

JOURNAL OF LAW & CYBER WARFARE

FOREWORD

Cyber Warfare and the Corporate Environment

By Chris Colvin, Daniel Garrie, and Siddartha Rao

ARTICLES

Cyberwarfare: Attribution, Preemption, and National Self Defense.

By John Dever and James Dever

Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy.

By James E. McGhee

Is Cyber Espionage a Form of Market Manipulation?

By Noah Bledstein

Volume 2 | Spring 2013 | Issue 1

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

All Rights Reserved.

www.jlcw.org

EDITORS

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

Associate Editors

Stephen Williams, Esq., Editor-at-Large

EDITORIAL BOARD

Alan Roper	Alex Carrillo
Chris Colvin	Dick Crowell
Douglas DePeppe	George Hull
Gus Dimitrelos	James Christiansen
Jeff Bardin	Jonathan E. Turner
Joseph E. Weiss	Larry Ponemon
Noah Bledstein	Patrick Grey
Richard Borden	Roei Haberman
Russell Walker	Thomas A. Johnson
Uma Chandrashekhar	William Spernow
Yoav Griver	

JOURNAL STAFF

Giri Vakkalanka	Kim Kopoff
Margaret Mak	Radhika Tiwari
Renee Almassizadeh	Sarah E. Haines

Is Cyber Espionage a Form of Market Manipulation

By Noah Bledstein*

On March 3rd 2013 the New York Times ran the article “As Hacking Against U.S. Rises, Experts Try to Pin Down Motive”.¹ The thrust of the article is that industry and government agencies have proof the Chinese are engaged in great deal of cyber espionage against American companies, but experts are having a hard time ascribing specific motives to many of the “attacks”.

The Chinese motives certainly aren’t limited to a single purpose. There seems little doubt that they steal intellectual property for its intrinsic value in making sophisticated products without incurring the expense of research and development. It has also been reported that they target sensitive corporate strategies in order to provide Chinese companies an upper hand when negotiating with foreign competitors. Why wouldn’t

* Noah Bledstein recently retired from his position as the Chief of Cyber Law, 24th Air Force, Lackland Air Force Base, TX. 24th Air Force provides combat-ready forces trained and equipped to conduct sustained cyber operations, fully integrated with air and space operations. Maj. (Ret.) Bledstein specializes in military cyber law, information operations law, intelligence oversight law, telecommunications law and the law of emerging technologies. From 2006-2009 he was the Chief of Cyber Law for Eighth Air Force JA where his clients included AFCYBER(P), the Air Force Partnership with Industry cyber defense initiative, the Cyber Division of the Global Strike Air Operations Center and the Air Force Information Operations Center.

¹ Perlroth, Sanger, and Schmidt, *As Hacking Against U.S. Rises, Experts Try to Pin Down Motive*, NEW YORK TIMES (March 3, 2013).

they? China does not draw a line between commerce and government, quite the opposite. However the article also points out that China is too heavily invested in the U.S. economy to want to hurt it.

The New York Times article pulls together two important factors without raising what, in retrospect, seems an obvious question; is a significant motive for Chinese cyber espionage the manipulation of U.S. stock and commodities markets through the use of illegally obtained “insider” information. Stated another way, is it possible to correlate the buying and selling of U.S. securities with intrusions into the companies which are being bought and sold? Does the SEC have access to the information about attacks on companies that would allow it to initiate enforcement actions to deter this sort of market manipulation?

A spate of recent news articles and public protests about the breadth and commercial focus of Chinese espionage appears to be the first real move toward public diplomacy as a means of addressing network espionage. These activities are often described using the language of warfare, however from a legal perspective the activities fall squarely within traditional espionage. This public discussion is a significant first step toward establishing international norms which are a pre-condition for the development of customary international law. Ironically, development of a body of customary international law of cyber warfare may have little substantive effect on this form of economic warfare.

It should be noted that this move toward openness was suggested in the Hathaway cyber report to the 44th President five years ago.² With regard to cyber

² Securing Cyberspace for the 44th Presidency A Report of the CSIS Commission on Cybersecurity for the 44th Presidency, Committee for Strategic and International Studies, December 2008.

warfare, standards clearly need to be established, however, an international legal standard for espionage already exists. Stated in laymen's terms the standards are: do unto others better than they are doing unto you, deny everything when caught and don't get caught in a way that allows the victim to exercise their jurisdiction over your people or assets. Espionage is legal under international law, but generally illegal under the laws of the country in which the spying is occurring. To restate the obvious, human intelligence operations require spies on the ground that can be caught, jailed, traded or executed. For our adversaries, cyber espionage has the great advantage that if and when the victims catch the hackers, the main consequences are the loss of access into the targeted systems and the loss of the use of the programs used to find and extract useful information from the targeted networks. Even these consequences assume that the victims have the resources and sophistication to close the "back doors" which allowed the hackers in and patch their systems to prevent the same malware from being used against their systems again. This doesn't provide the victims with much leverage.

Imprecise use of language is a substantive problem in this arena. Where cyber espionage is concerned the term "attack" is invariably misused. The vast majority of cyber espionage is more analogous to theft than physical assault. It is being widely reported that U.S. and other western corporate networks are probed, breached and mined for sensitive data on a regular basis. These activities can easily be characterized as theft and espionage, but most fall well short of rising to a level where they can be regarded as a use of force or act of war.

From a political and military perspective, particularly when the question is whether to consider the

use of kinetic or cyber responses to dissuade such hacking, it is only when activities are directly malicious, attributable to identifiable hostile forces and causing damage which is measurable that such activities can be accurately characterized as an “attack”. There is no bright line standard for what constitutes an “attack” in international law. Cyber “attacks” can include a spectrum of activities; some examples might be seeding a network with the electronic equivalent of time bombs for use during a conflict or modifying the substance of information on the network to make it unreliable.

As in the “real” or kinetic world, how a nation responds to a cyber-attack is always based on the relative value of the damage to the people, property or principles of the victim.³ The semantic problem when describing cyber conflict is that sloppy use of language causes confusion between warfare, criminal activity and nation state espionage. Whether intentional or not, this has caused a lack of clarity about the legal character of the activities in question and has caused confusion about exactly who in government or industry should receive the authority and funding to respond. How government or industry can respond is equally unclear.

It is important to note that even if clear rules for the military use of force in cyberspace or the conduct of “cyber war” existed, it would be of little help in this commercial context.

Practical problems require actionable solutions. This is what makes the possibility that Chinese actors are engaging in market manipulation so intriguing. Unlike other forms of cyber conflict, blatant stock manipulation by a major economic power could have tangible legal consequences inside the United States. All cyber activities leave records which, with enough

³ Schmitt, *Cyberspace and International Law: The Penumbral Mist of Uncertainty*, 126 HARV. L. REV. F. 176 (2013).

diligence, resources and effort, can be used as evidence. If the Securities and Exchange Commission or State's Attorney Generals are presented with forensically acceptable evidence of illegal market manipulation, either could initiate enforcement actions that would put Chinese or other threat actor's assets at risk. Civil forfeiture of assets connected to drug crimes has proved an effective tool for law enforcement. It seems likely that the dollar value of the property in question dwarfs that seized in drug cases.

To date treating espionage as a form of economic crime which can cause the perpetrator's property to be placed at risk does not appear to be a response that has been seriously considered. It could be that the United States government, the states and industry need to reconsider how to deal with this rapidly growing problem. What is really meant when our leaders talk about bringing "all aspects of national power" to the fight? In the age of "big data", it seems reasonable to suggest that the government can cooperate with industry to conduct research to correlate the cyber "attacks," more accurately described as espionage campaigns, with existing records of stock and commodities market transactions.

In light of corporate resistance to revealing hacks of their networks, this sort of effort will require legislation to clarify when Sarbanes Oxley reporting of such incidents is required as well as limitations of potential liability associated with such reporting. By collecting the right data and developing targeted analytic tools, law enforcement and intelligence organizations could look for hacking trends that appear related to subsequent market activity. Once alerted to the possibility of specific crimes they could "drill down" through the data to determine whether company logs provide enough evidence to support an investigation by

the Securities and Exchange Commission or a state attorney general. This could lead to exactly the same sort of enforcement actions which currently attempts to keep American companies and powerful economic actors honest.

What has been described as a “cyber war” may be a new form of economic warfare. More likely, targeted economic espionage is just one manifestation of the aggressive type of international and domestic capitalism that the Chinese view as the new normal.⁴ Regardless of how it is ultimately defined, this motive for nation state sponsored hacking of American companies is worth examination. It provides a rational explanation for some of the economic espionage China appears to have engaged in. This may not be a form of warfare or conflict our military, intelligence or financial regulatory communities are currently authorized, funded, equipped or trained to address, but reality dictates that we engage in the fight we find ourselves in.

If new technologies are allowing our adversaries to change the nature of warfare, it is time to use existing legal mechanisms to address this behavior. Diplomacy and warfare are ultimately about holding that which our adversaries value at risk. Continuing to accept the status quo is not an acceptable option. A broader understanding and more aggressive engagement in the current cyber conflict through new uses of information and analytic tools in concert with enabling legislation and aggressive enforcement of existing domestic laws is overdue.

⁴ Wong, *Hackers Find China New Land of Opportunity*, NEW YORK TIMES (May 22, 2013).