

JOURNAL OF LAW & CYBER WARFARE

ARTICLES

Mitigating Moral Hazard in Cyber-Risk Insurance

By Liam M.D. Bailey

The Deregulation and Swarming of Cyberwarfare:

The Need for and Limitations of Law in Enabling Aggressive
'Hacking-back' and Pre-Emption

By Dr. Mils Hills

Legal Considerations on Cyber-Weapons and Their Definition

By Stefano Mele

Internet Communication Blackout: Attack Under Non-International
Armed Conflict?

By Cassandra Mix

Bitcoin Laundromats for Dirty Money: The Bank Secrecy Act's (BSA)
Inadequacies in Regulating and Enforcing Money Laundering Laws over
Virtual Currencies and the Internet

By Sheng Zhou

Volume 3 | Spring 2014 | Issue 1

(c) 2013 – 2014. Journal of Law & Cyber Warfare.

All Rights Reserved.

www.jlcw.org

EDITORIAL BOARD

EXECUTIVE EDITORS

Editor-in-Chief

Daniel B. Garrie, Esq,

Executive Editor

Siddartha Rao, Esq.

Research Editor

Radhika Tiwari

INDUSTRY ADVISORS

Alan Roper	Jonathan Turner
Cedric Leighton	Joseph V. DeMarco
Christopher Burgess	Joseph Weiss
Dick Crowell	Larry Ponemon
Eric Jensen	Michael Schmitt
Gus Dimitrelos	Noah Bledstein
Jack Dever	Richard Borden
James Christiansen	Russell Walker
Jeff Bardin	Uma Chandrashekhhar
Jeremy Kroll	Vincent Scott
John Dever	William Spernow

MEMBERS

Kim Kopoff
Candice Lang
Sarah E. Haines
Stephen Williams
Valerie Strumwasser
Margaret Mak
Salvatore Scibetta

Internet Communication Blackout: Attack Under Non-International Armed Conflict?

By Cassandra Mix¹

Abstract:

The internet has become both a significant tool and vulnerability in most States' national security stratagem. Control of the internet could easily become a real part of modern armed conflict in the upcoming years. This was exemplified by Egypt's decision to cut off internet access within its borders during its January 2011 uprising. This paper will use the experience in Egypt as a case study, and argue that even if the violence of the protests had risen to the level of armed conflict, it is unlikely the governmental actions taken by Egypt would be classified as an attack under the law of armed conflict.

I. INTRODUCTION

In January 2011, the people of Egypt took to the streets seeking social reform.² On January 25th, protests began. The countrywide protest was organized primarily through the use of social media sites like Facebook and

¹ The Author is a recent graduate from J. Reuben Clark Law School - Brigham Young University. The Author would like to thank her parents for their love and support, and Professor Eric Jensen for all his help, guidance, and encouragement.

² Serajul I. Bhuiyan, *Social Media and Its Effectiveness in the Political Reform Movement in Egypt*, MIDDLE EAST MEDIA EDUCATOR, 1(1), 14-20, 15 (2011), available at <http://ro.uow.edu.au/meme/vol1/iss1/3>.

Twitter.³ The “Day of Rage,” as it is known, began as a peaceful gathering of citizens across the country of Egypt, but soon became violent.⁴ The first deaths on both sides occurred on that day,⁵ and the death count continued to rise the following day.⁶

Due to the wide usage of social media sites for organizational and communicational purposes the government of Egypt made the decision to shut down access to these sites on January 27th.⁷ The next day, the government limited public internet access.⁸ The same day troops were ordered into the streets, but they did not interact with the protestors or police.⁹ The announcement that President Mubarak was dismissing top officials in the government had no effect on the protestors.¹⁰

The internet was partially restored on February 2nd after 5 days of the government imposed blackout.¹¹ The protests continued. After 18 days of protests, on February 11th, President Mubarak resigned and governmental control of Egypt was turned over to the army.¹² At the end of the protests the final death count numbered in the hundreds.¹³

It seems clear that the use of social media significantly facilitated not only the organization of the

³ Al Jazeera & Agencies, *Timeline: Egypt's revolution*, AL JAZEERA, Feb 14, 2011, <http://english.aljazeera.net/news/middleeast/2011/01/201112515334871490.html>.

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Id.*

¹² *Id.*

¹³ *Id.*

protest but also shaped the way the events were shared with the world. Social media sites allow for almost instantaneous free interchange of ideas and information. This is only one of the reasons that these sites are used to organize movements all over the world. One activist in Cairo was quoted as saying, “We use Facebook to schedule the protests, Twitter to coordinate, and YouTube to tell the world.”¹⁴

Internet use is becoming increasingly integrated into all that we do. “From 2000 to 2010, global internet usage increased from 360 million to over 2 billion people.”¹⁵ People use the internet to communicate with each other through such things as VoIP, emails, and video conferencing. Even the very nature of how people fight wars has become dependent on the use of the internet.¹⁶ The internet allows almost instant communication, facilitating movement of troops and coordination of operations around the world. It also increases the vulnerabilities of critical infrastructure, such as water treatment plants and power grids.¹⁷

Attempts have been made and are being made to apply the law of armed conflict to cyber warfare.¹⁸ In

¹⁴ See Bhuiyan, *supra* note 2, at 16.

¹⁵ DEPARTMENT OF DEFENSE, DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 1 (2011), <http://www.defense.gov/news/d20110714cyber.pdf>.

¹⁶ *Id.*

¹⁷ Staff Writer, *Power Plants Vulnerable to Cyber Attack*, SAFETYISSUES.COM, Sept. 2007, <http://www.safetyissues.com/magazine/2007/09/aa0675.ph> p.

¹⁸ See INTERNATIONAL GROUP OF EXPERTS, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed.) (2013), *available at* <http://www.ccdcoe.org/249.html>; REX HUGHES, TOWARDS A GLOBAL REGIME FOR CYBER WARFARE (2009),

some instances this has been successful; in other instances application has just created more questions. For example, one can successfully apply the principle of distinction, prohibiting “attacks that cannot reasonably be limited to a specific military objective and which are indiscriminate or haphazard in their inclusion of civilian targets,” to the cyber world.¹⁹ This is relatively straightforward. Attacks must be specifically targeted at military objectives and limit the collateral damage on civilian targets. However, application of this principle creates confusion when determining the level of collateral damage assessment required before an attack is made in cyberspace to keep the operation in compliance with the law of armed conflict.²⁰ Much progress needs to be made in this area of law.

This transition into the digital age raises many questions about how we use the internet. The legalities of internet use not only affect how we can use the internet as individuals but also have implications for states. The events of the January 2011 uprising in Egypt raise questions about the legalities of state use and regulation of the internet. The use of the internet has become a tool in most militaries’ arsenals. Attempts to block the internet could easily become a real part of modern warfare in the

http://www.ccdcoe.org/publications/virtualbattlefield/07_HUGHES%20Cyber%20Regime.pdf (discussing the need for a global application of the Law of Armed Conflict to cyber warfare); Jeff Schogol, *Official: No options ‘off the table’ for U.S. response to cyber attacks*, STARS AND STRIPES (May 8, 2009), <http://www.stripes.com/article.asp?section=104&article=62555> (Air Force Gen. Kevin P. Chilton has said that “[t]he Law of Armed Conflict will apply to this domain.”).

¹⁹ James A. Lewis, *A Note on the Laws of War in Cyberspace*, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, 1 (2010), http://csis.org/files/publication/100425_Laws%20of%20War%20Applicable%20to%20Cyber%20Conflict.pdf.

²⁰ *Id.* at 3.

upcoming years. Understanding the legalities of operations like this one will be vital to functioning within the law of armed conflict.

This concern over the internet and its connection to armed conflict is illustrated by the experience in Egypt described above. President Mubarak impacted internet connectivity within Egypt to preserve national security in the face of potential armed conflict. While armed conflict never erupted in Egypt, it certainly could have as it did in other states involved in the Arab Spring. Therefore, it is worth considering how President Mubarak's blackout of the internet would have been viewed if the laws applicable during a non-international armed conflict would have applied. More specifically, would such actions have been classified as an "attack" in this hypothetical situation? To answer this question, this paper will use Egypt as a case study by building off the facts of the January 2011 uprising and assume that before Egypt made the decision to limit internet access the violence of the protests had risen to the level of armed conflict.²¹

In a situation like the proposed hypothetical, severing the internet within the borders of a country during a non-international armed conflict would not be considered an attack under *jus in bello* or law of armed conflict. This paper will address the legal reasoning behind this conclusion. Section II will discuss the type of law that is to be applied to the situation. Section III defines an "attack" under applicable laws and presents a proper methodology

²¹ See generally Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 2-3, Aug. 12, 1949, available at <http://www.icrc.org/ihl.nsf/WebList?ReadForm&id=365&t=com> (articles 2 and 3, which discuss what triggers application (armed conflict), are common to all the Geneva Conventions and so the commentary for these articles is the same for all the conventions).

for applying this definition in cyber warfare. Section IV will apply that methodology to the hypothetical armed conflict in Egypt and explain why the actions taken by Mubarak's government would not be considered an attack.

II. LEGAL PARADIGM: TYPE OF LAW

The type of law that is applied in any armed conflict depends on the classification of the conflict. Current bifurcation of the law of war into international armed conflict (IAC) and non-international armed conflict (NIAC) was set forth in the Geneva Conventions of 1949.²² The classification of a conflict is extremely important in discerning the applicable law. The full body of the law of armed conflict is applicable in an international armed conflict while only select parts, such as Common Article 3 of the Geneva Conventions, are applicable in a non-international armed conflict.

Prior to 1949, there was no bifurcation of the law of armed conflict.²³ The law at that time was designed to only apply to international conflicts.²⁴ International conflicts then were basically war between two states. Internal conflicts, more commonly known as civil wars, were not subject to any international regulation.²⁵ Until 1949, states refused to draft any such regulations because they felt that "insurrection and rebellion were a purely domestic matter"

²² Emily Crawford, *Unequal Before the Law: The Case for the Elimination of the Distinction between International and Non-International Armed Conflict*, 20 LEIDEN J. OF INT'L LAW 441-465, 6 (2007), available at <http://ssrn.com/abstract=1810175>.

²³ ROBERT KOLB & RICHARD HYDE, AN INTRODUCTION TO THE INTERNATIONAL LAW OF ARMED CONFLICTS 65 (2008).

²⁴ *Id.*

²⁵ *Id.*

that should have no external regulations.²⁶

In the wake of the Spanish Civil War and World War II, it was clear that there was a “stark absence of protections for civilians in wartime.”²⁷ While most states did not want to give up any sovereignty, they realized after these wars that there was a need for some minimal protections for civilians during internal conflicts.²⁸ Common Article 3 of the 1949 Geneva Conventions was the solution.²⁹ It laid out the fundamental principles that must guide all non-international armed conflicts.³⁰

In a nutshell, common Article 3 requires humane treatment of persons not taking direct part in hostilities and those placed *hors de combat*,³¹ “[doing] little to regulate combat or protect civilians against the effects of hostilities.”³² It only applies to hostilities that reach the level of armed conflict.³³ It is important to note that originally when common Article 3 applied no other part of the Conventions applied.³⁴ This means that provisions like Prisoner of War protections do not apply to a non-international armed conflict because they are contained in areas other than common Article 3.³⁵ Common article 3 is now considered to apply to all armed conflicts as a matter

²⁶ *Id.*

²⁷ GARY D. SOLIS, *THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR* 97 (2010).

²⁸ Crawford, *supra* note 22, at 8.

²⁹ Crawford, *supra* note 22, at 8.

³⁰ *Id.* at 9.

³¹ Solis, *supra* note 27, at 98.

³² James G. Stewart, *Towards a single definition of armed conflict in international humanitarian law: A critique of internationalized armed conflict*, 85, 850 *IRRC* 313, 320 (2003), available at http://www.icrc.org/eng/assets/files/other/irrc_850_stewart.pdf.

³³ *Id.* at 318.

³⁴ Solis, *supra* note 27, at 99.

³⁵ *Id.*

of customary international law.³⁶

Over the decades following the Geneva Conventions of 1949, the nature of armed conflicts continued to undergo significant changes.³⁷ The frequency and intensity of armed conflicts increased, most of these being of a non-international character.³⁸ Most casualties during non-international armed conflicts were consistently civilians.³⁹ States were beginning to realize that “[t]he *de minimus* rules provided for in Common Article 3 were insufficient to the task of regulating such widespread and brutal conflict.”⁴⁰ Modification of the current law was needed.⁴¹

In 1977, Additional Protocol I (API)⁴² and II (APII)⁴³ of the Geneva Conventions were adopted. These protocols assisted in clarifying the classification of armed conflicts, but still left some major issues as to what laws

³⁶ Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 14 (June 27), *available at*

<http://www.icj-cij.org/docket/index.php?p1=3&p2=3&code=nus&case=70&k=66&p3=0>.

³⁷ Crawford, *supra* note 22.

³⁸ Solis, *supra* note 27, at 99.

³⁹ Crawford, *supra* note 22.

⁴⁰ *Id.* at 11.

⁴¹ Solis, *supra* note 27 at 120.

⁴² Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3, *available at* <http://treaties.un.org/doc/Publication/UNTS/Volume%201125/volume-1125-I-17512-English.pdf> [hereinafter API].

⁴³ Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), June 8, 1977, 1125 U.N.T.S. 609, *available at* <http://treaties.un.org/doc/Publication/UNTS/Volume%201125/volume-1125-I-17513-English.pdf> [hereinafter APII].

applied in a non-international armed conflict.⁴⁴ For example, APII only applies to a subset of non-international armed conflicts. Instead of applying to “armed conflicts not of an international character,” APII limits its application to:

“[A]ll armed conflicts which are not covered by Article 1 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) and which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol.”⁴⁵

This means that, in contrast to common Article 3, APII does not apply to situations like the warring of two dissident groups.⁴⁶ The requirement of exercising control over part of the territory also excludes the “activities of the Irish Republican Army in Ireland, the Basque Separatists in Spain, and the Shining Path in Peru.”⁴⁷ The ICRC has pointed out that the criteria set forth in APII makes it impossible to apply APII in all cases of non-international armed conflict.⁴⁸

Throughout this period of change, situations arose

⁴⁴ Crawford, *supra* note 22, at 16.

⁴⁵ APII, *supra* note 43.

⁴⁶ Stewart, *supra* note 32, at 319.

⁴⁷ Solis, *supra* note 27, at 131.

⁴⁸ Solis, *supra* note 27, at 131.

that didn't fit neatly into the bifurcated system. One example would be internationalized armed conflicts. "Internationalized" armed conflicts are conflicts that do not rise to the level of an international conflict but transcend the category of non-international conflict.⁴⁹ An illustration of this type of conflict would be situations that began as a non-international armed conflict but because of third state intervention fall out of this classification.⁵⁰ This mixed conflict category began to blur the lines between international armed conflict and non-international armed conflict.⁵¹

The armed conflict in Lebanon provides a historic example of a mixed conflict category.⁵² Since 1975, Lebanon has suffered from armed conflict between warring groups within its borders.⁵³ In March of 1978, Israeli forces intervened in the southern part of Lebanon followed by a period of occupation.⁵⁴ This action by Israel moved Lebanon's conflict into something more than a non-international armed conflict but less than an international armed conflict (because Israel was not fighting against the Lebanese government).

This blurring is highlighted in the development of customary law. The United Nations General Assembly Resolution 2444, dated 19 December 1986, notes "the necessity of applying basic humanitarian principles in all

⁴⁹ Crawford *supra* note 22, at 16.

⁵⁰ *Id.*

⁵¹ *Id.* at 18.

⁵² Hans-Peter Gasser, *Internationalized Non-International Armed Conflict: Case Studies of Afghanistan, Kampuchea, and Lebanon*, 33 AM. U. L. REV. 145, 156 (1983), available at <http://www.wcl.american.edu/journal/lawrev/33/gasser.pdf>.

⁵³ *Id.*

⁵⁴ *Id.* at 157.

armed conflicts.”⁵⁵ Even though the UN resolution itself is non-binding, that same year the International Court of Justice (ICJ) recognized that certain elements of the law of armed conflict are applicable regardless of the type of armed conflict.⁵⁶ Specifically, it noted that the principles in Common Article 3 are applicable in “the event of international armed conflicts, . . . in addition to the more elaborate rules which are also to apply to international conflicts; and they are rules which, in the Court's opinion, reflect what the Court in 1949 called ‘elementary considerations of humanity’.”⁵⁷

In 1995, the International Criminal Tribunal of Yugoslavia (ICTY) recognized this major change, writing, “the aforementioned distinction [between international armed conflict and non-international armed conflict] has gradually become more and more blurred, and international legal rules have increasingly emerged or have been agreed upon to regulate internal armed conflict.”⁵⁸ In its view, the need to protect civilians shouldn't differ between conflict types.

“Why protect civilians from belligerent violence, or ban rape, torture or the wanton destruction of hospitals, churches, museums or private property, as well as proscribe weapons causing unnecessary suffering when two sovereign States are engaged in war, and yet refrain from

⁵⁵ Respect for Human Rights in Armed Conflicts, G.A. Res. 2444 (XXIII), (Dec. 19, 1968), available at http://www.un.org/depts/dhl/resguide/r23_en.shtml (follow “A/RES/2444(XXIII)” hyperlink).

⁵⁶ Military and Paramilitary Activities, *supra* note 36.

⁵⁷ *Id.*

⁵⁸ Prosecutor v. Tadic, Case No. IT-94-1-T, Decision on Interlocutory Appeal on Jurisdiction, ¶ 97 (Oct. 2, 1995) available at <http://www.icty.org/x/cases/tadic/acdec/en/51002.htm>.

enacting the same bans or providing the same protection when armed violence has erupted ‘only’ within the territory of a sovereign State?”⁵⁹

While the application of international armed conflict principles to non-international armed conflict situations was a big step towards eliminating the separation between the two, it does not equate to equal coverage. The ICTY clarified the application of these rules was limited to only a certain “number of rules and principles.”⁶⁰ Additionally, it stated it is the “general essence of those rules, and not the detailed regulation they may contain” that pertain to non-international armed conflicts.⁶¹

State practice also reflects this movement of using international armed conflict principles in non-international armed conflict situations.⁶² A recent study by the International Committee of the Red Cross (ICRC) of customary laws in international armed conflict and non-international armed conflict found that many areas of law in international armed conflict have crossed over into non-international armed conflict situations.⁶³ There have been many criticisms of the study. One critique involves the extensive use of military manuals as evidence of state

⁵⁹ *Id.*

⁶⁰ *Id.* at ¶ 126.

⁶¹ *Id.*

⁶² Crawford, *supra* note 22, at 26.

⁶³ Jean-Marie Henckaerts, *Study on customary international humanitarian law: A contribution to the understanding and respect for the rule of law in armed conflict*, 87, 857 IRRC 175, 198 (Mar. 2005), available at

http://www.icrc.org/eng/assets/files/other/irrc_857_henckaerts.pdf

(there have been many criticisms of the study but the overall trend in state practice of the application of IAC principles in NIAC situations still holds true).

practice.⁶⁴ Military manuals are a combination of law and policy.⁶⁵ In addition, the manuals do not always reflect actual implementation.⁶⁶ Another area that has received censure is the inconsistent application of the term “virtually uniform”⁶⁷ in deciding if state practice is customary law.⁶⁸ While there have been many criticisms, the results of the study continue to provide informative assistance into the migration of international armed conflict principles to non-international armed conflict.⁶⁹

One example of how principles of international armed conflict have migrated to non-international armed conflict is use of a flag of truce. This rule comes from the Hague Convention of 1907 article 32.⁷⁰ A fighter bearing a white flag of truce is immune from attack as long as he does not take part in hostilities.⁷¹ While originally only applicable in international armed conflict, through extensive state practice, it has come to be considered customary law and applicable in non-international armed

⁶⁴ John B. Bellinger, III & William J. Haynes II, *A US government response to the International Committee of the Red Cross study Customary International Humanitarian Law*, 89, 866 IRRC 443, 445 (2007) available at http://www.icrc.org/eng/assets/files/other/irrc_866_bellinger.pdf.

⁶⁵ *Id.*

⁶⁶ *Id.*

⁶⁷ See WILLIAM H. BOOTHBY, *WEAPONS AND THE LAW OF ARMED CONFLICT* 37 (2009) (state practice has to be virtually uniform, extensive and representative to establish a rule of customary international law).

⁶⁸ *Id.*

⁶⁹ Crawford, *supra* note 22, at 32.

⁷⁰ International Conferences (The Hague), Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land art. 32, 18 October 1907, available at <http://www.unhcr.org/refworld/docid/4374cae64.html>.

⁷¹ *Id.*

conflict situations as well.⁷²

Understanding the migration of international armed conflict principles into non-international armed conflict situations is vital to applying appropriate laws. Knowing what portions of targeting law and detention law have now migrated into non-international armed conflict allows states to more fully apply the law. However, confusion remains in many cases and allows states to manipulate the applicability of the law to suit their needs. An illustrative example of this situation is the United States' War on Terror.

After the attacks of 9/11 the United States declared a War on Terror.⁷³ This War on Terror is unlike any war before. It involves a state fighting against a non-state actor on an international scale. Such a conflict does not fit neatly into any specific classification. Without a specific classification, it is difficult to determine the applicable laws in situations like the treatment of detainees. In a memorandum issued by Pres. George W. Bush in 2002, the U.S. determined that "none of the provisions of Geneva apply to [the] conflict with al Qaeda in Afghanistan or elsewhere throughout the world because...al Qaeda is not a

⁷² MICHAEL N. SCHMITT ET AL., THE MANUAL ON THE LAW OF NON-INTERNATIONAL ARMED CONFLICT WITH COMMENTARY § 2.3.3.1 (2006), *available at* <http://www.iihl.org/iihl/Documents/The%20Manual%20on%20the%20Law%20of%20NIAC.pdf>.

⁷³ George W. Bush, President, U.S., Address to a Joint Session of Congress and the American People (September 20, 2001) (transcript available *at* <http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010920-8.html>).

High Contracting Party [to the Convention].”⁷⁴ This meant for the U.S. that the War on Terror was not an international armed conflict as defined by the Geneva Conventions. As a result, none of the provisions on the treatment of prisoners of war applied to the War on Terror.

In this same memorandum it was also argued that the War on Terror was not non-international armed conflict under common Article 3 because “the relevant conflicts are international in scope and common Article 3 applies only to ‘armed conflict not of an international character’.”⁷⁵ Therefore, the War on Terror was deemed to fall outside of the bifurcated classifications of the law of armed conflict and as a consequence none of the laws applied. Although the U.S. Supreme Court later declared that common Article 3 applied to the War on Terror,⁷⁶ there is still confusion about the required treatment of detainees under common Article 3.⁷⁷ The U.S. used this confusion to justify controversial interrogation techniques that arguably crossed the line of humane treatment.⁷⁸

The confusion concerning the applicable laws of armed conflicts in all varieties of conflict needs to be

⁷⁴ Memorandum from George W. Bush on Humane Treatment of al Qaeda and Taliban Detainees to The Vice President et al., 1 (February 7, 2002), available at http://www.aclu.org/files/assets/20100615_dos_release_1_doc_-_already_released.pdf.

⁷⁵ *Id.* at 2.

⁷⁶ See *Hamdan v. Rumsfeld et al.*, 548 U.S. 557, 631 (2006), available at http://www.law.yale.edu/Hamdan_v._Rumsfeld.pdf.

⁷⁷ TASK FORCE ON NATIONAL SECURITY AND THE RULE OF LAW, REAFFIRMING THE U.S. COMMITMENT TO COMMON ARTICLE 3 OF THE GENEVA CONVENTIONS: AN EXAMINATION OF THE ADVERSE IMPACT OF THE MILITARY COMMISSIONS ACT AND EXECUTIVE ORDER GOVERNING CIA INTERROGATIONS (2008), http://www.nycbar.org/pdf/report/GC_Report0702_all.pdf.

⁷⁸ *Id.* at 5.

eliminated. It is important for states to understand what law governs different levels of conflict so that they will not mistakenly violate the appropriate rules. In addition, states must be able to characterize operations under the correct context so as to correctly apply the law to their actions. The next section will help to clarify what laws apply to cyber warfare in non-international armed conflicts and lay out a framework for states to use.

III. "CYBER ATTACK"

The prior discussion of the applicability of International Armed Conflict rules to Non-International Armed Conflicts is important for this paper because the legality of Egypt's actions in shutting down the internet during the hypothetical armed conflict is dependent on the characterization of that action as an "attack," as that term is borrowed from the principles of International Armed Conflict. It is important to understand that if an action taken during an armed conflict would fall into the "attack" category, it will affect the legality of the action and place limits on the action itself. More specifically, if the actions taken by Egypt to shut down the internet amount to an attack, then Egypt's actions during its armed conflict with the protestors are governed by additional principles that might limit, as a matter of law, the actions that Egypt can take. However, there is no definition of the word "attack" in common Article 3 that would provide a method for interpreting Egypt's actions. Because of this lack of clarity, most scholars look to the definition of "attack" under international armed conflict.

This section will expand what an "attack" means in the context of cyber warfare beginning with what constitutes an attack in non-international armed conflict. Following that, it will determine what the core element of an attack is. Next, it will look at what test should be used

to classify something as an attack. Finally, some examples will be given of applying the chosen approach to cyber operations.

API defines “attacks” as “acts of violence against the adversary, whether in offence or defence.”⁷⁹ Using the term “violence” seems significant when considering the scope of actions that would fit within the definition of attack. While this protocol is only applicable in international armed conflict situations, the ICRC commentary to APII records that the definitions in API were to apply to both protocols.

“ Definition of attack ’

Protocol I defines attacks. This term has the same meaning in Protocol II. Article 49 '(Definitions of attacks and scope of application), ' paragraph 1, of Protocol I, reads as follows "Attacks" means acts of violence against the adversary, whether in offence or defence."⁸⁰

Attack is also defined in The Manual on the Law of Non International Armed Conflict (NIAC Manual). The NIAC Manual was written by three prominent LOAC scholars who were writing under the auspices of the San Remo Institute and for the purpose of establishing what laws apply in a non-international armed conflict. In defining “attacks,” they followed the language of API. They noted in their commentary that this is where they derived their definition because the drafters of API and APII agreed that the two protocols would have the same

⁷⁹ API, *supra* note 42, at art. 49.

⁸⁰ Commentary to PROTOCOL ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, AND RELATING TO THE PROTECTION OF VICTIMS OF NON-INTERNATIONAL ARMED CONFLICTS (PROTOCOL II), [8 June 1977] at para. 4783. Available at <http://www.icrc.org/ihl.nsf/COM/475-760019?OpenDocument>.

definition of attack.⁸¹

Though the U.S. is not a Party to API, it has declared many parts to be customary law,⁸² and has not specifically objected to the definition of attack. Many of the articles use the word “attack”, and apply it as defined by API.⁸³ In view of that, this definition of “attack” could be viewed as customary law. Accordingly, it is proper to use this definition in non-international armed conflicts.

With the migration of “attack” from international armed conflict to non-international armed conflict comes the migration of other principles, such as military objective, distinction and proportionality, associated with attacks. These additional principles migrate because they are linked to the application of attack and the law of non-international armed conflict does not have any corresponding principles.⁸⁴ They are necessary for states to plan and carry out attacks during non-international armed conflicts. This is significant because it once again blurs the lines between the laws of international and non-international armed conflicts.⁸⁵ APII part IV talks about targets that are protected from attack, however, it does not include any principles for use in targeting. Therefore, API articles 51, 52, and 57 must be used to define these principles.⁸⁶

The principle of distinction requires differentiating between civilian persons and objects and military persons

⁸¹ SCHMITT ET AL., *supra* note 72, at § 1.1.6.

⁸² Paul A. Walker, *Rethinking Computer Network ‘Attack’: Implications for Law and U.S. Doctrine*, J. OF NAT’L SEC. L. & POL’Y, FORTHCOMING 3 (Mar. 12, 2010), available at <http://ssrn.com/abstract=1586504>.

⁸³ *Id.*

⁸⁴ Kolb & Hyde, *supra* note 23, at 257.

⁸⁵ *Id.* at 259; see also Henckaerts, *supra* note 63.

⁸⁶ See SCHMITT ET AL., *supra* note 72.

and objects when attacking the enemy.⁸⁷ This principle is stated in API art 48.

“Article 48. BASIC RULE. In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.”⁸⁸

It seeks to protect those civilians who are not directly participating in hostilities by protecting them from its effects.⁸⁹

The principle distinction is important in a non-international armed conflict because it prohibits governments from retaliating against the civilian population as a whole for the acts of one group. This principle makes it illegal for states to bomb a large portion of a city full of civilians because there are a handful of fighters located there. The government must target the fighters specifically and limit the damage to civilian life and property.

Military objects are “those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.”⁹⁰ Objects are limited to those that would *effectively* make a military contribution. This would include weapons, bridges that are used by armed forces and buildings that hold

⁸⁷ *Id.* at § 1.2.2.

⁸⁸ API, *supra* note 42, at art. 48.

⁸⁹ SCHMITT ET AL., *supra* note 72, at § 1.2.2.1.

⁹⁰ API, *supra* note 42, at art. 52.

military meetings and personnel.⁹¹ Using an example from the scenario, the server hosting the social media site used by the protestors for communication would be a military objective because it allows communication between protestors and its destruction offers a definite military advantage.

The rule of proportionality requires a party to “[r]efrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.”⁹² This means that the damage and loss of civilian lives cannot be excessive when weighed against the value of the target.

In a non-international armed conflict, proportionality would mean that “[a]ll attacks must also be conducted bearing in mind the principle of proportionality.”⁹³ The test would be to weigh the value of the military advantage of a target against “the expected harm to civilians and civilian objects.”⁹⁴ If the harm is *excessive* in comparison then the attack would be forbidden. For instance, when deciding whether or not to attack a national power grid, the military benefit would be weighed against the possible damage that might result in loss of life or property.⁹⁵ In this example it would be necessary to consider the effects on places such as hospitals that might not have sufficient backup generators to maintain operation during a power outage.⁹⁶

The migration of “attack” from international armed

⁹¹ SCHMITT ET AL., *supra* note 72, at § 1.1.4.3.

⁹² API, *supra* note 41 42, at art. 57(2)(a)(iii).

⁹³ SCHMITT ET AL., *supra* note 72, at § 2.1.1.4.4.

⁹⁴ *Id.* at § 2.1.1.4.5.

⁹⁵ *Id.* at § 2.1.1.4.9.

⁹⁶ *Id.*

conflict to non-international armed conflict produces large shifts in the law of armed conflict. The movement has blurred the lines between the two types of armed conflict. These lines will continue to blur as the nature of armed conflicts continues to change.

In looking at the elements of attack, the essence seems to be “acts of violence.” Violence is characterized as “intense...often destructive action or force.”⁹⁷ Pulling an example from the kinetic world, an act of violence would be launching a rocket-propelled grenade. The result of pulling the trigger leads to a destructive and potentially deadly grenade explosion. Applying this definition to the cyber world requires a more subtle approach. Pushing a button (the action), which sends a virus like Stuxnet, could have violent results. The Stuxnet infiltration of Iranian computers caused actual damage to physical property.⁹⁸ Nonetheless not all viruses cause physical damage. Some cyber operations are as simple as a Distributed Denial of Service (DDoS) which shuts down a website by overwhelming it with requests, but causes no physical damage.⁹⁹

In deciding whether or not an action would be considered an attack, there must be some test to guide the classification. Paul Walker proposes that an effects or consequence test would be the most appropriate test to use for this determination.¹⁰⁰ In reaching this conclusion, he

⁹⁷ Dictionary: Violence, <http://www.merriam-webster.com/dictionary/violence> (last visited Feb. 7, 2014).

⁹⁸ *Iran admits Stuxnet's damage*, HOMELAND SECURITY NEWS WIRE, Apr. 18 2011, <http://www.homelandsecuritynewswire.com/iran-admits-stuxnets-damage>.

⁹⁹ Dictionary: DDoS, <http://dictionary.reference.com/browse/DDoS> (last visited Feb. 7, 2014) (a DDoS (abbreviation for ‘distributed denial of service’) is when numerous requests are sent to a computer or network causing it to become overloaded and shut down).

¹⁰⁰ Walker, *supra* note 82, at 21.

discusses three methods: “actor-based,” “results-based” and “consequence-based.” Walker analyzes each method’s effectiveness in classifying cyber operations as attacks.

The first method discussed was the “actor-based” methodology.¹⁰¹ This test defines “any action occurring between two forces engaged in combat” as an attack.¹⁰² This rule is based on the Commentary of article 49 of API.¹⁰³ Under this method, every action taken by a military force against another force would be considered an attack whether or not the action was violent in nature.¹⁰⁴ For instance, infiltrating an enemy’s network system to gather data would be considered an attack. Even if the intrusion was not violent and no damage resulted, it was an action taken against an opposing force.

The over-inclusiveness of this test is a serious stumbling block. This test would count actions such as espionage and psychological operations as attacks.¹⁰⁵ Most states would not accept this test because of the limitations it places on existing state practice.¹⁰⁶ Examples of state practice that would be affected include the “long-held notions regarding the distinction between espionage and attacks, especially where computers and computer networks are involved.”¹⁰⁷ Most states would not want to

¹⁰¹ *Id.* at 15.

¹⁰² *Id.* at 16.

¹⁰³ *Id.* at 15.

¹⁰⁴ *Id.* at 16.

¹⁰⁵ *Id.*

¹⁰⁶ *Id.* at 16; see also Paul Eckert & Phil Stewart, *Chinese entities world’s biggest economic spies: Pentagon*, REUTERS, May 19, 2012, available at <http://www.reuters.com/article/2012/05/19/us-usa-china-military-idUSBRE84I06X20120519> (there have been many recent incidents between the U.S. and China about the use of economic cyber espionage in the past year, but neither the U.S. or China would consider this an attack).

¹⁰⁷ Walker, *supra* note 82, at 16.

place this practice in jeopardy.¹⁰⁸

The “results-based” methodology looks at attacks from the opposite view. It asks if the operation accomplishes the same outcome that could have been reached with “bombs or bullets.”¹⁰⁹ This test also doesn’t limit its application to operations with violent results.¹¹⁰ There is no room for distinction between kinetic and cyber actions. For example, a DDoS action that does not result in any physical damage but shuts down the computer system would be classified as an attack under this approach.¹¹¹ The cyber result of shutting down the computer system would be the same if you used cyber or kinetic means.

This test also does not take into account the possibility that an action might have been achieved without using “bombs or bullets.”¹¹² For instance, an air traffic control tower could be shut down due to the actions of an undercover agent just as effectively as using a bomb but without all the resulting property damage.¹¹³ Classifying attacks using this method would severely limit the aims of humanitarian laws by not allowing non-violent actions to be used in place of destructive methods.¹¹⁴

The “consequence-based” method or effects test looks at the consequences of an action.¹¹⁵ If the effects of an action are violent then it is classified as an attack.¹¹⁶ The classification of the action is based on the potential violent consequences which must be reasonably

¹⁰⁸ *Id.*

¹⁰⁹ *Id.* at 17.

¹¹⁰ *Id.* at 18.

¹¹¹ *Id.*

¹¹² *Id.* at 20.

¹¹³ *Id.*

¹¹⁴ *Id.* at 19.

¹¹⁵ *Id.* at 20–21.

¹¹⁶ *Id.* at 20.

foreseeable.¹¹⁷ Reasonable foreseeability implies that “constant care” be taken in all military operations to spare the civilian population and objects.¹¹⁸ In cyber operations, for example, it would mean things such as keeping a current understanding of the targeted network in anticipation of potential overflow effects onto civilian objects from an operation.

It is also necessary to define what would be a violent consequence. Without a method for determining if a consequence is violent it cannot be determined if an act was an attack as understood under API. Walker defines violent consequences as those causing injury or death, physical damage or destruction.¹¹⁹ Mere inconvenience or deterioration in quality of life does not rise to the level of violence.¹²⁰ This method seems to be the most widely-accepted test used by scholars in classifying cyber actions¹²¹ and will be the test used in this paper.

Taking a look at some examples of violent and non-violent consequences, it becomes easier to recognize the distinction. In India and Bangladesh, there has been an

¹¹⁷ 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, 915-16 (1999), available at <http://ssrn.com/abstract=1603800>.

¹¹⁸ API, *supra* note 42, at art. 57.

¹¹⁹ Walker, *supra* note 82, at 24.

¹²⁰ *Id.*

¹²¹ See Michael N. Schmitt, *Wired Warfare: Computer Network Attack and Jus in Bello*, 84, 846 IRRC 365 (2002), available at http://www.icrc.org/eng/assets/files/other/365_400_schmitt.pdf; Walker, *supra* note 82, at 16 (Many expert scholars have used the “effects-based” methodology, and it has been applied in both *jus ad bellum* and *jus in bello*).

exchange of cyber operations defacing various websites.¹²² Most forms of defacement involve replacing the main webpage of a site with some type of propaganda message or image.¹²³ In the example of India and Bangladesh, Bangladeshi hackers have replaced the web content with “Bangladeshi flags and images of people tortured by Indian border guards.”¹²⁴ Even though the websites and their content are usually unavailable for a period of time there is no resulting physical damage or destruction of property.¹²⁵ The effects of this operation would not be considered violent consequences, thus, this would not be an attack.

In August 2012, Aramco – a state-owned oil company – was the target of a cyber-operation.¹²⁶ The state attributed this act to unnamed “foreign countries.”¹²⁷ It came in the form of a computer virus introduced to the company’s computer network through an e-mail.¹²⁸ The virus was reported to have “destroyed data on servers and erased hard-drives on individual computers.”¹²⁹ While

¹²² *India/Bangladesh cyberwar moves to new level*, INFOSECURITY, Mar. 6, 2012, <http://www.infosecurity-magazine.com/view/24328/indiabangladesh-cyberwar-moves-to-a-new-level/>.

¹²³ While many of these operations are undertaken by civilians, the principles are equally applicable to state and non-state actors.

¹²⁴ Sebastian Murdoch-Gibson, *Bangladesh-India cyber war rages on*, THE ARGUS, Mar. 12, 2012, <http://www.theargus.ca/articles/news/2012/03/bangladesh-india-cyber-war-rages-on>.

¹²⁵ *Id.*

¹²⁶ Wael Mahdi, *Saudi Arabia Says Aramco Cyberattack Came From Foreign States*, BLOOMBERG NEWS, Dec. 9, 2012, <http://www.bloomberg.com/news/2012-12-09/saudi-arabia-says-aramco-cyberattack-came-from-foreign-states.html>.

¹²⁷ *Id.*

¹²⁸ *Id.*

¹²⁹ *Id.*

there was no disruption of oil output,¹³⁰ the destruction of data would be considered physical damage to property. This result would fall into the category of a violent consequence, making this operation an attack.

It is also important to note that the object used to attack does not have to be classified as a weapon. Pulling from an example in the kinetic world, during the Persian Gulf War, Iraqi soldiers were buried alive using a plow attached to the front of a tank.¹³¹ The act of burying the soldiers alive is an attack, but the instrument used to carry out this attack, the plow, is not considered a weapon. The same principle applies in the cyber world. The instrument used to carry out an operation may not be categorized as a weapon, but the action could still be an attack. Conversely, just because a tool is called a weapon does not mean that every time it is used that action is an attack. In the cyber world a malicious piece of software, which is classified as a cyber-weapon,¹³² could be used in an operation without that operation being considered an attack. For instance, a cyber-weapon could be used to map a network in anticipation of a future attack without executing any actual attack, despite its capacity for such an action.

The “consequence-based” (effects test) is the most appropriate test to use. This methodology of looking at the effects of an action to determine its classification is easy to apply, making it an effective test for commanders and legal

¹³⁰ *Id.*

¹³¹ Eric Schmitt, *U.S. Army Buried Iraqi Soldiers Alive in Gulf War*, N.Y. TIMES, Sept. 15, 1991, <http://www.nytimes.com/1991/09/15/world/us-army-buried-iraqi-soldiers-alive-in-gulf-war.html?pagewanted=all&src=pm>.

¹³² Ellen Nakashima, *List of cyber-weapons developed by Pentagon to streamline computer warfare*, WASH. POST, May 31, 2011, http://articles.washingtonpost.com/2011-05-31/national/35264250_1_cyber-computer-warfare-stuxnet.

advisers to use. It does not have the over-inclusiveness problem of the “actor-based” methodology. It also gives the ability to distinguish between kinetic and cyber actions, which is not possible under the “results-based” method. Returning to the example of the Iranian Stuxnet virus, it’s now clear that that would qualify as an attack under the effects test because sending the virus resulted in physical damage to the property.¹³³ Conversely, the DDoS action that shuts down a website would not be an attack because there was no physical damage to the property even though in the past this would have only been possible through the use of “bombs or bullets.”

IV. APPLICATION TO HYPOTHETICAL

In applying this approach to the hypothetical, caution must be taken to remember that this is a *jus in bello* issue in a non-international armed conflict situation. In other words, in opposition to the actual facts of the uprising in Egypt where there was no armed conflict, the hypothetical assumes an existing armed conflict between the government of Egypt and various groups trying to overthrow that government. As discussed above, the law of armed conflict as applied to international armed conflicts has migrated over into non-international armed conflicts. Thus, the definition of attack from API applies in this situation. In this section, Walker’s effects test will be applied to the facts of the scenario. It will be shown that shutting down internet access is not an attack.

A. State Actors

¹³³ Jeremy Richmond, Note, *Evolving Battlefields: Does Stuxnet Demonstrate the Need for Modifications to the Law of Armed Conflict?*, 35 FORDHAM INT’L L.J. 842 (forthcoming Mar. 2012) (analyzing STUXNET as an *in bello* issue).

As a reminder, here are the basic facts of this hypothetical. The citizens of Egypt rose up in protest of the government. This protest became a non-international armed conflict. In an attempt to combat the use of the internet in organizing the protests, the Egyptian government severed internet access. This was done by calling each of the four ISPs and telling them to shut down access to the internet.¹³⁴ Each ISP pulled all Egyptian internet address from the global routing tables.¹³⁵ The four ISPs disconnected Egypt from the internet non-simultaneously within a period of about 13 minutes.¹³⁶ This blackout continued for 5 days.

When using the effects test to evaluate the government actions the first thing to look at is the results of the action. The effects are those which proximately result from the action on the ISP itself. Any reverberating effects must be “foreseeable in light of the information reasonably available to the attacker at the time.”¹³⁷ Severing the internet resulted in a loss of business for the ISPs and internet based companies, and no internet access to the citizens of Egypt. No internet meant that the citizens had no email, VoIP, or social media access and the protestors had no means of communication.

Any financial harm to the owners of the ISPs or other businesses is not property damage or destruction. At most it would be considered a deterioration in quality of

¹³⁴ Posting of Jim Cowie to Renesys blog, <http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml> (Jan. 27, 2011, 7:56 PM).

¹³⁵ *Id.*

¹³⁶ Antone Gonsalves, *Egypt Internet Shutdown Underscores Vulnerability*, INFORMATIONWEEK, Jan. 28, 2011, <http://www.informationweek.com/news/internet/policy/229200056>.

¹³⁷ SCHMITT ET AL., *supra* note 71 at § 2.1.1.4.9.

life for the business. Financial harm does not rise to the level of violent consequence. Therefore, this effect does not cause this action to be classified as an attack.¹³⁸

The blackout itself would not be considered an attack because there were no direct violent consequences. The loss of internet access did not inflict death, bodily harm, damage or destruction of property. The hurt felt was minimal. The citizens of Egypt were not able to access the internet and the protestors were not able to communicate using social media sites. This does not rise to the level of violent harm. Thus, this result would not classify this action as an attack.

When Egypt's government decided to black out the internet to disrupt the protestors, it did not use any form of kinetic force in order to interrupt internet communications. The government used its authority to order the ISPs to shut down services.¹³⁹ There was no resulting physical damage from the shutdown. Even under the very broadest reading of the term "violence", the government's process of cutting off Egyptians from the internet cannot be categorized as violent. The consequences of the method used by the government to limit internet access were also non-violent. Thus, the means used to limit internet access in this situation were not an attack. If the method used to shut down the internet had involved damage of property or

¹³⁸ John Markoff & Thom Shanker, *Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk*, N.Y. TIMES Aug 1, 2009,

<http://www.nytimes.com/2009/08/02/us/politics/02cyber.html> (Even though the effects of financial harm would not have been violent, the other possible ramifications of the action would play a role in the decision to use such methods. For example, in 2003 the U.S. government made plans to cyber-attack the Iraqi banking system. The goal was to freeze Saddam Hussein's assets. The plan was eventually rejected on the grounds that the potential effects of the cyber attack might have spilled over into Europe's banking systems).

¹³⁹ Gonsalves, *supra* note 136.

injury to persons then it would have produced violent consequences and been considered an attack.

It is also interesting to note that there has been no accusation from critics that Egypt's action was an attack. There has been much criticism from many sources but very few have called it an attack,¹⁴⁰ and none in reference to an attack as classified in regards to armed conflict.¹⁴¹ Criticisms seem to focus on the human rights aspect of the internet blackout. On the day the blackout began White House spokesman Robert Gibbs tweeted, "Govt must respect the rights of Egyptian people & turn on social networking and internet."¹⁴² That same day, D.C. based Center for Democracy and Technology President Leslie Harris said, "This action is inconsistent with all international human rights norms, and is unprecedented in internet history. Egypt's actions will only fuel unrest and make peaceful resolution of grievances far more difficult."¹⁴³ The lack of accusations of an attack may stem from the fact that there was no armed conflict in Egypt at the time. However, this as a whole seems to support the conclusion that this type of action would not be considered an attack.

¹⁴⁰ James Glanz, *How Mubarak shut down Egypt's internet*, THE AGE, Feb. 17, 2011 <http://www.theage.com.au/world/how-mubarak-shut-down-egypts-internet-20110216-1awjj.html> (using the term attack in the figurative, not the legal sense).

¹⁴¹ *Id.*

¹⁴² Mary Beth Sheridan, *U.S. warns against blocking social media, elevates Internet freedom policies*, WASH. POST, Jan. 28, 2011, <http://www.washingtonpost.com/wp-dyn/content/article/2011/01/28/AR2011012804554.html?sid=ST2011012806871>.

¹⁴³ Ryan Singel, *Egypt Shut Down Its Net With a Series of Phone Calls*, WIRED, Jan. 28, 2011, <http://www.wired.com/threatlevel/2011/01/egypt-isp-shutdown/>.

B. Role Reversal, Non-State Actors

The reverse situation, where the protestors block the government's access to the internet, should be considered as well. A non-state actor would not have the authority to regulate the ISPs and therefore would most likely have to use some sort of violence in order to accomplish the task. In considering the most probable methods to be used by the protestors and the resulting effects it is clear that in most instances the results would have been violent. The five methods to be considered here are the following: cutting the internet cables, blowing up the buildings housing the ISP servers, conducting a cyber-action to take down or damage the servers, an armed takeover of the ISPs, and persuading the ISPs to shut down access voluntarily.

The majority of the internet travel for Europe and Asia passes through the Egyptian fiberoptic corridor.¹⁴⁴ Severing these cables would not only affect the internet in Egypt but would also severely affect the internet around the globe.¹⁴⁵ That loss or disruption of the internet would not rise to the level of a violent consequence. However, if the protestors damaged or destroyed property in order to sever the connection, then this would be classified as an attack. Most likely the protestors would not have direct access to these cables and therefore would have to damage or destroy part of the cables in order to disconnect them.

If the protestors decided to target the servers of the ISPs instead by bombing the buildings in which they are housed it would be categorized as an attack. The bombings would cause damage and destruction of the servers and surrounding property. There is also a strong possibility that injury and death would result. Each of these outcomes

¹⁴⁴ Cowie, *supra* note 134.

¹⁴⁵ *Id.*

would be a violent consequence of such an action, and accordingly, such action would be an attack.

Using a cyber-operation to take down or damage the servers could be an attack. If the protestors used some tool or program that would cause the servers to shut down without physically damaging them, then the action would not be an attack. However, if a virus or other malware was used that permanently damaged the server in some way, it would be a violent consequence. For example, if the protestors sent a virus that caused the cooling fans in the servers to stop working, leading the servers to overheat and crash, this would be a violent consequence and classified as an attack.

Over-taking the ISPs by force would be an attack. The protestors would be armed and it would be reasonably foreseeable that some type of injury or death, damage or destruction would result from using force to shut down the ISPs. Hence, the results of such an action would be violent and considered an attack.

The only method that on its face would not be an attack would be to persuade the ISPs to voluntarily shutdown internet access. Having the ISPs willingly black out the internet would not involve any damage or destruction of property. It would be similar to having the Egyptian government issue the orders. Remember that the non-state actor (the protestor) is not shutting down the internet out of a matter of right. The Egyptian government had the legal ability to order the blackout. What is proper for a government to do is not always proper for a non-state actor to do. Nonetheless, just because the actor does not have a right does not mean that the action amounts to an attack. There would be no violent consequences as a result of persuading the ISPs to freely shutdown the internet. For that reason, it would not be an attack.

It can be seen from the discussion in this section that Egyptian government's actions in shutting down the

internet access in Egypt would not be an attack under the law of armed conflict in a non-international armed conflict. Egypt's actions did not result in any violent consequences. After looking at the situation if the parties had been reversed, it can be seen that most probable methods that could be used by the protestors to limit internet access would likely have resulted in violent consequences and have been classified as an attack.

V. CONCLUSION

Severing internet access within the borders of a country is not an attack in a non-international armed conflict. An attack is an act of violence. As a result of the blurring between international armed conflicts and non-international armed conflicts this definition applies in both contexts. To determine if an act is an attack, the effects tests should be applied. This test is the most appropriate test to use. The effects test looks at the consequences of the action and determines if the results are violent. Violent consequences are more than just mere inconvenience. They are consequences that result in injury or death, physical damage or destruction to property. When this test is applied to the hypothetical proposed, it can be seen that the Egyptian government's actions in shutting down the internet did not produce any violent consequences. Therefore, Egypt's actions of severing internet access within its borders would not be an attack in a non-international armed conflict.