackhats have varying motivations for their cyber attacks, but usually act just for the sheer thrill of it. They are contrasted from *Whitehats*, similarly skilled hackers who work for more benevolent purposes, that is, to secure critical systems and prevent the success of Blackhat attacks.[78]

(5) *Hacktivists* or hacker-activists have skills similar to Blackhats, but use their attacks in pursuit of their activist agenda. They are characterized as using non-violent means in promoting their causes, as what was experienced by a number of governmental

74. ANDRESS & WINTERFELD, *supra* note 61, at 195.

75. *Id.*

76. *Id.* at 196.

77. *Id.*

78. *Id.*

websites that were defaced in protest of the passage of the Philippine Cyber Crime Prevention Act.[79]

(6) *Patriot Hackers* are essentially Blackhats and Hacktivists working on a more political, and arguably patriotic, level. They are considered to have similar skill sets as Blackhats, and employ means similar to Hacktivists to promote political means. While unproven, patriot hackers are often thought of as actually working for their governments. Patriot Hacker actions were seen in the defacing of government websites of both the Philippines and China on the issues of the West Philippine Sea territorial dispute.[80]

Corporations, especially large ones, are also potential non-state actors in cyber warfare.[81] Andress and Winterfeld note that large corporations possess great power and resources that rival small states; and those corporations in the industry of technology have highly skilled employees and the latest technologies which may be used to carry out cyber attacks.[82]

It is even alleged that some corporations, specifically those with defense contracts such as Northrup Grumman, General Dynamics, Lockheed Martin, and Raytheon, perform cyber warfare activities that the government actively supports through the funding provided.[83] It was stated that U.S. Federal spending on computer security and classified programs totalled $10 billion annually, an amount expected to increase.[84]

79. *Id.* at 197. *See also* Camille Diola, *'Anonymous Philippines' hacks gov't websites anew*, PHIL. STAR, Jan. 15, 2013, *available at* http://www.philstar.com/cybercrime-law/2013/1/15/897221/anonymous-philippines-hacks-gov-t-websites-anew (last accessed Feb. 28, 2013).

80. ANDRESS & WINTERFELD, *supra* note 61, at 197. *See also* Ira Pedrasa, Palace websites attacked by 'Chinese networks,' *available at* http://www.abs-cbnnews.com/nation/04/23/12/palace-websites-attacked-'chinese-networks (last accessed Feb. 22, 2013) & INQUIRER.net, Filipino hackers fight back, deface Chinese sites, PHIL. DAILY INQ., Apr. 21, 2012, *available at* http://technology.inquirer.net/10235/filipino-hackers-fight-back-deface-chinese-sites (last accessed Feb. 28, 2013).

81. ANDRESS & WINTERFELD, *supra* note 61, at 197.

82. *Id.*

83. *Id.* at 198.

84. *See* Christopher Drew & John Markoff, *Contractors Vie for Plum Work, Hacking for U.S.*, N.Y. TIMES, May 30, 2009, *available at* http://www.nytimes.com/2009/05/31/us/31cyber.html?_r=0 (last accessed Feb. 28, 2013).

IV. CYBER WARFARE AND JUST WAR THEORY

Thus far, we have established the following peculiarities of cyber warfare as opposed to traditional war. First, the ethics of the conduct of war found in the U.N. Charter,[85] the Hague Conventions,[86] the Geneva Conventions,[87] and customary international law[88] have little application to cyber warfare.

Second, the role of individuals and non-state actors has evolved from unwilling victims to active participants.

Third, state responsibility for the acts of these non-state actors is becoming a legal trend in light of the advent of terrorist groups.

Fourth, the effects of an actual war may be achieved through the use of cyber warfare tactics, from such things as disruption of public utilities and transportation terminals to the loss of life. The difference here lies in the fact that as opposed to traditional war, these effects can be realized through data manipulation from a computer on the other side of the world.

Finally, the concept of "use of force" is highly antiquated in the context of cyber warfare. While an airport terminal or electric facility can be shut down through a cyber attack, the general effect is the same as if enemy forces had captured the airport or electric facility. Consider this as opposed to the situation where a cyber attack results in the derailing of a passenger train resulting in massive loss of life. In the former, no actual force was used, while in the latter, the cyber attack is practically equivalent to the use of force.

It is at this point that we briefly discuss the concepts of Just War or *Bellum Iustum* which we argue further proves that conventional international war concepts are antediluvian in light of cyber warfare.

---

85. U.N. Charter art. 2, ¶ 4. This Provision states that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." *Id.*

86. Convention (IV) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, *opened for signature* Oct. 18, 1907, 205 C.T.S. 277.

87. Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, *supra* note 22 & Convention relative to the Treatment of Prisoners of War, *supra* note 24.

88. *See generally* Peaceful Settlement of Disputes between States, G.A. Res. 37/10, U.N. Doc. A/RES/37/10 (Nov. 15, 1982); *See also* Declaration of Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, G.A. Res. 25/2625, U.N. Doc. A/RES/25/2625 (Oct. 24, 1970).

The Just War theory has consistently provided for an ethical framework in the conduct of traditional warfare.[89] This is composed of three phases of warfare, namely *jus ad bellum* or the right to wage war, *jus in bello* or the conduct during war, and *jus post bellum* or conduct after war.[90]

As regards *jus ad bellum*, five principles are contained: right authority, right intention, probability of success, last resort, and proportionality.[91]

Right authority is conventionally referred to as the proper, legitimate authority to wage war, hence, the government of a state.[92] This already presents issues of an aged doctrine as we know that cyber war can be waged by non-state actors such as hackers, or Blackhats.

Right intention is likewise lacking in its applicability to cyber warfare, as these non-state actors are not bound by the requirements of a just cause to wage war contained in international law conventions.[93]

Probability of success is thought of as a means to ensure that war resources are not utilized in futile efforts. However, cyber war can be conducted with minimal use of resources (such as a set of computers and individuals with hacking skills) and without actual deployment of troops to the battlefield.[94]

Last resort stipulates the use of force as an option only when other diplomatic modes have resulted in failure.[95] But cyber attacks are not usually a final resort, but often are a primary resort. Cyber attacks crippling the infrastructure of a state prove highly useful for invading forces, as in the example discussed in the case of Russia's invasion of South Ossetia.[96]

Finally, proportionality is difficult to calculate in cyber warfare. While it traditionally focuses on the cost-benefit analysis of waging war (the benefits must outweigh the harm caused), the unpredictable nature of cyber warfare makes its effects difficult to judge for purposes of proportionality. Again, for an aggressor cyber attacker, the disruption of, say, the stock exchange may cost unimaginable economic and financial distress at little or no cost to the attacker.

---

89. *See* Stanford Encyclopedia of Philosophy, War, *available at* http://plato.stanford.edu/entries/war/#2 (last accessed Feb. 28, 2013).

90. *Id.*

91. *Id.*

92. *Id.*

93. *Id.*

94. *Id.*

95. *See* Stanford Encyclopedia of Philosophy, *supra* note 89.

96. *The Threat from the Internet: Cyberwar*, *supra* note 69.

With regard to proper conduct of war, *jus in bello* contains two principles, namely distinction and proportionality.[97] The latter we have just previously discussed and will no longer be the focus of further discourse. Distinction as a war concept specifies that attacks should not be directed against non-combatants such as the civilian populace.[98] This delineation is highly improbable and practically impossible to map in a cyber war due to the highly integrated nature of the Internet. It is not as easy to conduct a cyber attack at a military installation without causing harm to non-combatants. While a geographic map may prove useful to distinguish military targets from civilian zones, the manner by which the topography of the Internet is made makes little or no distinction whatsoever.

Finally, *jus post bellum* defines justice after a war, focusing on the conduct and provision of responsibility and reparations.[99] Its three principles are: seeking a lasting peace, holding morally culpable individuals accountable, and extracting reparations.[100] Arguably, all three principles find difficult application in cyber warfare for the primary reason that cyber warfare can be conducted successfully not by states or *de facto states*, but non-state actors.

Hence, if the identity of these non-state aggressors is not ascertained, the negotiations towards long-term peace can never begin. All the more futile is the prosecution of morally culpable cyber attackers and the extraction of reparations from them without any damning evidence of their involvement in the conduct of war.

V. CONCLUSION

From all the foregoing, it is clear that technology has created more than globalization. It has given rise to an evolution of war, one that disregards political and physical boundaries, transcends state actions, and empowers non-state actors to the forefront of war as aggressors.

Concerns lie in the presence of non-state actors not only in physical attacks of terrorism, but in cyber terrorism and cyber warfare as well. The various conventions comprising international law on war are glaringly outdated, with the Geneva Convention's most recent treaty dating back to over 70 years ago.[101] The various protocols and agreements find little

97. *See* Stanford Encyclopedia of Philosophy, *supra* note 89.

98. *Id.*

99. *Id.*

100. *Id.*

101. Protocol Additional to the Geneva Convention of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), *adopted* June 8, 1977, 1125 U.N.T.S. 3.

application in a cyber war, where the theater of war is the newest frontier for global dominance.

Various laws have been enacted by states in reaction to the effects of a cyber war, with the U.S. pioneering the legal battle with numerous domestic laws relating to cyberspace such as the Computer Fraud and Abuse Act,[102] Federal Information Security Management Act,[103] Electronic Communications Privacy Act,[104] and the all-inclusive Patriot Act.[105]

However, municipal law is simply not enough to address security issues arising from cyber warfare. The application of these domestic laws is territorial in nature, and most cyber attackers would likely feel safe conducting their activities from a safe distance, perhaps in their home states.

There is also a great need for the international community to agree on the threats of cyber warfare. Resort to the traditional conventions will be less and less helpful through time.

102. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986).

103. Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541 (2002).

104. Electronic Communications Privacy Act (EPCA), 18 U.S.C. §§ 2510-22 (1986).

105. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (U.S.A. Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).