International Law Research; Vol. 2, No. 1; 2013
ISSN 1927-5234 E-ISSN 1927-5242
Published by Canadian Center of Science and Education

Article 2(4) and Cyber Warfare: How do Old Rules Control the Brave New World?

Jason D. Jolley[1]

[1] Post-Graduate Researcher (Law), School of Law, University of Glasgow, Glasgow, UK

Correspondence: Jason D. Jolley, Post-Graduate Researcher (Law), School of Law, University of Glasgow, Glasgow G12 8QQ, UK. Tel: 44-744-713-6506/1-216-832-0675. E-mail: j.jolley.1@research.gla.ac.uk

Received: August 23, 2012 Accepted: December 17, 2012 Online Published: July 5, 2013

doi:10.5539/ilr.v2n1p1 URL: http://dx.doi.org/10.5539/ilr.v2n1p1

1. Introduction

With the past attacks on Iranian nuclear infrastructure utilizing sophisticated weaponized computer code, such as the Flame worm, (Note 1) Stuxnet (Note 2) virus and Duqu (Note 3) worm, it is apparent that the age of cyberwarfare (Note 4) is upon us. While many commentators have been predicting this eventuality (Note 5) the transition from theory to reality has exposed gaps within the international legal framework regulating the use of force by states. (Note 6)

While many commentators argue that traditional rules on the use of force and *jus ad bellum* control by analogy, (Note 7) the debate is far from settled. The question becomes how do old rules control the brave new world of cyber warfare, (Note 8) in that we are applying rules of warfare developed over generations utilizing similar kinetic weapons (Note 9) to a new style of warfare that has only recently come into its own; with major cyber attacks starting in the Spring of 2007. (Note 10) Combined with the fact that the new style of warfare is unlike anything utilized before in the history of warfare, (Note 11) and the fact that the rules governing the use of force were arguably written with traditional 20th century warfare in mind, we have conundrum.

Since its inception and entry into force, the United Nations Charter article 2(4) controls the use of force by states. Article 2 (4) 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…" (Note 12) This seemingly straight foreword prohibition has one major issue. The Charter never defines what it means by the term "force" anywhere within the Charter. (Note 13)

One may suppose that when the drafters of the Charter articulated their thoughts on the prohibition of force, the drafters were mainly concerned with the military force that had been utilized in World War II (e.g., tanks, planes, conventional arms, and nuclear weapons), which had served as one of the impetus for the drafting of the Charter. (Note 14) This idea is supported by further reading article 51 of the Charter, the one exception to the article 2(4) prohibition on force, the drafters of the Charter seemingly associate force with an "armed attack." (Note 15) Article 51 posits 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…" (Note 16) This reading though does not end the debate surrounding what is meant by the term "force." That is, does the prohibition of the use of force only apply to kinetic weapons, (Note 17) that were considered armed attacks in 1947, or is the term "force" malleable in that it encompasses traditional weapon systems and future weapons system?

This debate is important given the technological changes in how wars are waged. While until recently wars were fought with weapons and tools almost identical as those found when the Charter was written, with the advent of the computer information systems and the internet, and states increasingly reliance upon these tools, there is a subtle albeit significant change in how states now may wage war. As Clarke states:

> [c]yber attacks have the potential to reach out from cyberspace into the physical dimension, causing giant electrical generators to shred themselves, trains to derail, high-tension power-transmission lines to burn, gas pipelines to explode, aircraft to crash, weapons to malfunction, funds to disappear and enemy units to walk into ambushes. (Note 18)

The ability for cyber attacks to carry out their attacks is unlike any form of weapon in history.

Cyber attacks do not rely on a delivery system *per se*, they simply rely on the information networks that span the globe, the same networks that states rely upon for everything from entertainment to banking to space travel. Indeed as the world's reliance upon information systems grows so to does the reach and potential impact of cyber attacks. One could say that states are creating the delivery system for their potential enemies every time they upgrade their information systems infrastructure. It is this availability of networks, combined with the ease of attack and the insidiousness nature of the attack that make cyber attacks even more attractive for certain types of warfare where deniability is important.

It is important at this juncture to distinguish and clarify the issue. As cyber warfare and cyber espionage are closely related, many of the same vulnerabilities that make a state susceptible to cyber warfare also make it susceptible to espionage. Espionage, being more akin to traditional information gathering, e.g., spying. The use of information systems and the Internet to conduct non-kinetic espionage is lawful under the current international treaties and norms. (Note 19) These varying uses of cyber space cloud the issue greatly as many commentators confuse the two as they assign different values to different acts.

This is the crux of the question presented. If a state can be negatively affected without the recourse to kinetic force, is it a violation of article 2(4)? Schmitt states, "the mainstream view among international law experts is that the "other manner" language extends coverage [of article 2(4)] to virtually any use of force not authorized within the charter." (Note 20) This still leaves the issue of what is force in a cyber attack?

Many commentators assume that the use of cyber-warfare is violative of U.N. Charters article 2(4) prohibition on the use of force. They assume so *argumentum a silentio,* without defining what force actually is or what act they are referring to. This article will attempt to define what force is for the purposes of article 2(4) for cyber warfare and attempt through the use of existing tests and positing a new test for force to show through case studies what force is and isn't for the purposes of article 2(4) in regards to cyber warfare.

This article will briefly analyze cyber attacks in Estonia, Republic of Georgia and Iran (Stuxnet and Flame) in an attempt to ascertain if the hostile acts against these states may be considered force for the purposes of U.N. Charter article 2(4) prohibition. These cyber attacks will be analyzed utilizing Schmitt's seven criteria for determining whether a cyber-attack meets the level of armed attack or force prohibited by article 2(4). (Note 21) This article will then consider these attacks in light of the "instrument-based test… [which] checks to see whether the damage caused by a new attack method previously could have been achieved only with a kinetic attack;" (Note 22) and a lastly will posit a totality-of-the-circumstances ("net effect") test to determine the effects of a cyber attack for the purposes of article 2(4) force. It is important to note that this article will not utilize what Carr refers to as the "Strict Liability Test" as this test automatically assumes that any cyber attack on critical infrastructure amounts to force. (Note 23) This article would argue that every cyber attack implicates a critical infrastructure in the form of a States networking and Internet / intranet and exposes its infrastructure to further exploitation even if it is not directly attacked. Therefore by this test one could argue that every cyber attack amounts to the use of force in violation of article 2(4) without ever addressing the actual harm or reason for the attack.

2. What Is Force?

This section will begin by looking at various definitions of force and positing a unified definition of force for the purposes of article 2(4) analysis of force. It will then address the related concepts of force and aggression and finally it will posit a framework for analysis for determining what force is.

2.1 Defining Force

The United Nations Charter never defines what it means when it uses the term 'force' as such per the Vienna Convention on the Law of Treaties article 31(1) "[a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose." (Note 24)

The object and purpose of the United Nations Charter is straightforward. Article 1 of the Charter states

The Purposes of the United Nations are*:*

> To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace… (Note 25)

We may distill article 1 to its core elements that include the "maintan[ance] of peace and security… the prevention and removal of threats to peace… and the suppression of acts of aggression…" (Note 26) Therefore the definition of 'force' which is prohibited by article 2(4) of the Charter must relate to the core elements as distilled *supra*.

As for the Vienna Convention on the Law of Treaties article 31(1) "ordinary meaning" (Note 27) we may turn to the Random House Dictionary. Random House lists 36 various definitions for force in various contexts. For instance, force may be a "physical power or strength possessed by a living being… [or] strength or power exerted upon an object; physical coercion; violence… [or] power to influence, affect, or control… [or] persuasive power; power to convince." (Note 28) These definitions may be germane to what he drafters of the U.N. Charter believed article 2(4) as it may be argued that article 2(4) encompasses all of these ideas. Whether force must be a physical act on behalf of an aggressor state or encompasses more and embodies other forms of coercion is debatable.

For instance, in the early 1970's many allies of the former Soviet Union argued that "economic aggression" (Note 29) against a state should be violative of the article 2(4) prohibition on the use of force. (Note 30) While this view never was fully embraced (Note 31) it does lend credence to the question of what are the boundaries of article 2(4) force. If we look to other sources such as physics for assistance we find little to dissuade from the argument that force must encompass a physical act.

In physics, force is defined in its most axiomatic terms as either a push or a pull on an object, (Note 32) "[i]n general, [] force is an interaction that causes a change." (Note 33) This too seems to be applicable to the article 2(4) definition, in that force utilized by a state is arguably intended to result in a change to whomever it is directed toward. In physics and for our purposes force may best be exemplified by Newton's First and Third Laws, which states "[a]n object initially at rest is predicted to remain at rest if the total force on it is zero, and an object in motion remains in motion with the same velocity in the same direction." (Note 34) Newton's Third Law holds "that for every action there is an equal and opposite reaction." (Note 35) That is that an object moving in a constant will only changed by an outside force acting upon it just as a state will remain on a path until a force acts against it. It is a given that in physics force relates to a physical body, but, does the law recognize it the same way?

Black's defines force as "[p]ower, violence, or pressure directed against a person or thing." (Note 36) If we break down the component parts to Black's definition we see that:

- Power is "the ability to act or not to act… Dominance, control or influence over another." (Note 37)
- Violence is "the use of physical force usually accompanied by fury. (Note 38)
- Pressure is the "exertion or the use of exertion against a person or thing that resists; coercion." (Note 39)

If one parses the various definitions of force posited, it becomes apparent that one of the key elements present within the definitions of force is its impact upon something physical. This article would posit that for the most part, the key to identifying what is force, is that it is an act that results in a physical change in something whether it be in physics or law the end result of a forceful act is a physical change in something. This article would posit that if the end result is a physical change then it is force under the traditional article 2(4) rubric.

The problem with the forgoing definition is that it does not fully encompass the new weapons systems / techniques involved in cyber warfare. The second part of the definition of force must embrace the differences between kinetic weapons systems and those, which are utilized in cyber warfare. To this end, this article would hold that force must be defined to encompass not only the corporal effect of an act, but also the electronic effect, or cyber effect that an attack might have on a nation. That is, if a state is subjected to a purely cyber attack that does reach the type of damage or effect that a kinetic weapon would have yet still results in damage to computer systems or information systems then that too would be an attack. One must remember that unlike past conflicts in cyber warfare military might goes beyond force of traditional arms. States weapons systems no longer occupy a traditional niche e.g., planes, tanks, and warships.

In cyber warfare lines of code are the new weapons, ones, which literally attack and disrupt lines of computer code either forcing an act to happen or preventing one from happening. (Note 40) Cyber warfare is the penetrating of a states computer systems with the intent to do military harm. (Note 41) Therefore the definition of force must encompass this fact. Force must be more than a kinetic idea.

For article 2(4) purposes and definition of force in cyber warfare, a subjective element must be introduced, that is, if a states computer networks are penetrated by another state, with the *intent* of doing military harm to the

offended state through cyber attacks and the offended state is harmed by the act, this is force as prohibited by article 2(4).

2.2 Force and Aggression

A closely related concept to force is aggression. Indeed many commentators believe the French language translation of article 51 of the U.N. Charter better represents the true intention of the drafters regarding force. (Note 42) In the French translation article 51 prohibits "*aggression armee*" ("armed aggression") (Note 43) instead of "armed attack" (Note 44) which according to Pierson is a much broader concept than the narrow interpretation normally associated with force. (Note 45) While the competing interpretations of article 51 seem to be in tension, guidance as to their interpretation may be found in the Vienna Convention on the Law of Treaties article 33(4) states that "when a comparison of the authentic texts discloses a difference of meaning which the application of articles 31 and 32 does not remove, the meaning which best reconciles the texts, having regard to the object and purpose of the treaty, shall be adopted." (Note 46) Given the purpose of the United Nations Charter as discussed *supra*, the French interpretation of article 51 arguably covers the use of cyber attacks against states much better than the English equivalent. This interpretation is bolstered by further acts of the United Nations General Assembly.

The United Nations General Assembly addressed the issue of aggression in Resolution 3314 (Note 47) where it defined aggression in article 1 as "the use 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, as set out in this Definition." (Note 48) While this document suffers from the same problem as the Charter, in that it is a pre-cyber age document. It does allow use to infer, what acts would constitute aggression in the cyber age.

For instance, Res. 3314 , art. 3 para. C holds that '[t]he blockade of the ports or coasts of a State by the armed forces of another State" constitutes aggression**,** so one could infer that the electronic blockading of banking data by one state of another states would constitute aggression in that it could have a similar economic affect as that of a traditional blockade. Indeed, if a state disrupts a states economy utilizing cyber attacks; this may constitute aggression, which by the general assembly's definition is against the U.N. Charter (while it is recognized that a General Assembly resolution has no force of law, it is arguably representative of state practice.)

2.3 Framework for Analysis

This section will analyze three recent cyber incidents that have occurred since 2007. The incidents have been widely reported in journals and newspapers but lack some specificity, e.g., definite attribution for the perpetrators, and in the case of Stuxnet and Flame incidents the actual damage incurred as a result of the attacks. As such this article will deal with each incident in general based upon what information is available to the public through popular media based upon the aggregate of numerous independent sources when available. While it is recognized that this lack of specificity is not ideal, these examples will serve their intended purpose of illustrating the issues surrounding the definition of force in cyber warfare.

2.3.1 Schmitt's Test

Michael N. Schmitt has hypothesized that "an effect-based analysis of a particular cyber incident [should be applied] to determine whether or not it equates to an armed attack as understood by article 51." (Note 49) Schmitt posits seven factors to be analyzed to determine if "a particular cyber event constitutes force… [they are:]

- [s]everity
- [i]mmediacy
- [d]irectness
- [i]nvasiveness
- [m]easurability
- [p]resumptive legitimacy [and]
- [r]esponsibility" (Note 50)

For severity Schmitt holds that any "consequences involving physical harm to individuals or property will alone amount to a use of force." (Note 51) He then places a minimum impact test on severity though stating that "[t]hose generating only minor inconvenience or irritation will never do so... the more the consequences [of the cyber attack] impinge on critical national interests…" the more likely they will be found to constitute the use of force. (Note 52) To Schmitt this is the most important element of the seven posited. (Note 53)

For immediacy, Schmitt states that the sooner the results of the attack "manifest" (Note 54) the greater the concern it is to states as they will have less time to seek a peaceful end to the matter. (Note 55) Directness relates to the "chain-of-causation" (Note 56) the but-for the cyber attack the results would not of happened.

The "invasiveness" element goes to the fact of how hard the defending state tries to protect a system from attack yet the aggressor state still penetrates the network. The more protected the system that is affected by the cyber attack the more invasive the attack. (Note 57) It must be noted although that Schmitt does limit this element in the event of espionage. "[C]yber exploitation is a pervasive tool of modern espionage. Although highly invasive, espionage does not constitute a use of force… under international law absent a nonconsensual physical penetration of the target-States territory…" (Note 58)

Measurability is seemingly straightforward in that it is the actual damage caused by the cyber attack. Schmitt does not look to the cost of the attack to the offended state, but the corporal damage, that is "X deaths, Y buildings destroyed, etc." (Note 59)

Presumptive legitimacy relates if the act is normally legitimate in international law. Schmitt utilizes the examples of "propaganda, psychological warfare, or espionage." (Note 60)

Lastly, responsibility relates to the state responsible for the attack under international law, Schmitt posits that "[t]he close the nexus between a state and the operation, the more likely the other State will be to characterize [it] as a use of force…" (Note 61)

2.3.2 Instrument – Based Test

This test is intended "to see whether the damage caused by a new attack method previously could have been achieved only with a kinetic attack." (Note 62) Carr utilizes the example of whether a cyber attack shuts down a "power grid." (Note 63) Carr posits that if it does it is then force as the same results could have only previously been achieved via conventional weapons. (Note 64)

2.3.3 The Net – Effect Test (Note 65)

This article would propose an alternative means for the testing of force in cyber warfare for the purposes of article 2(4). This test would look at the cyber attack in its totality to determine whether the net effect of the attack was such to constitute a military use of force against a state. This test does not concentrate on any given elements of an attack nor place any weight on the fact that the results of the attack are similar to those of a kinetic attack. (Note 66) This test utilizes the basic legal definition of force as stated by Black's in that it looks at the "[p]ower, violence, or pressure directed" (Note 67) at a state via a cyber attack in its totality.

In this test power and pressure are much more relevant in their non-physical form and refer more to the impact upon a network or computer system that may not be able to be measured through a normal means of force. For instance, if an aggressor state launches a cyber attack which shuts down a large portion of a states banking system, causing fear or panic in its population, without causing any physical manifestation, yet causes the states economy to suffer because the aggressor state is displeased at an act of the offended state.

Under the net effect test this would be a use of force in contravention to article 2(4). It would be force in that this attack was directed at a state with the intent to punish the state for a lawful act, the cyber attack impacted a core component of the states infrastructure (banking), and the attack negatively impacted a states population causing fear or panic. The net effect of the attack was that of applying pressure or exerting power against a state for an act, therefore the attack was force. Warfare has now evolved to the point where no corporal force need be utilized to affect a state negatively.

3. Case Studies

In this section we will briefly analyze three major cyber incidents that have occurred since 2007. We will analyze the use of the

(1) Stuxnet Virus on Iranian nuclear centrifuges;

(2) the Flame Malware infestation of Iranian gas and oil systems; and the

(3) DDOS (distributed denial of service) attacks on Estonia (2006) and the Republic of Georgia (2008) (while these are two separate attacks they will be analyzed jointly in that the methods of attack were very similar).

It is important to note although that while every effort has been taken to be accurate, the facts for analysis have been derived from popular reporting and as such their veracity cannot be ascertained. It is also important to note that the analysis of each attack will be brief as it is beyond the scope of this article to go into an in-depth analysis

on one of these attacks let alone three. The analysis given here is for representative purposes and is not intended for a full legal or technical analysis of either the law or the individual incidents.

3.1 Stuxnet Virus

The Stuxnet virus (worm) was reportedly the first weaponized computer virus to target a specific industry. The virus "was almost certainly designed to make damaging, surreptitious adjustments to the centrifuges used at Natanz, Iran's uranium enrichment site" (Note 68) The virus was first discovered in July 2010 and reportedly destroyed or damaged up to 2,000 of Iran's centrifuges used in the enrichment of uranium. (Note 69)

The virus was a highly specialized program designed specifically "to target Simatic WinCC Step7 software, an industrial control system made by the German conglomerate Siemens." (Note 70) Which controlled various machines in different industries. What was unique about Stuxnet was its ability to "phone home [contact outside computer servers in Europe]… and let the attackers update Stuxnet on infected machines with new functionality or even install more malicious files on systems." (Note 71) While much is still unclear as to how the attack was carried out (many media reports subscribe to the theory that it passed to the Iranian computers via a smuggled USB thumb drive (Note 72)) and the popular media is rife with theories, everyone can agree that this attack was carried out without any kinetic force being applied yet Iranian centrifuges were destroyed.

If traditional weapons had been used to knock out the nuclear reactors then Iran would have the right to respond in self-defense. (Note 73) Since cyber-weapons were utilized, there is no consensus on whether the use of cyber weapons actually constitutes force.

While the dearth of solid verifiable facts in the Stuxnet attacks make it difficult to accurately verify the tests utilized this article will attempt to do so for theoretical purposes.

We will begin with the instrument-based test. This test is intended "to see whether the damage caused by a new attack method previously could have been achieved only with a kinetic attack." (Note 74) The Stuxnet attack would clearly constitute force under this test as if reports are true that up to 2,000 centrifuges were destroyed by the virus. Prior to the cyber age, such results only could have occurred through the use of a kinetic attack, such as a bombing or use of other explosives.

Schmitt's test begins with severity; here the Stuxnet virus appears to exceed the requirement to be considered force in that it "involves physical harm to… property… which [seemingly] impinge[d] on critical national interests." (Note 75) In this instance the destruction of up to 2,000 centrifuges clearly meets this prong. As this is the most important prong in Schmitt's test one could argue that by meeting it force has been used in a cyber attack. We will look at the test in its totality though to ensure proper analysis.

The next prong of Schmitt's test, immediacy, is more difficult to analyze in that it is unknown how long it took for the virus to "manifest." (Note 76) Since Iran and whoever conducted the attack although have never sought out a peaceful solution to the incident, as Schmitt discusses, this article would posit that this prong is not met. Closely related to this prong though is what Schmitt refers to as the directness prong or the "chain-of-causation" (Note 77) is met in that but-for the virus (Note 78) the results would not have happened.

One may posit for the invasiveness prong, that Iran did everything within its powers to protect its nuclear centrifuges; therefore this prong is easily met. While we do not know the true damage caused by the Stuxnet virus on the Iranian centrifuges, we may presume that the actual damage caused is measurable, that is how many centrifuges were actually damaged by the attack. Therefore the measurability prong would be met.

The presumptive legitimacy is not met. This prong relates to whether the use of a cyber weapon was legitimate in international law. This attack, without Security Council approval, and without the excuse of self-defense, meets the legitimacy prong, in that the aggressor state acted illegitimately hence the more likely that such an act is unlawful force. Lastly, the responsibility prong failed in that it is a nullity as no state has accepted responsibility for the attack.

For the purposes of the Schmitt test, the use of the Stuxnet virus on the Iranian nuclear centrifuges would arguably constitute force. The problem herein though is that there are too many unknowns involved with the analysis to say for certain under this test that it is or is not force.

Under the net-effect test, it is important to look at the cyber attack in its totally that is from the macro to the micro. To begin with, one may consider the political environment, prior state or international actions, and the potential motivation of aggressor states. In addition one may address as Riesman posits "[w]ill a particular use of force, whatever its justification otherwise, enhance or undermine world order?" (Note 79) Once these macro questions are answered one may address the micro level questions and look at the effects of the cyber attack

including what was stated *supra* the "power, violence or pressure directed" (Note 80) at the state by the cyber attack.

In the Stuxnet attack, Iran was (and is) under sever political pressure to stop the production of enriched uranium, which many commentator believe will lead to the inevitable acquisition of atomic weapons by Iran. (Note 81) Add to the fact that both the United States and Israel have both the technology and the military and political will to conduct such an attack, (Note 82) and one may start to see the trend that this was an attack for article 2(4) purposes. Add to the fact that the attack displayed power on behalf of the attacking states in that they were able to attack a high security target without notice, that the attacks created violence in the form of destroying centrifuges, and was pressure upon the government, the net effect of the cyber attack should be considered to be force.

3.2 Flame Malware Attacks

The Flame malware attacks are a recent and developing series of attacks first reported in the media in late-May, early-June 2012 (Note 83). While to date there have been no reports of damage cause by the Flame malware, (Note 84) as has been described as a "cyber-espionage toolkit" (Note 85) rather than an offensive weapon. This is an interesting, albeit routine use of cyberspace, as it is not intended to cause physical damage yet may be argued it is force in that it is appropriating sensitive information important to a states security. While many commentators have stated that it is a state-sponsored cyberweapon, (Note 86) one must ask if it truly is.

While it has been reported that the Flame Malware is closely related to the Stuxnet virus, (Note 87) the purpose behind Flame has been different from Stuxnet which caused corporal damage, and Flame is more of an espionage tool. (Note 88) This is an important distinction in our attempt to define force for cyber attacks under article 2(4) and highlights one of the difficulties of utilizing an effect based definition, in that the effect of cyber espionage will not normally be corporal damage.

This article will apply the three tests posited supra to the Flame malware attacks based upon the reported attacks on the Iranian oil production facilities as "Kaspersky Lab['s stated that] the Flame virus has struck Iran the hardest, but has been detected in the Palestinian territories, Sudan, Syria, Lebanon, Saudi Arabia and Egypt… And Israel." (Note 89) Leading some to speculate that this attack was focused at Iran and it's ability to produce oil, as one of the effects of the Flame malware was to wipe hard drives of data in "Iran's energy industry." (Note 90)

An analysis of the Flame malware allows us to demonstrate the difficulties of discerning what constitutes a use of force and what is force in cyber attacks. As it is arguable that the use of Flame malware is an attack, but was it force for the purposes of article 2(4)?

While there is very little facts available concerning what, if any damage the Flame malware has caused, it is apparent that the intent of the malware was to steal protected information and disrupt the energy infrastructure in Iran. (Note 91) While under a strict liability standard, (Note 92) this would be a use of force as it affects a nations infrastructure, would any other test hold so?

As discussed supra we will begin with the instrument-based test, as it is the easiest to deal with. This test is intended "to see whether the damage caused by a new attack method previously could have been achieved only with a kinetic attack." (Note 93) This test would fail in this incident as while some damage has been reported to the hard drives of the servers (Note 94) no kinetic weapon known (Note 95) could have wiped data from a hard drive without causing damage to anything else. There have been no reports of the computer systems themselves being damaged, just the data being wiped from their hard drives, a solely unique problem to cyber weapons. Under the instrument-based test the Flame malware would not constitute force.

For continuity purposes we will next apply Schmitt's test in the same manner we did *supra*.

Schmitt's test begins with severity, this raises several questions in regards to the Flame malware involving what damage it actually did. Media reports state (Note 96) that the Flame malware did wipe the hard drives of computers and servers, which arguably is physical, albeit minimal damage, so one may argue that the Flame malware did "involve physical harm to… property… which [seemingly] impinge[d] on critical national interests." (Note 97) It is arguable that the wiping of the hard drives seemingly impacted "critical national interests." (Note 98)

In this instance although without a tangible means of assessing the damage caused, a *prima facie* subjective analysis would hold that this prong has not been met. The physical impact is just too minor and the national interests arguably were not impacted that long. The first prong of Schmitt's test has not been met.

The next prong of Schmitt's test, immediacy, is here, as it was with the Stuxnet virus, more difficult to analyze in that it is unknown how long it took for the virus to "manifest." (Note 99) This prong must be considered a nullity for the purposes of our analysis.

Interesting enough the "chain-of-causation" (Note 100) prong raises more questions than may be answered at the present, while it is recognized that the malware did cause minimal damage, one must ask what the long-term effects of the Flame malware will be to the state of Iran in that what intelligence and data was given to the aggressor state is unknown. In that respect the true damage to the state of Iran is unknown, but the chain-of-causation that Schmitt discusses could arguably be met if the attack results in long-term damage to Iran's national security.

Again as stated *supra,* the invasiveness prong is seemingly met in that Iran theoretically did everything within its powers to protect its computer systems and secrets; e this prong is easily met. The measurability prong though must again be a nullity in that based upon the reporting and data available one cannot assess the measure of damages that this malware caused. If one is to believe the Iranian government (Note 101) it was minimal but that report must be treated with skepticism until independent verification is available.

The presumptive legitimacy prong is again a mixed question as traditionally the "nondestructive, surreptitious intelligence collection" (Note 102) against another state has been legal under customary international law and as Scott states "[n]o international convention has ever addressed the legality of peacetime espionage." (Note 103) The only question then becomes the legality of wiping the data from the hard drives of the infected computer systems. This is arguably beyond the normal cyber esponage, but as discussed *supra* the affects of such an act were minimal. So balancing the factors the subjective interpretation on this would be that the use of Flame is a legitimate one in the respects to cyber espionage.

Lastly, the responsibility prong again fails in that no state has accepted responsibility for the attack.

Under this analysis the Flame attacks technically would not amount to force under art 2(4).

If we look at the Flame attack at the macro level, it would appear that the intent of the attack was driven more towards intelligence gathering and economic sabotage than that normally associated with traditional uses of force. While it is accepted that economic sabotage may rise to the level needed to amount to force or as *casus belli*, in the instant matter it is unknown whether the primary purpose of the Flame malware was to gather intelligence and then cover its use under the guise of sabotaging the computers it infects. Given that any information technology infrastructure would be following standard best practices of backing up their data, it would seem to one that this wiping of data from hard drives was intended to be more of a nuisance than anything. While this is conjuncture on the part of this article, absent any further information it seems most likely. From the macro standpoint this would appear not to be force.

One may argue although, that at a micro level this was intended to convey a hostile message to Iran, which could act as a threat to its national security. In addition the malware targeted infrastructure on national importance, but the reported *de minimis* damage caused lends credence that this attack while targeting a national infrastructure did not rise to the level of force on any level.

3.3 Attacks on Estonia (2006) and the Republic of Georgia (2008)

The DDOS (Note 104) attacks against Estonia and the Republic of Georgia, while both geographically and temporally different are very similar for our purposes and as such will be considered together. Estonia was targeted during May 2007, (Note 105) and the Republic of Georgia in August 2008, (Note 106) both attacks had been blamed on individuals and groups operating within Russia though never proven. (Note 107) Both attacks were for political (Estonia) and political – military reasons (Republic of Georgia). The attacks on Estonia purportedly in response to the Estonia government removing a Soviet War memorial in the city of Tallinn, (Note 108) and the attacks on the Republic of Georgia as a precursor to the invasion of Russian troops of South Ossetia. (Note 109)

Both incidents were distributed denial of service attacks in which specific computers were bombarded with millions of requests per second, with the result of these systems being overloaded and eventually shut down. The DDOS attacks in both cases targeted government websites, media outlets, banking systems and other infrastructure. (Note 110)

As discussed *supra*, we will begin with the instrument-based test; this test is intended "to see whether the damage caused by a new attack method previously could have been achieved only with a kinetic attack." (Note 111) An instrument-based test is difficult to apply in this situation in that in both cases, in Estonia and Republic of Georgia, critical information systems were knocked out, albeit temporarily. The differentiation herein, is that

no physical damage was inflicted, that is, once the attacks ceased, the systems inflicted started operating again. As such, this article would posit that the instrument-based test, as applied here, would not find that the attacks were force.

We now attempt to apply Schmitt's test to these attacks. Again as stated *supra*, Schmitt's test begins with severity. The severity of the attacks on Estonia and the Republic of Georgia were severe in the sense that they knocked out forms of communication and critical infrastructure, for instance during the DDOS attack on Georgia, numerous banks could not operate as the Georgia banking system had shut down its online banking sector, and the Georgian banks could not communicate with the "international banking community." (Note 112) But to satisfy this prong the attacks need to "involve physical harm to… property… which [seemingly] impinge[d] on critical national interests." (Note 113) Here there was no physical harm, while a critical national interest was attacked, this prong is not met.

The immediacy prong was met in that once the DDOS attacks were launched in a relatively short period they were "manifest." (Note 114) They had an almost immediate impact on connectivity, while initially this would have been a minor slow down in accessing information; they bloomed to a full-scale denial of service within a relatively short period. (Note 115) This prong is met.

The "chain-of-causation" (Note 116) prong again was met, in that there was a causal connection between the attacks and the denial of service.

As for the invasiveness prong, this is harder to judge as most of the sites involved were network servers probably employing low-grade security. Unlike the previous examples, the servers involved here did not enjoy military grade software and probably have been hacked previously. So it would be hard to argue that these attacks were invasive in that sense.

The measurability prong though was met in that it was easy for the affected governments and institutions to quantify the damage done by measuring everything from lost profits on behalf of the banking center, to lost server days and lost website days for the other components impacted. This prong would be met.

The presumptive legitimacy prong is not met here, as the attacks are not legal under international law as they are arguably the interference of internal state matters by another state, which is illegal in international law. (Note 117)

Lastly, the responsibility prong is met in that while Russia has not taken direct responsibility itself, it has admitted that parties unknown within Russia carried out the attacks and has seemingly adopted the attacks. As such Russia is arguably responsible for the acts of those individuals residing within its territory that conducted the attacks. (Note 118)

As for whether this attack would be considered force under the Schmitt test is a difficult question as at best the results are a push. That is, that the primary question of the first prong was a negative, and the weighing of the subsequent prongs are mixed, it comes down to a judgment call, in that respect this article would posit that under the Schmitt test the DDOS attacks on Estonia and the Republic of Georgia would be a negative.

Under the net-effect test this seems to be recourse to force on the part of the aggressor state, whether by the state of Russia or forces acting within Russia. These attacks were seemingly intended to intimidate and to harm the respective states for an act in the case of Estonia, and as a precursor to other force on the behalf of Georgia. In addition the timing of these attacks left no real doubt that some party was sending a message to the states, lending credence to the theory that they were meant to intimidate ("power" in Black's definition) and to potentially coerce / apply pressure on the affected states.

4. Conclusion

If we look at the three case studies, we see that if the cyber attack results in corporal damage then all of the tests posited would find the attacks to be force. The tests also seemingly agree that when the focus of the cyber attacks is purely espionage that result in no or minimal damage those attacks do not rise to the level of force either.

The problem arises when the attack falls within the gray areas in between. In addition, as the cyber attacks on Estonia and the Republic of Georgia demonstrate, states may be attacked and result in very little corporal damage, but are arguably a use of force as they are a form of coercion placed upon the state.

It is important to remember that the world is continuing to become dominated by cyber space. The vast majority of services, from shopping, banking, and game playing to finding a mate and social interactions, all now seemingly evolve around the use of cyber space. Critical infrastructure relies almost entirely upon it to control everything from water purification plants to oil processing, to communications, and practically everything else.

We are a digital world that relies on cyber space, according to the International Telecommunication Union, an incredible 86.7% of the world population have cellular subscriptions (78.8% for developing economies). (Note 119) With 73.8% of the developed world (26.3% undeveloped) having Internet access. (Note 120) This fact alone changes the idea of force as someone theoretically could disrupt cellular communications using a virus that could disrupt billions of people's lives and never truly have a corporal effect.

This is where the tests go wrong where they place emphasis on the corporal effect of the attacks. While this is logical given the traditional and practical interpretation of force (Newtonian), it is not practical given the changing nature of technology. As technology changes, so must the concept of force. In a theoretical attack on the United States, if one were able to shut down cyber communications and transfer of information via the internet, for all sense and purpose one could shut down the entire U.S. Government without intentionally doing any corporal damage.

It is because of this reliance upon cyber space that the definition of force and how to test for force in international law needs to be reassessed. In addition, collective action needs to be taken on the part of the international community. This collective action needs to be through a multilateral treaty prohibiting cyber warfare and adopting the Security Council definition of cyber warfare as stated in Security Council Resolution 1113. (Note 121)

Without a prohibition on cyber warfare states will continue to utilize cyber warfare without regard to international norms, as long as a state may argue that their acts do not violate international law they will exploit that fact to the detriment to other nation states which will result in a continued escalation of nefarious acts in cyber space.

Acknowledgements

The author wishes to thank Dean Mark J. Sundahl, Cleveland – Marshall College of Law, for his assistance in this paper. This paper started initially as an independent legal research project as part of my LL.M course work at Cleveland – Marshall that Dean Sundahl was kind enough to supervise. I would also like to thank Prof. Christian Tams, University of Glasgow, for his supervision and assistance in my continuing research. Any errors contained herein are completely mine alone.

Notes

Note 1. Ben Johnson, *Malware Worm "Flame" Stealing Data, Recording Audio From Personal Computers in Middle East* (May 29, 2012), Slate.Com, http://www.slate.com/blogs/trending/2012/05/29/

Note 2. *See*, Kim Zetter, *Clues Suggest Stuxnet Virus Was Built for Subtle Nuclear Sabotage* (Nov. 15, 2010), Threat Level, Wired.com, http://www.wired.com/threatlevel/2010/11/stuxnet-clues/. (Discussing the belief that Stuxnet was created to specifically target Iranian nuclear reactors in an effort to disrupt Iran's believed pursuit of nuclear weapons.)

Note 3. Chloe Albanesius, *Iran Working to Control Duqu Virus Attack* (Nov. 14, 2011), PCMag.com, http://www.pcmag.com/article2/0,2817,2396348,00.asp. (Discussing the Duqu virus that had infected Iranian nuclear reactors with the intent to gather information.)

Note 4. *See*, Richard A. Clarke and Robert K. Knake, *Cyberwar* 6 (Kindle ed. 2010), (defining cyberwar as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption…") *See also*, U.N. Security Council Res. 1113 (2011), S/RES/1113 (2011), (stating that "[c]yber warfare is the use of computers or digital means by a government or with explicit knowledge of or approval of that government against another state, or private property within another state including:

-Intentional access, interception of data or damage to digital and digitally controlled infrastructure.

-Production and distribution of devices which can be used to subvert domestic activity.")

Note 5. *See, e.g.,* Jeffrey K. Walker, *The Demise of the Nation-State, the Dawn of New Paradigm Warfare, and the Future for the Profession of Arms*, 51 A.F. L. Rev. 323 (2001). ("Certainly the most ballyhooed of the new military-technological frontiers is in the area cyber warfare. This is an interesting but extremely complicated area of military operations, particularly from the legal viewpoint. Many within the military legal community think that computer network operations, international cyber law enforcement, and notions of use of force in cyber space easily fit by analogy into the existing law of war regime. I think otherwise. Just as the instantaneous transmission of ideas has done no small part to radically undermine the traditional internal sovereignty of nation-states, so will it undermine traditional international law notions that have been built up since the time of

Grotius on a presumption that the only important actors are sovereign states in control of geographically defined borders. In cyber space, borders simply don't matter.")

Note 6. *Cf.* Charles J. Dunlap Jr., *Perspectives for Cyber Strategists on Law for Cyberwar*, Strategic Studies Quarterly, Spring, 2011, at 81. (Quoting Jeffrey Addicott that "international laws associated with the use of force are woefully inadequate in terms of addressing the threat of cyberwarfare.")

Note 7. *Id. See also,* 51 A.F. L. Rev. 323 (2001.

Note 8. Aldous Huxley, *Brave New World* (1932).

Note 9. Similar in the respect that while the delivery systems and damage done by kinetic weapons has dramatically improved, the kinetic weapons systems utilized today are still the same basic weapons that have been used for hundreds of years.

Note 10. Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, 16 May 2007, THE GUARDIAN, http://www.guardian.co.uk/world/ 2007/may/17/ topstories3.russia

Note 11. 51 A.F. L. Rev. 323 (2001).

Note 12. U.N. Charter art. 2 para. 4. (Emphasis added).

Note 13. *Cf.* Ian Brownlie, *International Law and the Use of Force by States* 361 (1963). ("[T]he terms 'use of force' and 'resort to force' are frequently employed by writers [but] they have not been the subject of detailed consideration.")

Note 14. Anthony Clark Arend and Robert J. Beck, *International Law & The Use of Force* 8 (1993).

Note 15. *See generally*, Thomas Buergenthal and Sean D. Murphy, *Public International Law in a Nutshell*, §12-1 (4th ed. 2006) (Kindle ed.).

Note 16. U.N. Charter art. 51. (Emphasis added).

Note 17. Jeffrey Carr, *Inside Cyber Warfare* 58 (2010).

Note 18. Richard Clarke, *War From Cyberspace*, The National Interest, Nov. – Dec. 2010, at 31.

Note 19. Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A. F. L. Rev. 121, 139 (2009), (stating that "[a]rticle 24 of the Annex to the 1907 Hague Convention IV recognizes the lawfulness of espionage during armed conflict, specifically providing that "ruses of war and the employment of measures necessary for obtaining information about the enemy and the country are considered permissible." No international convention has ever addressed the legality of peacetime espionage and espionage has been practiced by states for centuries. Additionally, international law does not prohibit espionage as a fundamentally wrongful activity.") (Internal citations omitted).

Note 20. Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Colum. J. Transnat'l L. 885, 889 (1999).

Note 21. See, Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Colum. J. Transnat'l L. 885 (1999). *See also*, Jeffrey Carr, *Cyber Warfare* 658-661 (2010).

Note 22. Jeffrey Carr, *Inside Cyber Warfare* 59 (2010).

Note 23. *Inside Cyber Warfare* 59 (2010).

Note 24. Vienna Convention on the Law of Treaties, art. 31(1) (1969), 1155 U.N.T.S. 331.

Note 25. U.N. Charter art. 1, para. 1.

Note 26. *Id.*

Note 27. Vienna Convention on the Law of Treaties, art. 31(1) (1969), 1155 U.N.T.S. 331.

Note 28. Dictionary.com, *Force* (June 8, 2012), Random House Dictionary (Unabridged), http://dictionary.reference.com/browse/force.

Note 29. Derek W. Bowett, *Economic Coercion and Reprisals By States*, 13 Va. J. Int'l L. 1 (1972). ("States like Poland, Egypt and Czechoslovakia adhered [to]the concept of the "use or threat of force" should embrace economic aggression.") *But cf.*, Ian Brownlie, *International Law and the Use of Force by States* 362 (1963) ("[W]hilst it is correct to assume paragraph 4 [of art. 2] applies to force other than armed force, it is very doubtful if it applies to economic measures of a coercive nature.")

Note 30. 13 Va. J. Int'l L. 1 (1972).

Note 31. *Id*.

Note 32. Glenn Elert, *The Physics Hypertextbook* (2012), http://physics.info/newton-first/.

Note 33. *Id*.

Note 34. Benjamin Crowell, *Light and Matter* 127 (2010).

Note 35. *See, e.g.,* The Physics Classroom, *Newtons Third Law* (2012), http://www.physicsclassroom.com/class/newtlaws/u2l4a.cfm.

Note 36. Black's Law Dictionary 1257 (9th ed. 2011). (iPhone / iPad ed.)

Note 37. *Id*. at 1288.

Note 38. *Id*. at 1705.

Note 39. Collins English Dictionary (10th ed. 2009).

Note 40. *See, e.g.,* Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 1-9 (Kindle ed. 2010). (Discussing Israel's potential use of cyber techniques to disrupt Syrian Air Defense radars so they did not fire on Israeli aircraft during the bombing raid on a Syrian reactor Sept. 7, 2007).

Note 41. See, *id*. at 6. (Defining cyber war as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."

Note 42. U.N. Charter art. 51 states 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 any time such action as it deems necessary in order to maintain or restore international peace and security."

Note 43. Charles Pierson, *Preemptive Self-Defense in an Age of Weapons of Mass Destruction: Operation Iraqi Freedom*, 33 Denv. J. Int'l L. & Pol'y 150, 158 (2004).

Note 44. U.N. Charter art. 51.

Note 45. 33 Denv. J. Int'l L. & Pol'y 150, 158 (2004).

Note 46. Vienna Convention on the Law of Treaties, art. 33(4) (1969), 1155 U.N.T.S. 331.

Note 47. U.N.G.A. Res. 3314, A/9890 (1974); 1974 U.N. Rep. 143-144.

Note 48. U.N.G.A. Res. 3314, A/9890 (1974); 1974 U.N. Rep. 143-144.

Note 49. Charles J. Dunlap, Jr., *Perspectives For Cyber Strategists on Law For Cyberwar*, Strategic Studies Quartl'y 81 (Spring 2011).

Note 50. *Id. See also,* Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, *in Proceedings of Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* 155-156 (2010).

Note 51. Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, *in Proceedings of Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* 155 (2010).

Note 52. Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, *in Proceedings of Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* 156-158 (2010).

Note 53. *Id*.

Note 54. Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, *in Proceedings of Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* 156 (2010).

Note 55. *Id*.

Note 56. *Id*.

Note 57. *Id*.

Note 58. Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, *in Proceedings of Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* 156 (2010).

Note 59. *Id.*

Note 60. For an interesting discussion concerning the use of cyber psychological warfare during the second Gulf War, *see*, Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 9-11 (Kindle ed. 2010). (Discussing the United States penetration of secure Iraqi email systems and utilizing the system to dissuade Iraqi commanders from taking part in the defense of Iraq.)

Note 61. Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, *in Proceedings of Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* 156 (2010).

Note 62. *Id.*

Note 63. *Inside Cyber Warfare* 59 (2010).

Note 64. *Id. Cf.* Mathew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 Yale J. Int'l L. 421, 422 (2011). (Discussing a theoretical attack on Iran's nuclear reactors and the fact that if conventional weapons were used to gain the same results as a cyber attack then Iran would have the right to respond in kind.)

Note 65. This test is adapted from, W. Michael Riesman, *Criteria For Lawful Use of Force In International Law*, 10 Yale J. Int'l L. 279, 281 (1984-1985). ("[A]ppraisals of state resort to coercion can no longer simply condemn them by invoking Article 2(4), but must test permissibility or lawfulness by reference to a number of factors, including the objective and the contingency for which coercion is being applied.") *See also, id*, at 284. ("The net effect of a mechanical interpretation of Article 2(4) may be to superimpose on an unwilling polity an elite, an ideology, and an external alignment alien to its wishes.")

Note 66. It goes without saying although the more similar the end result of a cyber attack is to a corporal or kinetic attack the more likely it is to find that force has been used in contravention to art 2(4).

Note 67. Black's Law Dictionary 1257 (9th ed. 2011) (iPhone / iPad ed.).

Note 68. *See*, Christopher Williams, *Stuxnet: Cyber attack on Iran 'was carried out by Western powers and Israel'*, The Telegraph (21 Jan. 2011), http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.html. *See also*, CBS News, *Iran Confirms Stuxnet Worm Halted Centrifuges* (Nov. 29, 2010), http://www.cbsnews.com.2102-202_162-7100197.html

Note 69. Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History* (July 11, 2011), Wired.com, http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1.html.

Note 70. *Id.*

Note 71. *Id.*

Note 72. *Id.*

Note 73. *See*, Mathew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 Yale J. Int'l L. 421, 422 (2011).

Note 74. Jeffrey Carr, *Inside Cyber Warfare* 58 (2010).

Note 75. Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, *in Proceedings of Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* 156 (2010).

Note 76. *Id*.

Note 77. *Id*.

Note 78. Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, *in Proceedings of Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* 156 (2010).

Note 79. W. Michael Riesman, *Criteria For Lawful Use of Force In International Law*, 10 Yale J. Int'l L. 279, 282 (1984-1985).

Note 80. Black's, note 29 *supra* at 11.

Note 81. *See*, Brian Siegal, *Will Iran Wiggle Out of Global Demand To End Nuclear Quest* (June 6, 2012), Miami Herald, http://www.miamiherald.com/2012/06/14/2849996/will-iran-wiggle-out-of-global.html

Note 82. Ellen Nakashima and Joby Warrick, Stuxnet Was Work of U.S. and Israeli Experts, Officials Say (June 1, 2012), Wash. Post, http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

Note 83. Mathew J. Schwartz, *Flame Espionage Malware Seeks Middle East Data*, Information Week (May 29, 2012),

Note 84. Malware is defined as "software programs designed to damage or do other unwanted actions on a computer system…" TechTerms.com, *Malware* (accessed June 17, 2012), http://www.techterms.com/definition/malware.

Note 85. Elinor Mills, *Flame Malware Network Based on Shadowy Domains, Fake Names* (June 4, 2012), CNET, http://news.cnet.com/8301-1009_3-57446652-83/flame-malware-network-based-on-shadowy-domains-fake-names/.

Note 86. Elinor Mills, *Flame: A Glimpse Into The Future of War* (June 2, 2012), CNET, http://news.cnet.com/8301-1009_3-57445975-83/flame-a-glimpse-into-the-future-of-war/?tag=mncol;txt.

Note 87. Matthew Schwartz, *Flame Malware Code Traced To Stuxnet*, Information Week (June 11, 2012), http://www.informationweek.com/news/security/attacks/240001841#. ("In 2009, part of the code from the Flame platform was used in Stuxnet," said Alex Gostev, the chief malware researcher at Kaspersky Lab… "We believe that source code was used, rather than complete binary modules," he said, which suggests some degree of collaboration or crossover.")

Note 88. Mathew J. Schwartz, *Flame Espionage Malware Seeks Middle East Data*, Information Week (May 29, 2012), http://www.informationweek.com/news/security/attacks/240001094. ("The malware appears to have been developed not to target industrial control systems, as with Stuxnet, but to support other information-gathering and perhaps offensive capabilities. "From the initial analysis, it looks like the creators of Flame are simply looking for any kind of intelligence--e-mails, documents, messages, discussions inside sensitive locations, pretty much everything," said Aleks Gostev, a security researcher at antivirus vendor Kaspersky Lab…")

Note 89. Ali Akbar Darein, *Iran: 'Flame' Virus Fight Began With Oil Attack*, AP (May 30, 2012), http://www.google.com/hostednews/ap/article/ALeqM5jCs_9NmCUz0zKecVG4qgOKSI4iow.

Note 90. Greg Keizer, *Attacks on Iranian Oil Industry Led to Flame Malware Find*, Computerworld (May 29, 2012), http://www.computerworld.com/s/article/9227551/Attacks_on_Iranian_oil_industry_led_to_Flame_malware_find.

Note 91. Ali Akbar Darein, *Iran: 'Flame' Virus Fight Began With Oil Attack*, AP (May 30, 2012), http://www.google.com/hostednews/ap/article/ALeqM5jCs_9NmCUz0zKecVG4qgOKSI4iow.

Note 92. Jeffrey Carr, *Inside Cyber Warfare* 58 (2010).

Note 93. *Id*.

Note 94. Ali Akbar Darein, *Iran: 'Flame' Virus Fight Began With Oil Attack*, AP (May 30, 2012), http://www.google.com/hostednews/ap/article/ALeqM5jCs_9NmCUz0zKecVG4qgOKSI4iow.

Note 95. Outside of a electro-magnetic pulse (EMP) weapon, which arguably is not a kinetic weapon.

Note 96. Ali Akbar Darein, *Iran: 'Flame' Virus Fight Began With Oil Attack*, AP (May 30, 2012), http://www.google.com/hostednews/ap/article/ALeqM5jCs_9NmCUz0zKecVG4qgOKSI4iow

Note 97. Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, *in Proceedings of Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* 156 (2010).

Note 98. *Id*.

Note 99. Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, *in Proceedings of Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* 156 (2010).

Note 100. *Id*.

Note 101. CBS News, Iran: Powerful "Flame" Computer Virus Briefly Hit Oil Industry But Qas Defeated With Data Recovered (May 30, 2012). http://www.cbsnews.com/8301-202_162-57443629/iran-powerful-flame-computer-virus-briefly-hit-oil-industry-but-was-defeated-with-data-recovered/. ("Gholam Reza Jalali, who heads an Iranian military unit in charge of fighting sabotage, claimed that Iranian experts had detected and defeated the "Flame" virus. He told state radio that the oil industry was the only governmental body seriously affected and that all data that had been lost were retrieved.")

Note 102. Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 45 Air Force L. Rev. 217 (1999). ("[C]ustomary international law has evolved such that spying has become the long-standing practice of nations. Indeed, while the surreptitious penetration of another nation's territory to collect intelligence in peacetime potentially conflicts with the customary principle of territorial integrity, international law does not specifically prohibit espionage.")

Note 103. *Id*. at 218.

Note 104. *See,* Dictionary.com, *ddos*, Collins English Dictionary (10th ed.), accessed June 17, 2012, http://dictionary.reference.com. (DDOS or distributed denial of service attack is "a method of attacking a computer system by flooding it with so many messages that it is obliged to shut down.")

Note 105. Nate Anderson, *Massive DDoS Attacks Target Estonia; Russia Accused* (May 14, 2007), Ars Technica, http://arstechnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/. *See also*, Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 11-16 (Kindle ed. 2010).

Note 106. Dancho Danchev, *Coordinated Russia vs Georgia Cyber Attack In Progress* (Aug. 11 2008), ZDNet, http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670. *See also*, Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 16-20 (Kindle ed. 2010).

Note 107. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 19 (Kindle ed. 2010). ("[T]he Russian government claimed that the cyber attacks were a populist response that ws beyond the control of the kremlin.")

Note 108. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 11-16 (Kindle ed. 2010).

Note 109. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 16 – 20 (Kindle ed. 2010).

Note 110. *Id.*

Note 111. Jeffrey Carr, *Inside Cyber Warfare* 58-60 (2010).

Note 112. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 19 (Kindle ed. 2010).

Note 113. Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, *in Proceedings of Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* 156 (2010).

Note 114. *Id.*

Note 115. In the Georgian attacks, the attacks on government websites started about a month prior and gradually manifested over time. These attacks though were a combination of hacking and DDOS, initially they were low level defacing of websites and such. *See*, Danchev, note 107, *supra*.

Note 116. *Id.*

Note 117. U.N. Charter art. 2(4). *See also, Declaration On Principals Of International Law Concerning Friendly Relations And Cooperation Among States In Accordance With The Charter of the United Nations*, U.N.G.A. Res., 2625 (1970), A/8082 (1970). ("No State or group of States has the right to intervene, directly or indirectly,

for any reason whatever, in the internal or external affairs of any other State. Consequently, 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, are in violation of international law.")

Note 118. *Cf.*, International Law Commission, *Draft articles on Responsibility of States for Internationally Wrongful Acts*, art. 11 (2001). ("Conduct which is not attributable to a State under the preceding articles shall nevertheless be considered an act of that State under international law if and to the extent that the State acknowledges and adopts the conduct in question as its own.")

Note 119. International Telecommunication Union, *Key ICT Indicators For Developed and Developing Countrries And The World (Totals and Penetration Rates)* (2011), http://www.itu.int/ITU-D/ict/statistics/at_glance/ KeyTelecom.html.

Note 120. *Id*.

Note 121. U.N. Security Council Res. 1113 (2011), S/RES/1113 (2011), (stating that "[c]yber warfare is the use of computers or digital means by a government or with explicit knowledge of or approval of that government against another state, or private property within another state including:

-Intentional access, interception of data or damage to digital and digitally controlled infrastructure.

-Production and distribution of devices which can be used to subvert domestic activity.")