

JOURNAL OF LAW & CYBER WARFARE

FOREWORD

Cyber Warfare, What are the Rules?

By Daniel B. Garrie

ARTICLES

Cyber Attacks and the Laws of War

By Michael Gervais

If You Wish Cyber Peace, Prepare for Cyber War: The Need for the Federal Government to Protect Critical Infrastructure From Cyber Warfare.

By Michael Preciado

They Did it For the Lulz: Future Policy Considerations in the Wake of Lulz Security and Other Hacker Groups' Attacks on Stored Private Customer Data

By Jesse Noa

A New Perspective on the Achievement of Psychological Effects from Cyber Warfare Payloads: The Analogy of Parasitic Manipulation of Host Behavior

By Dr. Mils Hills

Volume 1 | Winter 2012 | Issue 1

(c) 2012 – 2013. Journal of Law & Cyber Warfare.

All Rights Reserved.

www.jlcw.org

EDITORS

Daniel B. Garrie, Esq., Editor-in-Chief
Siddhartha Rao, Esq. Executive Editor

Associate Editors

Candice Lang, Esq., Editorial Fellow
Stephen Williams, Esq., Editor-at-Large

EDITORIAL BOARD

William Spernow	Jeff Bardin
Alex Carrillo	Dick Crowell
Uma Chandrashekhar	Gus Dimitrelos
Patrick Grey	George Hull
Thomas A. Johnson	Alan Roper
Jonathan E. Turner	Russell Walker
Judge David Harvey	Joseph E. Weiss
Michael Schmitt	

FOREWORD

Cyber Warfare, What Are The Rules?

By Daniel B. Garrie*

What is not cyber-warfare? Al-Qaeda terrorists fly two jetliners into the twin towers killing almost 3,000 people.¹ An American plane flies over Hiroshima and drops an atomic bomb killing over 90,000 people.² The Nazis force hundreds of thousands of people into gas chambers and kill millions of people.³ A group of soldiers execute hundreds of innocent people.⁴ A

* Daniel Garrie is the Senior Managing Partner and co-founder of Law & Forensics LLC a boutique consulting firm specializing in complex e-discovery management, digital forensic investigation, and cyber security preparedness. Mr. Garrie has served as an Electronically Stored Information Liaison, Forensic Neutral and Expert for the L.A. Superior Courts, 2nd Circuit, 3rd Circuit, 7th Circuit, New York Supreme Court, and Delaware Supreme Court. . He has published over 100 articles, been cited by the Supreme Court, and the second edition of his treatise *Dispute Resolution and E-Discovery* will be published by Thomas-West in 2013. He can be reached at Daniel@lawandforensics.com

¹ *Padilla ex rel. Newman v. Bush*, 233 F. Supp. 2d 564 (S.D.N.Y. 2002).

² See, e.g., Gabriella Blum, *Laws of War and the Lesser Evil*, *The*, 35 YALE J. INT'L L. 1 (2010).

³ Noah Feldman, *Choices of law, choices of war*, 25 HARV. JL & PUB. POL'Y 457 (2001).

⁴ Matthew Lippman, *Convention on the Prevention and Punishment of the Crime of Genocide: Fifty Years Later*, 15 ARIZ. J. INT'L & COMP. L. 415 (1998).

military releases poisonous gases upon opposing forces.⁵ All of these actions if committed constitute acts of war and war crimes (albeit some may argue that not all of these acts constitute war crimes).⁶ While the devil is in the details, the crux is that in all of these scenarios there is physical evidence: DNA, radiation signature, witnesses; bullets; and gas residue.⁷ In cyber warfare, what is the physical evidence? A binary string of 10101010 in the digital ether?

Since the establishment of the United Nations, wars of aggression have been outlawed,⁸ and multilateral conventions refer to “armed conflict” instead of “war.”⁹ The word cyber does not appear in these texts or in the

⁵ See, e.g., Gabriella Blum, *Laws of War and the Lesser Evil*, *The*, 35 *YALE J. INT'L L.* 1 (2010); Army Reg. 27-10, *U.S. Army Field Manual: The Law of Land Warfare*, para. 31 (1956); British Manual of Military Law, Pt. III, sec. 115, n. 2 (1958).

⁶ AFP 110-31, *International Law—The Conduct of Armed Conflict and Air Operations*, 19 November 1976, 1-10.

⁷ Joshua E. Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 *AFL REV.* 43 (2009).

⁸ Article 2 of all four 1949 Geneva Conventions use this language: “The present Convention shall apply to all cases of declared war or of any other armed conflict which may arise...” U.N. Charter art. 2, para. 4. United Nations Charter, Article 2(4) prohibits the use or the threat of force in international relations. Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations, U.N. General Assembly Official Records, 25th Sess., U.N. Doc.A/RES/2625 (1970); see also, Robert Rosenstock, *The Declaration of Principles of International Law Concerning Friendly Relations: A Survey*, 65 *AM. J. INT'L L.* 713, 720 (1971).

⁹ “The law of war is to be found not only in treaties, but in the customs and practices of states which gradually obtained universal recognition, and from the general principles of justice applied by jurists and practiced by military courts. This law is not static, but by continual adaptation follows the needs of a changing world.” Trial of the Major War Criminals Before the International Military Tribunal, Nuremberg, 14 November 1945-1 October 1946 (Nuremberg, Ger., 1947), 221.

multitude of others that adjoin these legal frameworks.¹⁰

This Journal seeks to promote legal scholarship that can aid the global community as a whole to address this new dimension of war. With the advent of cyber warfare the complexity of what is war is even more clouded and the application of law to this is even murkier.

The focus of this journal is on cyber-warfare.¹¹ Cyber-warfare occurs when one country perpetrates a cyber attack against another country that would to the reasonable person constitute a state act of war.¹² The purpose of the Journal is to encourage dialog to explore and define what constitutes a cyber attack and what constitutes a reasonable expectation of cyber-security.¹³

Below are two of the hundreds of scenarios on which the law remains silent: Would a cyber-assassination by a foreign government constitute an act of war? Is a nation's cyber attack initiated in self-defense

¹⁰ Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 NAVAL L. REV. 132, 140 (2005); Frank J. Cilluffo et al., *Bad guys and good stuff: When and where will the cyber threats converge*, 12 DEPAUL BUS. L.J. 131 (1999).

¹¹ Hannah Lobel, *Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict*, 47 TEX. INT'L LJ 617 (2011); Solce, *The Battlefield of Cyberspace: The Inevitable New Military Branch - The Cyber Force*, 18 ALB L.J. SCI. & TECH. 293, 301 (2008); Jeremy Richmond, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict*, 35 FORDHAM INT'L LJ 842 (2011).

¹² Stephen Dycus, *Congress's Role in Cyber Warfare*, J. NAT'L SECURITY L. & POL'Y 155, 162 (2010) ("Cyber warfare, as that term is used here, refers to conflicts that utilize cyber or electronic weapons either offensively or defensively, or both."); Understanding Cyber Warfare, *available at* <http://cyber.laws.com/cyber-warfare> (last visited Feb. 5, 2013).

¹³ Roger W. Barnett, *A Different Kettle of Fish: Computer Network Attack*, 76 INT'L J. STUD., 21, 31–32.

that results in the deaths of thousands of civilians an act of war? Is it a war crime?

The assassination by bullet of a foreign leader is an act of war and proving it is a matter of using the physical evidence to connect the dots.¹⁴ However, what about an individual working for a foreign government attends a speech, say at the United Nations, and using a wireless device kills five world leaders by sending a signal to their pace makers or insulin pump, that tells the device to send a fatal dose.¹⁵

In this scenario, a trail will be hard to find and even if found, it could be a plant, meaning spyware could have been used to put spyware on an unknowing attendee who by simply turning their phone to silent triggered the incident.¹⁶ This scenario, where five foreign leaders may have been assassinated by a foreign government, raises a slew of complex and new legal issues, such as: How do we prove a country was an actor? What evidence is needed to establish guilt? How does one acquire such digital evidence?

Another complex scenario, a foreign government defends itself (pre-emptively or post cyber attack) against a cyber attack and in defending itself retaliates in a way that results in massive civilian

¹⁴ David Kretzmer, *Targeted killing of suspected terrorists: Extra-judicial executions or legitimate means of defence?*, 16 EUR. J. INT'L L., 171 (2005).

¹⁵ U.S. GEN. ACCOUNTING OFFICE, AIR TRAFFIC CONTROL: WEAK COMPUTER SECURITY PRACTICE JEOPARDIZE FLIGHT SAFETY (MAY 1998); Ellen Nakashima & William Wan, *China's Denials on Cyberattacks Undercut*, WASH. POST, Aug. 24, 2011, at A12.

¹⁶ Major Erik M. Mudrinich, *Cyber 3.0: The Department of Defense Strategy for Operating Cyberspace and the Attribution Problem*, 68 AFL REV. 167 (2012).

deaths.¹⁷ For example, say a foreign government is cyber attacked by several foreign governments that results in a nuclear powered aircraft carrier almost melting down, which if it had melted down would have killed thousands of civilians. As a defensive measure the attacked country responds triggering defensive digital counter cyber attack that results in the foreign governments' power grids going down, causing tens of thousands of civilian deaths. The origin of the power failure was the counter attack, but the fragile infrastructure, feeble cyber security, and the antiquated state of the power grid all contributed.

The aforesaid defensive scenario presents a slew of issues, including: whether a non-lethal cyber warfare attack is a "use of force" that can be returned, or merely an act that violates international law.

Would the defensive counter measures constitute an act of war?¹⁸ Do they constitute war crimes against humanity? Who is to be held responsible? The computer programmers who wrote the code? The military project manager who oversaw the creation of the code? The commander who hit the button setting off the event? The hardware engineer who created the computers that enabled the attack? What constitutes an act of war is blurred? Moreover, establishing who is the perpetrator, or enemy, in a cyber warfare scenario is an even greater challenge.

As a cyber-security and legal professional where I am asked to bridge these realms I often find that many

¹⁷ See, e.g., Charles P. Trumbull IV, *The Basis of Unit Self-Defense and Implications for the Use of Force*, 23 DUKE J. COMP. & INT'L L. 121 (2012); Sean Murphy, *The Doctrine of Preemptive Self-Defense*, 50 VILL. L. REV. 699 (2005).

¹⁸ Hans Boddens Hosang, *Force Protection, Unit Self-defense, and Extended Self-Defense*, THE HANDBOOK OF INTERNATIONAL LAW OF MILITARY OPERATIONS, 420..

scenarios lack bright lines as in the examples above, which makes the legal realm even more complex.

As a bridge between these realms, it is apparent there is a vast divide between the cyber and legal realms. No one disputes that (1) the digital realm blurs the complicated and often confusing rules that govern modern day warfare and (2) the rules of warfare have changed and will continue to evolve. It is my belief that the threshold is shifting and thus mandates the need to redefine the act of war itself and the laws that govern the conflict.¹⁹ The focus of the Journal of Cyber Warfare is to ask these tough questions and engage legal,

¹⁹ As a response to cyber intrusions by foreign groups against US commercial interests, the President should consider an executive order expanding the powers of the Federal Intelligence Surveillance Court (or FISC) to allow companies to petition for a government response to offenses committed against the company. Presently in the United States, the FISC is responsible for issuing warrants for domestic surveillance of suspected foreign operatives in the U.S. Between international arbitration, FISC, and civil courts; corporations that are hacked by agents of sovereign nations have little realistic recourse.

Imagine a scenario whereby an American corporation in the aerospace industry is hacked. All investigations point to the responsible party being an agent of a sovereign nation. While the corporation may be able to recover fiscally through insurance policies, the damage to the industry and the ability of this company to compete nationally and internationally is permanently altered. With an expansion of the FISC, this corporation would be able to petition a government body, such as the Department of Defense. If the DOD agrees with the seriousness of the hack and the long standing implications of this act, then the DOD would then make a special appeal for emergency action on behalf of the company that would be heard within 24 hours. If the expanded FISC agreed that action was necessary, the DOD would be permitted to take action against the sovereign nation.

This expansion of the court would require an expansion of the bench, a position which I would openly pursue to ensure the judiciary is fully informed on the ways and means of cyber intrusions.

technology, government, and to shape the evolution of these new rules of war.