Cyber Terrorism,
Cyber Security, and War:
Fighting in a Virtual World

American Bar Association
International Law Section
2012 Fall Meeting
Miami Beach, FL

David Z. Bodenheimer
Crowell & Moring LLP
Washington, DC

© 2012 Crowell & Moring LLP
“Last summer, the world’s top software-security experts were panicked by the discovery of a drone-like computer virus, radically different from and far more sophisticated than any they’d seen. The race was on to figure out its payload, its purpose, and who was behind it. As the world now knows, the Stuxnet worm appears to have attacked Iran’s nuclear program. And, as Michael Joseph Gross reports, while its source remains something of a mystery, Stuxnet is the new face of 21st-century warfare: invisible, anonymous, and devastating.”

By Michel Joseph Gross
April 2011
Cyber War?

“If we were in a cyberwar today, the United States would lose.”

Statement for Record

“Seizing Opportunity While Managing Risk in the Digital Age”

Michael McConnell

Introduction

Mr. Chairman, Members of the Committee,

Thank you for the opportunity to speak to the Committee on Commerce, Science and Transportation today.

First, I want to open with a simple statement:

If we were in a cyberwar today, the United States would lose.

Or No Cyber War?

The Cyber War Has Not Begun

James Andrew Lewis

Center for Strategic and International Studies

March 2010

Expanded attention to cybersecurity is a good thing, but it seems that it is difficult to discuss this topic without exaggeration. We are not in a ‘cyber war’. War is the use of military force to attack another nation and damage or destroy its capability and will to resist. Cyber war would involve an effort by another nation or a politically motivated group to use cyber attacks to attain political ends. No nation has launched a cyber attack or cyber war against the United States.

Indeed, it would be a bold nation that would do so. A deliberate attack on the United States could trigger a violent if not devastating response. No nation would be foolish enough to send a missile, aircraft or commando team to attack critical infrastructure in this country. The same logic applies to cyber attack. Foreign leaders will not lightly begin a war with the United States and the risk of cyber war is too high for frivolous or spontaneous engagement.
Are Cyber War & Terrorism Bad?
Cyber Contrarians & Doubters

“pork-hungry politicians”

“no substantive basis” for cybersecurity threats

“ulterior motives and conflicts of interest”

The rise of the cybersecurity-industrial complex

“The $100 billion Washington will spend on cybersecurity in the next decade may be less about guarding America from a real threat, and more about enriching revolving-door lobbyists and satisfying *pork-hungry politicians*."

“‘The notion that our power grid, air traffic control system, and financial networks are rigged to blow at the press of a button would be terrifying if it were true,’ Brito and Watkins write. ‘But fear should not be a basis for public policymaking.’ The public has been given *no substantive basis* for such fears.” [Carney, *The Washington Examiner* (Apr. 28, 2011)]
**President Obama**

“[T]his cyber threat is one of the **most serious** economic and **national security challenges** we face as a nation.”

“Yet we know that cyber intruders have probed our electrical grid and that in other countries **cyber attacks have plunged entire cities into darkness**.”

“And last year we had a glimpse of the future face of war. As Russian tanks rolled into Georgia, **cyber attacks crippled Georgian government websites**.”
Sen. Lieberman

“A sophisticated attacker could cripple most of our financial system, take down a lot of the electric grid, or cause physical devastation equal to or greater than conventional warfare. The fact is the threat of cyber attack is among the most serious threats America faces today.”

[Protecting Cyberspace as a National Asset: Hearings before Sen. Comm. on Homeland Security (June 15, 2010)]

Sen. Collins

“But lurking beyond those serious threats are potentially devastating attacks that could disrupt, damage, or even destroy some of our nation’s critical infrastructure, such as the electric power grid, oil and gas pipelines, dams, or communications networks. These cyber threats could cause catastrophic damage in the physical world.”

Cyber 9/11 on Banks

(8) According to the National Journal, Mike McConnell, the former Director of National Intelligence, told President Bush in May 2007 that if the 9/11 attackers had chosen computers instead of airplanes as their weapons and had waged a massive assault on a United States bank, the economic consequences would have been "an order of magnitude greater" than those caused by the physical attack on the World Trade Center. Mike McConnell has subsequently referred to cybersecurity as the "soft underbelly of this country".

S. 773

Iranian Cyber Attacks

Bank of America & J.P. Morgan Chase Cyber Attacks. "I don’t believe these were just hackers," Lieberman said on Friday evening while appearing on C-SPAN. "I believe this was done by Iran and the Qods force, which has its own developing cyber attack capacity."

"In a ‘highly classified’ report last week the Joint Chiefs of Staff’s Intelligence Directorate, or J-2, confirmed continuing Iranian cyber attacks against U.S. financial institutions, NBC said.”

Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials.

“The Chinese have attempted to map our infrastructure, such as the electrical grid,” said a senior intelligence official. “So have the Russians.”

“For a society that runs on power, the discontinuity of electricity to chemical plants, banks, refineries, hospitals, and water systems presents a terrifying scenario. Economists recently suggested that the loss of power to a third of the country for three months would result in losses of over $700 billion.”
Intelligence Warning

“The Chinese are relentless and don’t seem to care about getting caught. And we have seen Chinese network operations inside certain of our electricity grids. Do I worry about those grids, and about air traffic control systems, water supply systems, and so on? You bet I do.”

(Joel Brenner, head of U.S. Office of National Counterintelligence Executive, Apr. 21, 2009)

Panetta compares cyber threat to Pearl Harbor

“We could face a cyber attack that could be the equivalent of Pearl Harbor. [Such an attack could] take down our power grid, take down our financial systems in this country, take down our government systems, take down our banking systems. They could virtually paralyze this country.”

[Defense Secretary Panetta, Aug. 11, 2011]
Real-World Cyber Attacks

**Stuxnet Attack**

Nuclear Facility Attack. Penetrated & sabotaged control systems at Iranian *Bushehr nuclear power facility* [Senate Stuxnet Hearings (Nov. 17, 2010)]

- Military-grade “cyber missile”
- Exploited 4 “zero-day” vulnerabilities
- Employed stolen digital certificates
- Took months & millions $$ to build

**Pipeline Explosion**

Pipeline Attack. “A previous historic example includes a reported case of stolen code that impacted a pipeline. In this case, code was secretly ‘Trojanized’ to function properly and only some time after installation it instructed the host system to increase the pipeline’s pressure beyond its capacity. This resulted in a three kiloton explosion, about one-fifth the size of the Hiroshima bomb.”

Foreign Cyber Threats

- **40,000 Hackers:** “There are forty thousand Chinese hackers who are collecting intelligence off U.S. information systems and those of our partners.” (Adm. McConnell, Jan. 2008)

- **Daily Attacks.** “A defence force source said yesterday that attacks initiated from China occurred almost on a daily basis.” (Australian Defense Force, Apr. 2009)

- **Classified Data Compromised.** “A China-based cyber espionage network had accessed 1200 computers in 103 countries containing classified documents.” (Munk Centre for Int’l Studies, Apr. 2009)

China Cyber Dominance

“According to its “Cyber Warfare Doctrine,” China’s military strategy is designed to achieve global “electronic dominance” by 2050, to include the capability to disrupt **financial markets, military and civilian communications capabilities, and the electric grid** prior to the initiation of traditional military operations.”

Cyber War, Terrorism & the Private Sector: Do You Care?

Wiped Out?
**International Law**

- **Hague Conventions**
  - Laws of War & War Crimes
  - 1899 & 1907

- **Geneva Conventions**
  - Humane treatment
  - 1949

- **UN Charter**
  - Right to self-defense
  - Articles 51 & 74

**Cyber Attacks Covered?**

- **Limits on Cyber Attack?**
  - Military necessity & proportionality
  - Attribution (no unprovoked attacks)

- **Limits on Cyber Targets?**
  - Interdependent military/civilian IT
  - Humanitarian needs

- **Defense vs. Offense?**
  - Right to defend, not retaliate
  - Espionage not limited
Cyber Terrorism & War

“One is the threat of cyber attack. Many nation states, like Russia, China, North Korea, and Iran, have offensive cyber attack capabilities, while terrorist groups like Hezbolla and al Qaeda continue to work to develop capabilities to attack and destroy critical infrastructure like the electric gird through cyber attacks.”


Global Arms Race

“Cyber security the new ‘arms race’” Van Loan

“I really look at [cybersecurity] almost as the new arms race. There isn’t a day that goes by without someone somewhere trying to breach the Government of Canada’s information systems.”

(Public Safety Minister Van Loan, CTV News, May 27, 2009)
Going on the Offensive: Contractors in Cyber War

International Law
- Authority to attack?
- Authentication?
- Rogue virus?

U.S. Law
- Electronic surveillance & wiretapping laws
- Covert operations (Title 10 vs. Title 50)
- Posse Comitatus (DoD & domestic operations)

$50 Billion Lawsuit

“One lawsuit alone, filed May 12 by a purported national class of Verizon customers, seeks $50 billion in damages.”

[“Court Will Decide State Secrets Issues First in NSA Phone Surveillance Class Action Suit,” Privacy Law Watch, June 9, 2006]
Contractor Liability Risks on the Cyber Battlefield

What Happens When You Sell IT Security that Fails?

- Gov. Contractor Defense
  - Commercial specifications

- SAFETY Act Coverage
  - No terrorist attack

- 85-804 Indemnification
  - Limited agency authority

- Legislative Proposals
  - Political limitations

Contractor vs. ???

- Government Claims?
- 3rd Party Lawsuits?
- Insurance Coverage?

Boyle vs. UTC, 487 US 500 (1988)
Collateral Damage: Types of Cyber Disputes

- **Botnet Sponsor**
  - Government takes over system to launch attack

- **Denied Network Access**
  - Government cuts off access during an attack

- **Disrupted IT Systems**
  - Government causes collateral damage during attack

Private Sector Remedy?

- **Eminent Domain**
  - 5th Amendment action for Government taking?

- **Contract Disputes Act**
  - Contractor right of action?
  - Timely remedy?

- **Federal Tort Claims Act**
  - Private sector remedy for tort?
Questions?

David Z. Bodenheimer
Crowell & Moring LLP

dbodenheimer@crowell.com

(202) 624-2713