Goettingen Journal of International Law 1 (2009) 3, 375-396

The Use of Cyber Force: Need for Legal Justification?

Marco Benatar*

Table of Contents

Abstract 376
A. Introduction: "Here Come the Cyber Wars" 376
B. The Concept of Cyber Force 378
C. The Legality of Cyber Force 380
I. Article 2(4) UN Charter – Narrow Interpretation 380
1. Textual Exegesis 381
2. Travaux Préparatoires 383
3. Subsequent Practice 384
4. Conclusion 386
II. Article 2(4) UN Charter – Broad Interpretation 387
1. Instrumentality Approach 387
2. Consequentiality Approach 389
III. Article 51 UN Charter 392
D. Future Prospects 394

* Cand. Jur., Lic. Jur. (Vrije Universiteit Brussel); LL.M. (New York University).

doi: 10.3249/1868-1581-1-3-benatar

Abstract

This short essay presents a legal analysis of *cyber force*, an intangible form of international coercion that exploits computer networks leaving havoc in its wake. After providing recent examples of this phenomenon, as well as circumscribing its scope, the essay sets out to determine to what extent cyber force can be reconciled with contemporary *jus ad bellum*. Two key questions will be addressed: is cyber force a use of force as defined in article 2(4) of the UN Charter, and if so, could it conceivably rise to level of an armed attack justifying self-defence as meant by article 51 of the same document? In order to respond to these queries, the analysis hinges upon the interpretative techniques of the Vienna Convention of the Law of Treaties as well as the current doctrinal debates regarding cyber force. The essay ends with a brief consideration of plausible prospects with respect to the regulation of this novel form of coercion.

A. Introduction: "Here Come the Cyber Wars"[1]

Among tech savvy pundits, Estonia is renowned for two things, one commendable, the other unenviable. The tiny Baltic country has the reputation of being the most "wired" country of Europe where regular online elections and free Wi-Fi abound.[2] Unfortunately, Estonia is also the first country ever to have experienced a large-scale co-ordinated attack against state-run computer systems.[3] The reason for this digital onslaught: a controversial decision to remove a Soviet war monument, the Bronze Soldier of Tallin, from the city centre, much to the ire of the local Russian population. What followed was a cyber siege lasting three weeks, with attacks launched against a plethora of public websites.[4] Quite surprisingly,

1 M. Weiss, Here Come the Cyber Wars: Are We Ready?, *Reason.Com* (17 August 2007) available at http://www.reason.com/news/show/121896.html (last visited 15 June 2009).

2 J. Davis, Hackers Take Down the Most Wired Country in Europe, *Wired Magazine* (21 August 2007) available at http://www.wired.com/politics/security/magazine/15-09/ff_estonia (last visited 15 June 2009).

3 A. Kobilnyk, 2008 – Year of the First Cyber-War?, *First Science.Com* (13 January 2008) available at http://www.firstscience.com/home/perspectives/editorials/2008-year-of-the-first-cyber-war_41826.html (last visited 15 June 2009).

4 P. Finn, Cyber Attacks Stalk Estonia, *Washington Post*, 19 May 2007; D. B. Hollis, 'Why States Need an International Law for Information Operations', 11 *Lewis &*

the destructive effect of this computerized aggression was not the result of highly sophisticated hacking tools. Rather, it was brought about by relatively primitive Distributed Denial of Service attacks (DDos) in which a website is flooded by constant requests, overwhelming the server thereby causing it to malfunction.[5] No state has claimed responsibility and despite Estonia pointing its finger to the Russian government, no involvement of the latter has been conclusively proven. In the aftermath of the attacks, NATO established the Cooperative Cyber Defence Centre of Excellence in Tallin.[6]

If more recent instances of digital aggression are anything of an indication, the future looks grim for peace in cyberspace. In August 2008, the world witnessed the first (known) case of cyber attack coinciding with actual armed conflict during the Russian-Georgian War.[7] More recently, in July of this year, unidentified hackers hit multiple targets in South Korea and the United States.[8] Governments are bracing themselves for the worst. McAfee, a major computer security company, observes: "[…] with an estimated 120 countries working on their cyberattack commands, in 10-20 years experts believe we could see countries jostling for cyber supremacy".[9]

Besides demonstrating that reliance on high-tech is a double-edged sword, cyber attacks raise a hugely important legal question: are they illegal uses of force? The UN Charter and customary international law proclaim the prohibition of the use of force between states. But what is precisely meant by "force" and can we interpret the use of force in a way that includes cyber attacks within its gamut? If we can construe cyber force as a *species* of illegal coercion, this might help bolster the legal abnegation of interstate violence. If, however, we fail in our enterprise, there will remain scant legal impediments to launching the computer wars of tomorrow.

Clark Law Review (2007) 4, 1024-1025; S. L. Myers, 'E-stonia' Accuses Russia of Computer Attacks, *New York Times*, 18 May 2007; The Cyber Raiders Hitting Estonia, *BBC News* (17 May 2007) available at http://news.bbc.co.uk/2/hi/europe/6665195.stm (last visited 20 July 2009).

5 Kobilnyk, *supra* note 3.

6 The website of the Centre: http://www.ccdcoe.org/ (last visited 20 July 2009).

7 J. Markoff, Before the Gunfire, Cyberattacks, *New York Times*, 12 August 2008.

8 Targets included the White House, Pentagon, State Department (US), Presidential Office and Defense Ministry (South Korea). Governments Hit by Cyber Attack, *BBC News* (8 July 2009) available at http://news.bbc.co.uk/2/hi/technology/8139821.stm (last visited 20 July 2009); New 'Cyber Attacks' Hit S Korea, *BBC News* (9 July 2009) available at http://news.bbc.co.uk/2/hi/asia-pacific/8142282.stm (last visited 20 July 2009).

9 McAfee, Cybercrime: The Next Wave, Virtual Criminology Report (2007), 12, available at http://www.mcafee.com/us/research/criminology_report/default.html (last visited 15 June 2009).

This paper aims to tackle this conundrum. Firstly, a rudimentary definition and typology of cyber force will be provided, as well as a comparison of this novel concept with the germane notions of cyber crime and cyber espionage. Thereafter, the core topic, the legality of cyber force, will be addressed. An attempt will be made to reconcile article 2(4) of the UN Charter with cyber force using the interpretative techniques of the 1969 Vienna Convention on the Law of Treaties (VCLT). This will be followed by a short discussion of article 51 of the UN Charter. Here, the central question is whether cyber force could conceivably rise to the level of an "armed attack". Finally, the paper looks at future prospects of incorporating computer attack in international law.

B. The Concept of Cyber Force

For the purpose of this paper, *cyber force*[10] is defined as coercive measures[11] that are (1) taken by a state or an entity whose actions are attributable to the state and (2) travel through cyberspace[12] exploiting the interconnectedness of computer networks to cause harmful effects in another state.

Varying greatly in intensity, ranging from web vandalism to attacking critical infrastructures, cyber force ultimately takes on one of three forms. The first type, *syntactic attack*, targets the *operating system* of a computer by means of malicious code or hacking.[13] Examples include worms which

[10] Legal literature on this topic gives many names to these (or similar) types of coercive acts. Examples include "cyber force", "cyber attack" and "information warfare". For the purpose of this paper, such terms are used interchangeably.

[11] Coercion involves "the government of one state compelling the government of another state to think or act in a certain way by applying various kinds of pressure, threats, intimidation or the use of force." See C. C. Joyner, 'Coercion', marginal number 1, in R. Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (2009), available at http://www.mpepil.com (last visited 15 June 2009).

[12] Originally employed by sci-fi author William Gibson to describe an alternate computerized world of reality, the notion of cyberspace now has evolved into a technical term. Although no commonly accepted definition exists, cyberspace is conceived as a space where computer networks, information systems and the Internet interact. See W. Gibson, *Neuromancer* (Ace Books, 1984), 51.

[13] Malicious code is computer language that can destroy or obstruct files and programs on the targeted computer. V. M. Antolin-Jenkins, 'Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?', 51 *Naval Law Review* (2005), 139.

consistently copy themselves resulting in major slowdown,[14] trap doors that grant attackers unauthorized access to enter a computer system,[15] and logic bombs that lie dormant in computers for long periods of time until a trigger activates them upon which they unleash havoc.[16] Hacking involves breaking into a computer in order to spy or exploit an operating system. Access can be gained by relying on human weakness (social engineering), using sniffer programs to intercept passwords, user names etc. (eavesdropping) or using a dictionary program to try all possible code combinations (brute-force intrusion).[17]

Semantic attacks, the second kind of cyber force, are not aimed at operating systems but rather the *accuracy of information* retained by computers. The goal is to corrupt data so as to mislead users into thinking that information is true. This is particularly dangerous when a governmental website is targeted, for the public at large will be inclined to trust the data and act accordingly.[18]

Thirdly, *mixed attacks* involve a *combination* of syntactic and semantic attacks. Understandably, this category of cyber warfare has the ability to bring about extreme levels of devastation if well-orchestrated.[19]

In order to delineate the concept of cyber force, the latter has to be distinguished from similar acts. The first such distinction is between cyber force and *cyber crime*. The difference is twofold. In terms of the perpetrator, acts of cyber force are committed by a state or state-related entity, whereas private entities commit cyber crime.[20] As for the applicable law, interstate computer attacks are regulated by international law, in contrast to cyber

14 J. Barkham, 'Information Warfare and International Law on the Use of Force', 34 *New York University Journal of International Law and Politics* (2001) 1, 63.

15 C. C. Joyner & C. Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework', 12 *European Journal of International Law* (2002) 5, 836.

16 Barkham, *supra* note 14, 63.

17 S. J. Cox, 'Confronting Threats Through Unconventional Means: Offensive Information Warfare as a Covert Alternative to Preemptive War', 42 *Houston Law Review* (2005) 3, 887-888.

18 Antolin-Jenkins, *supra* note 13, 140.

19 *Id.*, 141.

20 D. M. Creekman, 'A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China', 17 *American University International Law Review* (2002) 3, 653.

crime, which is a matter of domestic criminal law and law enforcement.[21] With respect to the second point of difference some subtle distinction is in order. Cyber crime is not purely a matter of domestic legislation that eludes international law. The European Cybercrime Convention is an excellent example of efforts undertaken at the intergovernmental level to form a common policy on cyber crime.[22]

Cyber force also differs from *cyber espionage*. They share the commonality of using the same techniques to penetrate the computer networks of a targeted state yet they diverge in terms of finality. The goal of espionage is to obtain sensitive information for a variety of purposes, in contrast to a cyber attack which aims to generate deleterious effects akin to an act of force. From a legal perspective, espionage is generally punishable under domestic law and amounts to a legitimate, if unfriendly, act under international law, whereas cyber attacks violate the rules of international law related to the recourse to force.[23]

C. The Legality of Cyber Force

I. Article 2(4) UN Charter – Narrow Interpretation

This section will examine the notion of force as defined in article 2(4) of the UN Charter, the cardinal provision of the *jus ad bellum*.[24]

21 J. J. Rho, 'Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable Under the Alien Tort Statute', 7 *Chicago Journal of International Law* (2007) 2, 701-702.

22 *Council of Europe Convention on Cybercrime*, 23 November 2001, Treaty Doc. 108-11, ETC No. 185.

23 Y. Dinstein, 'Computer Network Attacks and Self-Defense', in M. N. Schmitt & B. T. O'Donell (eds), *Computer Network Attack and International Law* (2002), 105; S. P. Kanuck, 'Information Warfare: New Challenges for Public International Law', 37 *Harvard International Law Journal* (1996) 1, 276; W. G. Sharp, *Cyberspace and the Use of Force* (2000), 123-132.

24 The UN Charter includes various rules dealing with the use of force as well as international peace and security in the broader sense. Within this legal framework, article 2(4) plays a pivotal role by virtue of the fundamental rule it enshrines. Therefore, it is fair to refer to this rule as "the mother of all provisions relating to the use of force in the Charter". See N. Schrijver, 'Article 2, paragraphe 4', in J-P Cot, A. Pellet & M. Forteau (eds), *La Charte des Nations Unies: Commentaire Article par Article* (2005), 446. Furthermore, this paper will be solely dedicated to the use of force to the exclusion of the law of armed conflict (*jus in bello*). For an excellent short overview of the relationship between cyber attacks and humanitarian law, see:

> "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

The interpretative techniques enshrined in the 1969 Vienna Convention on the Law of Treaties (VCLT) will serve as a "toolbox".[25] Although article 4 of the VCLT stipulates that it only applies to treaties concluded after its entry into force, its rules of interpretation have acquired customary force and are held to be applicable to the UN Charter.[26] The goal here is to determine whether we can conceive of a new notion of force, cyber force, which fits within article 2(4) without stretching the provision to its breaking point.

1. Textual Exegesis

When attempting to unearth the ordinary meaning of a term, one feels naturally drawn to the dictionary.[27] A brief overview of some major dictionaries of the English language is sufficient to discover that force has several connotations. In the narrow sense it designates physical force. In the broader sense it comprises a host of measures. Thus, it is possible from a purely linguistic perspective to argue for either an expansive or limited reading of the concept of force.[28]

M. N. Schmitt, H. A. Harrison Dinniss & T. C. Wingfield, Computers and War: The Legal Battlespace, Harvard Program on Humanitarian Policy and Conflict Research, International Humanitarian Law Research Initiative Briefing Paper (June 2004) available at http://www.ihlresearch.org/ihl/pdfs/schmittetal.pdf (last visited 15 June 2009).

25 *Vienna Convention on the Law of Treaties*, 23 May 1969, 1155 U.N.T.S. 18232 [VCLT]; The VCLT covers the most important areas of the law of treaties, including the rules on interpretation, which can be found in articles 31-33. The following interpretative elements will be used: text, context, *travaux préparatoires*, and subsequent practice.

26 G. Ress, 'Interpretation', in B. Simma (ed.), *The United Nations Charter: A Commentary*, 2nd ed. (2002), 18.

27 This is a valid tool of interpretation in international law and is often used by the ICJ. See A. Aust, *Modern Treaty Law and Practice*, 2nd ed. (2007), 183.

28 H. Brosche, 'The Arab Oil Embargo and United States Pressure Against Chile: Economic and Political Coercion and the Charter of the United Nations', 7 *Case Western Reserve Journal of International Law* (1974) 1, 19; This is hardly an

Examining the context in which article 2(4) operates yields more interesting results. Firstly, article 2(4) merely mentions "force" without any qualifying adjectives. The framers undoubtedly were aware of the diverse forms of coercion available to states, so it is possible that a deliberate choice was made to develop a rule that could flexibly adapt to new and unforeseeable forms of violence and keep its relevance as a norm of conduct for international relations.[29]

Secondly, other articles of the UN Charter do explicitly refer to "armed force".[30] From this we could reason *a contrario* that whenever the drafters meant to say armed force, then they would not be hesitant to write that *ad verbatim* in the UN Charter.[31]

Thirdly, the use or threat of force is only illicit when it targets the "territorial integrity or political independence of any state", or is conducted in "any other manner inconsistent with the Purposes of the United Nations".[32] Evidently, military coercion can generate these deleterious effects. That does not however prevent other forcible measures from achieving the very same consequences.[33]

idiosyncrasy of English; the French (*la force*) and Spanish (*la fuerza*) counterparts yield the same imprecise results.

29 Comment, 'The Use of Nonviolent Coercion: A Study in Legality under Article 2(4) of the Charter of the United Nations', 122 *University of Pennsylvania Law Review* (1974) 4, 999.

30 Art. 41 Charter of the United Nations: "The Security Council may decide what measures not involving the use of *armed force* are to be employed to give effect to its decisions […]" (emphasis added); Art. 46 Charter of the United Nations: "Plans for the application of *armed force* shall be made by the Security Council with the assistance of the Military Staff Committee" (emphasis added); Art. 47.3 Charter of the United Nations: "The Military Staff Committee shall be responsible under the Security Council for the strategic direction of any *armed forces* placed at the disposal of the Security Council […]" (emphasis added). Brosche, *supra* note 28, 20.

31 Comment, *supra* note 30, 997.

32 The aforementioned purposes of the UN can be found in Art. 1(1) Charter of the United Nations: "To maintain international peace and security, and to that end: […] and to bring about by peaceful means, […], adjustment or settlement of international disputes or situations which might lead to a breach of the peace" and Art. 2(3) Charter of the United Nations: "All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered".

33 By way of illustration, the imposition of a comprehensive trade embargo (economic coercion), spreading subversive propaganda (ideological coercion) or isolating a government in the international arena (diplomatic coercion) can be as invidious (if not more) to the political independence of a state as the onslaught of a bombing campaign.

Advocates of the restricted reading of article 2(4) refute these assertions. Firstly, the seventh perambulatory clause of the UN Charter states that "*armed* force shall not be used save in the common interest" (emphasis added). The UN Charter is structured in such a manner that the preambulatory clauses are broader in scope than the provisions that follow and implement them. Hence, it would run counter to the design and consistency of the treaty for article 2(4) to prohibit force in the broad sense, whilst the goal of the UN is to abnegate force in the narrow sense.[34] Moreover, article 41 contains a list of measures "not involving the use of armed force" that the Security Council can adopt under Chapter VII including the "complete or partial interruption of […] means of communication". In this day and age it is not hard to accept that the internet fits this description to a tee.[35]

We can conclude from this analysis that the wording of article 2(4) is ambiguous to say the least. The very same text is conducive to radically opposed understandings of the concept of force.[36]

2. Travaux Préparatoires

The proposals and ensuing discussions of the UN Conference on International Organization (UNCIO) of 1945 form the essential starting point for any historical inquiry into the *raison d'être* of the UN Charter. This is certainly the case with respect to article 2(4), due to the electrifying debates and divergence of views it gave rise to.[37]

During the drafting of what would become article 2(4), a host of unsuccessful proposals were submitted in favor of expanding the prohibition to virtually all conceivable uses of force. Ecuador suggested outlawing

See M. S. McDougal & F. P. Feliciano, *The International Law of War: Transnational Coercion and World Public Order* (1994), 28-30.

34 M. N. Schmitt, 'Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework', 37 *Columbia Journal of Transnational Law* (1999) 3, 904.

35 Hollis, *supra* note 4, 1041.

36 It is disappointing that the language of a fundamental rule such as this one is plagued by a high degree of indeterminacy. However, see *contra* O. Schachter, 'The Right of States to Use Armed Force', 82 *Michigan Law Review* (1984) 5/6, 1625: "These interpretive questions concerning the meaning of "force" and "threat of force" are of importance in some situations and they indicate that the precise scope of the article requires further definition. However, they are essentially peripheral questions. They do not raise questions as to the core meaning of the prohibition and do not, therefore, require one to conclude that article 2(4) lacks determinate content".

37 Schrijver, *supra* note 24, 443.

moral and physical force,[38] whilst Iran endorsed banning direct and indirect political force.[39] The most famous attempt was made by the Brazilian delegation, who suggested the following amendment: "All members of the Organization shall refrain in their international relations from the threat or use of force and from the threat or use of economic measures in any manner inconsistent with the purposes of the Organization".[40] The proposal was ultimately torpedoed by a vote of 26 to 2.[41] The overwhelming refusal to expand article 2(4) can thus be seen as a confirmation of the restrictive view on force as denoting only armed force.

3. Subsequent Practice

A good indicator of subsequent practice can be found in the various resolutions adopted within the institutional framework of the UN that deal with issues of peace and security. When such declarations garner widespread support they can become authoritative accounts of how the UN Charter should be interpreted.[42]

The Declaration on Friendly Relations,[43] adopted on the 25th anniversary of the organization as a landmark resolution,[44] prohibits the threat or use of force in international relations. During the committee sessions, opposing arguments were voiced as to the scope of "force". The majority of Western nations wanted to maintain the restricted notion of armed force. The African and Asian group preferred a purpose-based analysis irrespective of the form of pressure. The Central and South

38 6 U.N.C.I.O. Docs. 561 (1945); 3 U.N.C.I.O. Docs. 399, 423 (1945).

39 6 U.N.C.I.O. Docs. 563, 588 (1945).

40 6 U.N.C.I.O. Docs. 559 (1945).

41 6 U.N.C.I.O. Docs. 334-339, 405, 609 (1945). It is interesting to observe that although in 1945 it was in large part the Third World advocating and the West opposing the inclusion of economic force, the tables would turn radically a few decades later: at the height of the Arab Oil Crisis, Western scholars went to great lengths to qualify the economic boycott of the OPEC countries as an illegal use of force. See C. E. Cameron, 'Developing a Standard for Politically Related State Economic Action', 13 *Michigan Journal of International Law* (1991) 1, 218-219.

42 A. Boyle, 'Soft Law in International Law-Making', in M. D. Evans (ed.), *International Law*, 2nd ed. (2006), 146.

43 Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), 24 October 1970 [Friendly Relations Declaration].

44 G. Arangio-Ruiz, *War, The UN Declaration on Friendly Relations and the System of the Sources of International Law* (1979), 1.

American group was divided on the matter.[45] In the end, the final text makes no mention of other forms of interstate pressure and uses terms that can only relate to armed force.[46] In addition, the declaration links the principle on non-intervention in domestic affairs to economic and political coercion.[47] Therefore, the majority view connects article 2(4) with force and the principle of non-intervention with other forms of coercion.[48]

The Declaration on the Non-Use of Force[49] strengthens that conclusion.[50] In a similar fashion, the structure and language of this resolution implies a separation of coercive measures with armed force on the one hand and other types of pressure on the other hand.[51]

Beyond the confines of the United Nations, the term "force" is used in numerous treaties often without any further specification or qualifying adjectives.[52] Such is the case for various mutual defense pacts (e.g.

45 Schmitt, *supra* note 35, 906-907.

46 "war of aggression", "violate the existing international boundaries of another State", "violate international lines of demarcation", "irregular forces or armed bands", "acts of civil strife or terrorist acts", "military occupation". Schmitt, *supra* note 35, 907.

47 Friendly Relations Declaration, *supra* note 45: "No State may use or encourage the use of economic political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind".

48 A. Randelzhofer, 'Article 2(4)', in B. Simma (ed.), *The United Nations Charter: A Commentary*, 2nd ed. (2002), 118; *Contra* Arangio-Ruiz, *supra* note 46, 99-100. Although not defining the precise scope of the non-use of force rule, Arangio-Ruiz asserts that other forms of coercion are included in this prohibition. His main argument is derived from the fact that neither the Declaration nor the Charter have a differentiated sanction for economic and political coercion as opposed to armed force.

49 Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations, G.A. Res. 42/22, 18 November 1987 [Declaration on the Non-Use of Force].

50 The drafting history of the text also reflected deep divisions between nations akin to those witnessed during the negotiations of the Declaration on Friendly Relations; C. Gray, 'The Principle of Non-Use of Force', in V. Lowe & C. Warbrick (eds), *The United Nations and the Principles of International Law: Essays in Memory of Michael Akehurst* (1994), 34.

51 Para. 1 Subpara. 7 Declaration on the Non-Use of Force: "States have the duty to abstain from armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements"; Para. 1 subpara. 8 Declaration on the Non-Use of Force: "No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind".

52 Schmitt, *supra* note 35, 906.

NATO[53]), international organizations (e.g. African Union[54]) and other international instruments (e.g. Rome Statute[55]).

4. Conclusion

It is apparent from this analysis that the UN Charter adopts a clear-cut approach to force by distinguishing three types: armed, economic and political.[56] All can lead to a violation of international law, namely the principle of non-intervention,[57] but only force of an armed nature can violate the norm enshrined in article 2(4) and therefore constitute a use of force in the technical sense.[58] Later attempts in the General Assembly to replace this model with a broader one failed.

53 Art. 1 *North Atlantic Treaty*, 4 April 1949, 34 U.N.T.S. 243: "The Parties undertake, as set forth in the Charter of the United Nations, […] to refrain in their international relations from the threat or use of force in any manner inconsistent with the purposes of the United Nations".

54 Art. 4(f) *Constitutive Act of the African Union*, 11 July 2000, OAU Doc. CAB/LEG/23.15: "Prohibition of the use of force or threat to use force among Member States of the Union".

55 Preamble *Rome Statute of the International Criminal Court*, 17 July 1998, 2187 U.N.T.S. 90: "Reaffirming the Purposes and Principles of the Charter of the United Nations, and in particular that all States shall refrain 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".

56 Schmitt, *supra* note 35, 909.

57 This principle is enshrined in various sources: implicitly in Art. 2(1) of the UN Charter (sovereign equality), explicitly in the Friendly Relations Declaration and the Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, G.A. Res. A/RES/36/103, 9 December 1981, as well as the jurisprudence of the International Court of Justice (e.g. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, ICJ Reports 1986, para. 202: "The principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference; though examples of trespass against this principle are not infrequent, the Court considers that it is part and parcel of customary international law. […] international law requires political integrity […] to be respected."

58 Some are, however, critical of the view that instrumentality should be the definitive factor for determining whether an act fits in the use of force paradigm. See McDougal & Feliciano, *supra* note 34, 240-241.

II. Article 2(4) UN Charter – Broad Interpretation

Acknowledging the conclusion above, one can endeavor to demonstrate that cyber attacks are perhaps not a new kind of force but instead a new kind of *armed* force. However, in order to do so, recourse will be sought to a more expansive legal technique, namely analogy.[59] Showing that cyber attacks are sufficiently similar to typical examples of armed force would allow for a broadening of the scope of article 2(4) to include cyber force.

1. Instrumentality Approach

How we legally qualify an act is contingent upon the type of tool that is used (armed, economic or political) rather than the harmful consequences that it causes.[60] This approach Hollis calls "instrumentality".[61]

In essence, the notion of armed force is one of weaponry.[62] So which weapons are authorized? The *jus ad bellum* remain silent on this issue. Not that this is a surprising state of affairs, given that article 2(4) does not even mention the word "armed" in its treatment of the prohibition of armed force.[63] In a similar vein, the International Court of Justice (ICJ) observed the following in its advisory opinion on the legality of nuclear weapons: "These provisions [pertaining to the use of force in the UN Charter] do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon […]".

Fortunately, several scholars have filled the void by construing an interpretation of armed force. The traditionalist understanding of armed

59 S. Vöneky, 'Analogy in International Law', in R. Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (2009), available at http://www.mpepil.com (last visited 15 June 2009).

60 Kanuck, *supra* note 23, 289.

61 Hollis, *supra* note 4, 1041.

62 J. N. Bond, 'Peacetime Foreign Data Manipulation as One Aspect of Offensive Information Warfare: Questions of Legality under the United Nations Charter Article 2(4)', *Advanced Research Project, Naval War College* (1996), 78.

63 See *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, ICJ Reports 1996, 244.

force consists of two elements, namely that an act of coercion is military as well as physical.[64]

The first condition, the *military* nature of the forcible measure, heavily relies on the ongoing leaps and bounds that military technology makes. The level of sophistication that characterizes modern weaponry develops at a rapid rate seeing that superior technology is paramount for keeping the edge and exerting a deterrent effect on potential adversaries. If article 2(4) cannot keep pace with this evolution, then it would become a redundant artifact merely able to regulate the means of combat known to the drafters of the UN Charter.[65] Figuring out when new forms of warfare meet the military requirement is a hard exercise, bearing in mind that there are no legal guidelines to follow. One way of approaching this quandary would be to accept that a weapon is military in nature, only when it is part of the official arsenal of the army of a state.[66]

A study of the United States Armed Forces illustrates how computer attacks can become a significant means of warfare and thus meet the requirement of military force. Firstly, the ability to use computer technology in combat situations has been comprehensively conceptualized in military doctrine. The key document in this regard is the *Joint Doctrine on Information Operations*[67] which theorizes a relatively wide spectrum of

64 D. Bowett, *Self-Defence in International Law* (1958): "taking the words [of article 2(4)] in their plain, common-sense meaning, it is clear that, since the prohibition is of the use or threat of force, they will […] apply [….] only to physical, armed force"; Randelzhofer, *supra* note 50, 118: "[…] only military force is the concern of the prohibition of the use of force"; C.H.M. Waldock, 'The Regulation of the Use of Force by Individual States in International Law', in 81 *Hague Academy of International Law, Recueil des Cours* (1952), 492: "[…] the word "force" in Article 2 (4) undoubtedly covers only armed or physical force […]. There seems to be general agreement on this point".

65 D. B. Silver, 'Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter', in M. N. Schmitt & B. T. O'Donell (eds), *Computer Network Attack and International Law* (2002), 84.

66 This does not imply that a use of force has to be carried out by the armed forces (by way of illustration, the forcible act can also violate article 2(4) when perpetrated by paramilitaries, mercenaries, police forces etc.). See Joyner & Lotrionte, *supra* note 15, 854; H. B. Robertson, 'Self-Defense against Computer Network Attacks', in M. N. Schmitt & B. T. O'Donell (eds), *Computer Network Attack and International Law* (2002), 134-135.

67 Joint Chiefs of Staff, Joint Publications 3-13, Joint Doctrine for Information Operations (2006) available at http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf (last visited 15 June 2009).

techniques (so called IO "core capabilities").[68] Furthermore, major steps are underway to develop the army's computer network operations. In November 2006, an ambitious decision was made to establish an Air Force Cyber Command (AFCYBER).[69] Although the project was cancelled, in June 2009 Defense Secretary Gates ordered the creation of U.S. Cyber Command (USCYBERCOM), a new digital force set to reach full operational capacity by October 2010.[70]

Conversely, it is hard to see how the inherent intangibility of computer attacks can be reconciled with the second requirement, *physical/kinetic force*, which is traditionally understood as involving "any explosive effect with shock waves and heat".[71] Nevertheless, certain commentators poke holes in this theory, pointing to a host of non-physical actions that they consider violations of the prohibition on force. In their view, a weapon does not always need to be physical to come under the purview of article 2(4). However, the examples given are fallacious when put under legal scrutiny.

For instance, it has been argued that "locking-on" to a fighter jet is an illegal use of force justifying a military response[72] thus proving that non-physical coercion can fall within the *jus ad bellum*. This is a questionable statement for there is a far more compelling legal analysis: when an aircraft has been locked-on to, the pilot can preemptively exercise the right of self-defense in accordance with article 51 of the UN Charter.[73]

2. Consequentiality Approach

In his major work on the use of force, Brownlie established a new juridical basis for assimilating weapons to the use of force that would

68 There are 5 IO core capabilities: PSYOP (Psychological Operations), MILDEC (Military Deception), OPSEC (Operations Security), EW (Electronic Warfare) and CNO (Computer Network Operations).

69 8th Air Force to Become New Cyber Command, *U.S. Air Force* (3 November 2006) available at http://www.af.mil/news/story.asp?storyID=123030505 (last visited 20 July 2009).

70 The Secretary of Defense, Memorandum concerning the Establishment of a Subordinate Unified U.S. Cyber Command under U.S. Strategic Command for Military Cyberspace Operations (23 June 2009) available at http://online.wsj.com/public/resources/documents/OSD05914.pdf (last visited 20 July 2009).

71 I. Brownlie, International Law and the Use of Force by States (1963), 362.

72 M. S. Martins, 'Rules of Engagement for Land Forces: A Matter of Training, Not Lawyering', 143 *Military Law Review* (1994), 44.

73 R. W. Aldrich, 'How Do You Know You Are at War in the Information Age?', 22 *Houston Journal of International Law* (2000) 2, 240.

otherwise be left out.[74] He argues that modes of warfare bring about the "destruction of life and property".[75] Therefore, a consequence-based test should be applied: if an act causes considerable harm to human beings and their surroundings, the requirement of physical force is fulfilled.

A number of commentators have taken Brownlie's words to heart and sought its application to cyber warfare. This is not surprising, as the consequences doctrine is ideal for categorizing forcible measures like cyber attacks which do not fit the definition of "physical force" but do have the potential to cause considerable physical damage[76]. The consequentiality model has been most famously applied to cyber attacks by Schmitt. He starts by pointing out that there are "easy cases" that fit the instrumentality model: cyber attacks that cause direct physical destruction and harm to human life analogous to armed force and that should therefore be equated to the latter.[77] This is the case when hackers take control of air traffic control systems and cause airplanes to crash[78] or give instructions to a nuclear plant that lead to its meltdown.[79]

On the other hand, there are instances of computer warfare that cannot be easily integrated into the classic force paradigm. He responds to this problem by enumerating a set of criteria that distinguish armed force from economic and political coercion with respect to their consequences. If a cyber attack meets these criteria then it strongly resembles armed force and could come under the purview of article 2(4).[80] Those requirements are the following:

1) severity (physical injury or destruction)
2) immediacy (high degree of immediacy of consequences)

74 Brownlie, *supra* note 74, 362.
75 *Id.*, 362.
76 T. A. Morth, 'Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter', 30 *Case Western Reserve Journal of International Law* (1998) 2/3, 591.
77 Schmitt, *supra* note 35, 913-914.
78 Bowman highlights the vulnerability of the U.S. Federal Aviation Administration (FAA). If a terrorist group or unfriendly power managed to launch a concerted attack on the computer systems that the FAA relies on, it could have a devastating impact on air travel. See M.E. Bowman, 'Is International Law Ready for the Information Age?', 19 *Fordham International Law Journal* (1996) 5, 1939.
79 In some sense, computer warfare allows low-tech states to "go nuclear" by exploiting the nuclear capabilities of the targeted states. See Dinstein, *supra* note 23, 105.
80 Schmitt, *supra* note 35, 913-914.

3) directness (consequences closely linked to the act of force)
4) invasiveness (high level of intrusion on the rights of the targeted state)
5) measurability (consequences easily ascertainable)
6) presumptive legitimacy (presumption of impermissibility until proof of self-defense).[81]

Although Schmitt's model remains the most refined theory to date for addressing the legality of cyber attacks under the *jus ad bellum*, this is not to say that it has resolved the issue definitively.[82]

Firstly, the issue of vagueness is problematic. Take for instance the criterion of "directness". Schmitt gives the example of a university that has to put its military research project on hold due to constant cyber intrusions into the campus laboratories. Obviously this will affect performance on the battlefield,[83] but is the correlation between the harm and the attack sufficient to amount to cyber force?

Secondly, Schmitt's model, just like the instrumentality approach, suffers from "under-inclusiveness". Cyber force has novel features that make it an extremely dangerous weapon but also different from conventional weaponry. As a result, certain instances of cyber force will not fulfill Schmitt's criteria. By way of illustration, destroying information held by the banking systems of a given country can bring the entire financial sector to its knees. Moreover, the whole operation can be effectuated in a matter of minutes and without a single casualty. No type of armed, political or economic force can accomplish such a feat, so there simply is no analogy to be made. This begs the question: does the uniqueness of cyber attack preclude it from being regulated by article 2(4)?[84]

Thirdly, on a more theoretical level, one can contemplate the value of this style of analogous reasoning. On the one hand, there is a sense of legitimacy in "treating like cases alike". On the other hand, some scholars claim that analogies should be limited when dealing with customary and treaty rules (in our case article 2(4) and its crystallization into custom). With respect to treaty provisions, certain jurists state that the result of applying an

81 *Id.*, 914-915.
82 In all fairness, Schmitt concedes that his test is limited in scope, describing it as a mere prescriptive shorthand and acknowledging that further gray zones will arise. *Id.*, 915.
83 *Id.*, 917.
84 Hollis, *supra* note 4, 1042.

analogical technique must correspond with the reasonable intentions or consent of the parties to the treaty as derived through interpretation.[85] As demonstrated above, it was not possible to convincingly argue for a notion of cyber force using the classical interpretive methods of the VCLT. Thus, this might temper the validity of a contradictory result based on an analogical argument. Regarding customary rules, some scholars advocate the inapplicability of analogical techniques, given that custom must derive from the consensus of states. Of course, in order for this argument to ring true, one has to accept the premise of voluntarism in international law.[86]

III. Article 51 UN Charter

So far, the focus in this paper has been on fitting cyber attacks within the contours of article 2(4). The next legal issue to consider is the compatibility of cyber force with article 51 of the UN Charter, which regulates the right to invoke self-defense in the event of an armed attack:

"Nothing in the present Charter shall impair the inherent right of individual or collective self-defense 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. (…)."

Both concepts are intrinsically linked in that all armed attacks constitute uses of force but only certain forceful acts rise to the level of an armed attack. The importance of this connection is twofold.

Firstly, evaluating whether cyber force can fulfill the requirements of an armed attack is entirely contingent upon accepting cyber force as a use of force. Thus, if cyber force is not a use of force in the sense of article 2(4), neither will it be an armed attack as understood in article 51. It is worth noting that the analysis that leads us to conclude that article 2(4) exclusively encompasses armed force is strengthened here. Beyond the obvious linguistic argument that the UN Charter refers to an *armed* attack, article 51 is often linked to the notion of aggression[87] which was elucidated by the UN General Assembly in its *Definition of Aggression*.[88] Aggression is "the use

85 Vöneky, *supra* note 62, marginal note 19.

86 *Id.*, marginal note 20.

87 C. Gray, *International Law and the Use of Force* (2004), 109; interestingly, the French version of the UN Charter prohibits "*aggression armée*" and not "*attaque armée*".

88 Definition of Aggression, G.A. Res. 3314 (XXIX), 14 December 1974 [Definition of Aggression].

of *armed* force by a State against the sovereignty, territorial integrity or political independence of another state, or in any other manner inconsistent with the Charter of the United Nations".[89] The resolution subsequently gives a non-exhaustive inventory of actions that are considered aggression. It is apparent from this illustrative list that the aggressive acts are physical and armed in nature.[90]

Secondly, the partial overlap between the use of force and armed attack creates a legal vacuum: a state can be the victim of unwarranted armed coercion, yet unable to exercise a forceful response in self-defense. The ICJ illustrated this gap in the *Nicaragua* case in which it qualified the US supply of arms and logistics to the Contras as an illegal use of force, but refrained from equating it to an armed attack.[91] The judges reiterated this line of jurisprudence in the *Oil Platforms* case. They replied negatively to the US claim that the mining of an American vessel by Iran amounted to an armed attack, because in their view it failed to meet the *Nicaragua* standard according to which only the "most grave" forms of force will constitute an armed attack.[92]

Figuring out when a cyber force is sufficiently *severe* to rise to the level of an armed attack is crucial. One way of achieving this is through the threshold of "critical national infrastructure". The latter can be described as a collection of public and private institutions in a variety of sectors that are essential for a country's survival.[93] In its 2003 strategy paper, the US

89 Article 1 Definition of Aggression, *supra* note 91.

90 Examples include: invasion by armed forces of state, bombardment and blockade of ports or coasts. Article 3 Definition of Aggression, *supra note* 91. Schmitt, *supra* note 35, 925-926.

91 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, ICJ Reports 1986, paras. 191, 195.

92 *Case concerning Oil Platforms (Islamic Republic of Iran v. United States of America)*, Judgment, ICJ Reports 2003, paras. 51, 63, 64 and 72. However, see *contra* E. Wilmshurst, Principles of International Law on the Use of Force by States in Self-Defence (2005), *Chatham House*, ILP WP 05/01, 6, available at http://www.chathamhouse.org.uk/research/international_law/current_projects/#force (last visited 15 June 2009): "An armed attack means any use of armed force, and does not need to cross some threshold of intensity.".

93 The USA PATRIOT Act describes critical infrastructure as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters". USA PATRIOT Act of 2001 § 1016, 42 U.S.C. § 5195c (Supp. II 2002).

government recognizes the need to maintain and protect computer systems from imminent threats and describes key portions of cyberspace as critical national infrastructure.[94]

Currently the Department of Homeland Security has the task of protecting cyberspace and operates on the presumption that cyber attacks constitute criminal activity.[95] Some, however, suggest that in light of the great danger computer warfare poses to a state's safety, it would be preferable to approach cyber attacks from a national security perspective and allow for rigorous defense.[96] In that case, the *jus ad bellum* paradigm would come into play: if a cyber attack targets and causes damage to critical infrastructure (vital target) that would justify self-defense measures. If it affects a computer system that has not been given the "critical infrastructure" designation (non-vital target), but still resembles armed force to a sufficient degree, then it would still qualify as an illegal use of force.[97] Conversely, others disagree with this proactive approach. After all, there is no international consensus on what constitutes critical infrastructure so essential that any attack on it would justify a forcible response. States have full discretion to determine this in their national policy, therefore the threat of abuse is extremely high.[98]

D. Future Prospects

This paper has shown that the relationship between computer attacks and the *jus ad bellum* is an uneasy one and it would be hard to make any sweeping statement as to the legality or illegality of cyber force. Firstly, it was shown that strict adherence to the traditional methods of treaty interpretation (textual exegesis, *travaux préparatoires*, and subsequent practice) yield limited results: to claim that cyber force fits article 2(4) and

94 Executive Branch of the U.S. Government, The National Strategy to Secure Cyberspace (2003), available at http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

95 S. M. Condron, 'Getting It Right: Protecting American Critical Infrastructure in Cyberspace', 20 *Harvard Journal of Law & Technology* (2007) 2, 407.

96 *Id.*, 407-408; E. T. Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense', 38 *Stanford Journal of International Law* (2002), 240; J. P. Terry, 'Responding to Attacks on Critical Computer Infrastructure: What Targets? What Rules of Engagement?', 46 *Naval Law Review* (1999), 185-187.

97 Creekman, *supra* note 20, 654-656.

98 Antolin-Jenkins, *supra* note 13, 165-166.

51 is overreaching. Secondly, the treatment of doctrinal models based on more expansive interpretations proved to be extremely useful in this regard, however, their ability to include all instances of cyber force is doubtful. Thirdly, although it is theoretically conceivable that a serious computer attack could rise to the level of an armed attack, this possibility is entirely contingent upon equating cyber force with an illegal use of force to begin with. Thus, given the current legal framework it would be most prudent to adopt an *ad hoc* approach when assessing new cases of digital aggression.

The inability to definitively outlaw cyber force is not necessarily a reason for disillusionment. Maybe it is better as a matter of policy not to integrate cyber force in the *jus ad bellum*. Using computer warfare to achieve military aims has the advantage over conventional weapons of being highly efficient and less prone to cause any loss of life.[99] Why then would we want computer operations to be subject to the highly stringent conditions for using force? Besides the question of policy, one could argue that there is already sufficient law to regulate interstate cyber conflict. After all, as mentioned in the pages above, even if a cyber attack does not amount to a use of force, it is still an intervention, which constitutes a violation of international law. In addition, authors have demonstrated that the use of cyber force might transgress the International Telecommunications Convention (which prohibits harmful interference with communications of other states party to the treaty)[100], the laws of neutrality[101] and international humanitarian law[102].

For those who do want to see cyber force become an integral part of international law, two possibilities seem to be at hand. The first is to wait for international organizations, primarily the United Nations, to address the issue of cyber warfare. Resolutions and state practice could crystallize into custom and/or change the way we construe the UN Charter's rules on the use of force.[103] It is hard to tell whether relying on international

99 Joyner & Lotrionte, *supra* note 15, 856.

100 R. D. Scott, 'Legal Aspects of Information Warfare: Military Disruption of Telecommunications', 45 *Naval Law Review* (1998), 62.

101 Due to the nature of cyberspace, launching a cyber attack often entails packets of information having to pass through neutral states in order to reach the targeted nation. See G. K. Walker, 'Information Warfare and Neutrality', 33 *Vanderbilt Journal of Transnational Law* (2000) 5, 1079-1202.

102 Schmitt, Harrison Dinniss & Wingfield, *supra* note 24; J. T. G. Kelsey, 'Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare', 106 *Michigan Law Review* (2008) 7, 1427-1452.

103 *Id.*, 1449-1450.

organizations will lead to the creation of a new legal framework any time soon, especially in a domain as fundamental as peace and security. A second possibility consists in designing a treaty on cyber war, a proposal which has been discussed at length by several writers.[104] Once again, it is hard to predict how states will respond to the call for regulation. In any event, the cyber wars of tomorrow will not be put on hold as a result of their ambiguous legality.

[104] D. Brown, 'A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict', 47 *Harvard International Law Journal* (2006) 1, 179-221; Hollis, *supra* note 4, 1057-1061; P. A. Johnson, 'Is it Time for a Treaty on Information Warfare?', in M. N. Schmitt & B. T. O'Donell (eds), *Computer Network Attack and International Law* (2002), 439-455; S. J. Shackelford, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law', 27 *Berkeley Journal of International Law* (2009) 1, 246-251.