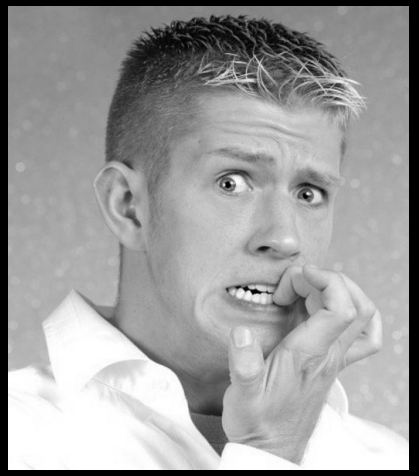
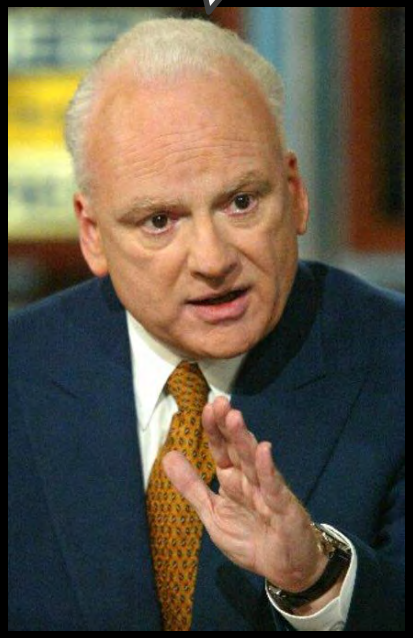
CYBER TERRORISM AND CYBER WARFARE

A Clear and Present Danger, the Sum of All Fears, or Much To Do About Nothing?

Dr. Barry Cartwright
International CyberCrime Research Centre
School of Criminology
Simon Fraser University



We need to take measures now to avert a cyber war disaster.



Richard Clarke, White House terrorism adviser

The next Pearl Harbor could very well be a cyber attack.

Leon Panetta, CIA Director

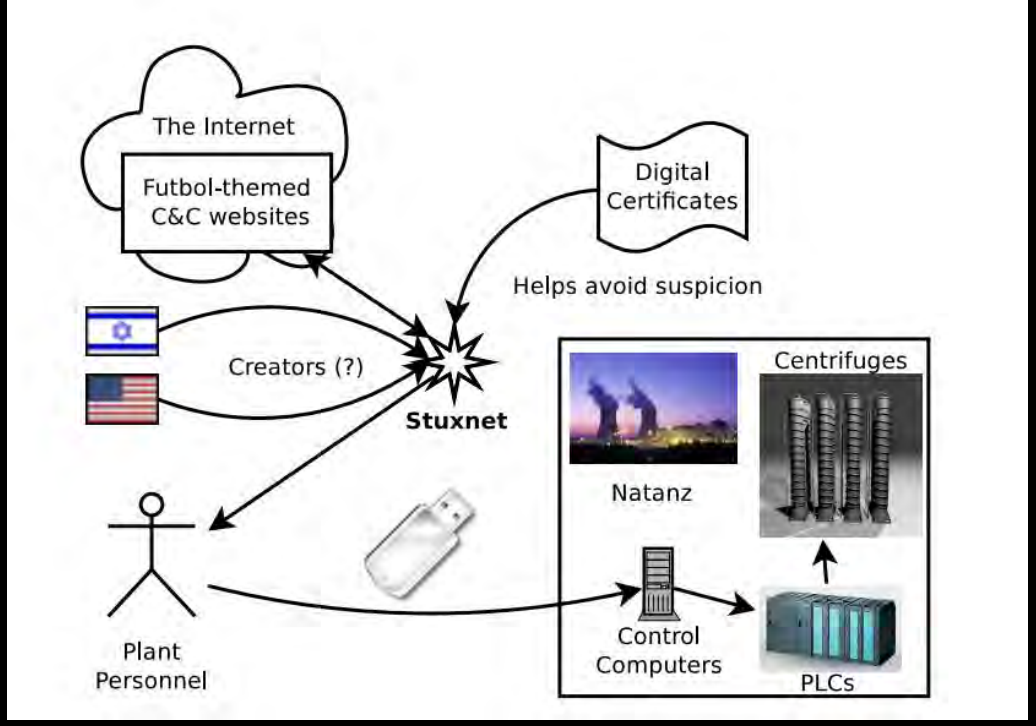
Stuxnet is the Hiroshima of cyber-war.

Labelling Theory

- Deviance is not a quality of the act itself, but rather, the consequence of rules and sanctions being applied to the "offender" by rule makers and rule enforcers
- "The deviant is the one to whom the label has been successfully applied"
- The likelihood of an act being labelled as deviant depends upon who commits the act, who believes they are being harmed, and who has the power to impose (or to deflect) the label (Howard Becker, 1963)

The Dreaded Stuxnet Worm

- Purportedly developed by Israel, some think with help from the US
- Targeted Iran's so–called "nuclear enrichment program"
- May have destroyed around 1,000 centrifuges, more than 10% of Iranian nuclear capacity
- Stuxnet was "limited," in that it only infected certain types of computers, could only be installed from a flash drive, and had an expiry date


The Internet
Futbol-themed C&C websites
Digital Certificates
Helps avoid suspicion
Creators (?)
Stuxnet
Centrifuges
Natanz
Plant Personnel
Control Computers
PLCs


L1 N I1 I2 I3 I4 I5 I6 I7 I8
AC/DC 115..240V
INPUT 8xAC/DC
SIEMENS
SIPLUS 230RC
ESC
OK
OUTPUT 4xRELAY/10A


Oh, oh. I think we're hooped.

Definition, Attribution and Retaliation

- Stuxnet illustrates problems of definition—is it cyberespionage, cyberterrorism, or out-and-out cyberwarfare? (each warrants a different response)
- Stuxnet illustrates problems of attribution—no way of knowing for sure whodunit, and who to retaliate against
- Stuxnet also illustrates significance of labelling, and who gets to decide who's the outlaw and thus subject to punishment
- If Iran did this to the US, and the US could come even remotely close to proving it, then Iran would either be in the dark, or glowing in the dark

Flame

- “Originated no earlier than 2010” (Wattanajantra, 2012)
- Kaspersky Labs said that Flame was “one of the most complex threats ever discovered”
- Symantec stated that Flame “was likely written by an organized, well-funded group of people working to a clear set of directives”
- Built specifically to collect information from hotspots like Iran and Syria
- Able to replicate itself across “secure” computer networks, turn on computer microphones and cameras, identify the location of mobile devices

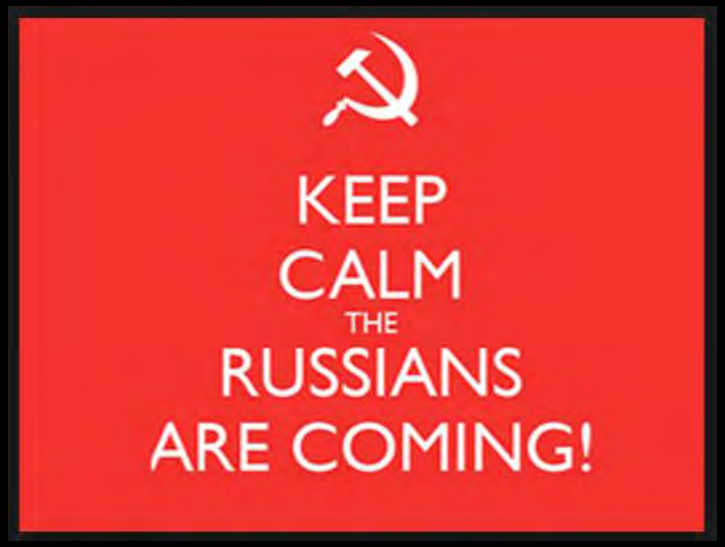
Who would design such a dastardly, devious device?

A. The Russians
B. The Chinese
C. Israel
D. The United States
E. C and D only

BURNING QUESTIONS

The Russians are Coming

- Alleged that the Russian security services launched a cyber-attack against the Ukrainian power grid on December 23, 2015
- Three different energy companies taken down for several hours, resulting in a loss of power in various areas (Lee, Assante & Conway, 2016)
- Also managed to mount denial of service attacks on the energy companies' call centres (making it impossible for affected people to report the problem)

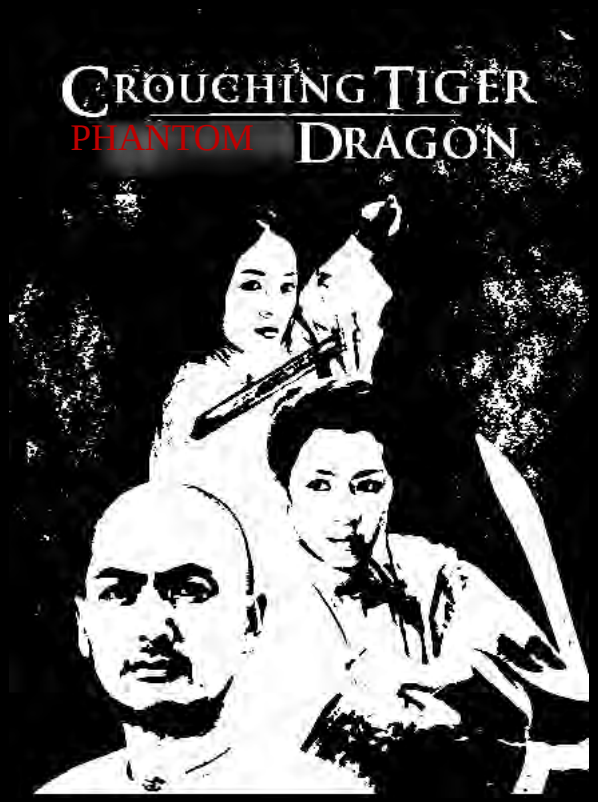


Where are They Coming From?

- Used spear phishing techniques, delivering malware-infected email to administrators and IT services
- BlackEnergy3 with KillDisk component embedded in Word documents and Excel spreadsheets (Lee, Assante & Conway, 2016)
- It is thought that the same actors also used BlackEnergy3 and KillDisk against a large Ukrainian railway company and a large Ukrainian mining company (Wilhoit, 2016)

The "Myth" of Cyberterrorism

- "Crouching Tiger, Phantom Dragon," by Helms, Constanza & Johnson, 2012
- Say that the history of cyber-terrorism has been surprisingly uneventful, despite media hype and government machinations surrounding the cyber-terror discourse



Defining Terrorism

- "No cyber-attack has risen to the level of being considered a serious candidate for classification as an act of terrorism" (Helms, Constanza & Johnson, 2012)
- It has proven quite difficult to come up with a universally agreed-upon definition of "terrorism," not to mention a definition of "cyber-terrorism"
- Emerald Archer (2014) agrees that there is no universally accepted definition of cyber terrorism, and that so far, there have been no "real," successful cyber terrorist attacks
- One person's "terrorist" might be another person's "freedom fighter"

THE CRUSADES

bite me

1095-1149

1990-Present

Terrorism is In The Eye of the Beholder

- Comes down to having the political power and military might to affix and enforce the "label"

- We should ask ourselves:
  1. Who's invading whose territory?
  2. Who's killing whose civilians?
  3. How else are the oppressed and occupied supposed to fight back against superior forces and technology?
  4. Who says that freedom of speech in cyberspace only applies to the US and its like-minded allies?

Existential vs. Symbolic Threats

- They notion of "security" is itself symbolic—do security measures (either simply announced or actually practiced) make us feel "safe," or "unsafe"?
- The fear of cyber terrorism—coupled with the suspicion and distrust of computer technology—is greater than the risk of cyber terrorism
- With its rapid growth and seeming lack of regulation, the Internet would appear to offer the "anonymity" and "shock" value associated with terrorism
- Public discourse surrounding cyber terrorism (driven in part by the media) whips up fear— "digital Armageddon," "electronic Chernobyl" (Helms et al., 2012)

How Terrorists Do Use Cyberspace

1. Publicity and propaganda
2. Fundraising
3. Sharing information
4. Planning and coordination
5. Recruitment and mobilization (Helms et al, 2012)

Governments and political parties use cyberspace for similar reasons!

Bulletin of the Atomic Scientists

IT IS 5 MINUTES TO MIDNIGHT

Reflections

Bulletin of the Atomic Scientists
2014, Vol. 70(1) 21–31

DOI: 10.1177/0096340213516741
http://thebulletin.sagepub.com

SAGE

Are new technologies undermining the laws of war?

Braden R. Allenby

SEVEN

MINUTES PAST MIDNIGHT

What Does "War" Mean?

- The term "war" is often diluted, e.g., the "war" on obesity or the "war" on cancer
- Real "war" is always violent, and potentially lethal
- War is instrumental (a means to an end)—violence (or the threat of violence) is used to render the opponent defenseless, and bend them to your will
- "The act of war is always political" (Rid, 2012)

The Siberian Pipeline Explosion

- According to Thomas Rid, the most violent cyber-attack so far is the 1982 Siberian pipeline explosion
- USSR tried to obtain the necessary software to run the computerized control systems from the United States, who told them to go fly a kite
- The USSR then got the software from Canada, but it is alleged that the CIA inserted a malicious code that drove the pumps, turbines and valves to work far beyond their capacity

Not So Fast!

- There are no media reports confirming the story
- The KGB denied the story
- When the CIA declassified the dossier (which described the attempt to give the USSR defective technology), there was no mention of an explosion
- There has been no firm evidence of extensive structural damage or casualties

Even if we do attribute this to the US government, we need to ask how they knew for a fact that it was North Korea that was behind the attack on Sony, whether the government should be protecting corporate interests, and whether the retaliation was proportionate.

WORLD

TRENDING Edmonton | AirAsia | WJC | NHL | Greenspan | Magnotta | Best of 2014 | Torture | Ghomeshi

North Korea accuses U.S. of shutting down its Internet, calls Obama a 'monkey in a tropical forest'

The Syrian Electronic Army

- Syrian Electronic Army (SEA) is a well-equipped group of pro-government hackers that supports the regime of Syrian President (and well-known Terrorite), Bashar al-Assad
- Opponents of the Assad regime have been targeted for arrest and torture as a consequence of personal information gleaned from their email traffic by the Syrian Electronic Army
- SEA has also been accused of hacking government internet traffic in Qatar and Turkey, and attacking the Twitter account of the Associated Press, posting a message about Barrack Obama being injured in an explosion at the White House
- Rumoured that Russia and Iran, who are both supporters of the Assad regime, have been training and equipping the SEA
- US government has been helping Syrian activists to smuggle communication equipment into Syria, and providing funding to train groups like Cyber Arabs (who are opposed to the Syrian government)

Attribution

- Who do you blame?
  1. The Syrian government, who may or may not be funding the Syrian Electronic Army ?
  2. The Syrian Electronic Army, who may be difficult to find and target?
  3. The Russian and Iranian governments, who are rumoured to be supporting Syria and the Syrian Electronic Army?
  4. The US, who have been helping Syrian activists to smuggle communication equipment into Syria, and providing funding?

…and Retaliation

- Who should do the retaliation?
  1. Should the US retaliate against Russia and Iran?
  2. Should Russia and Iran (as supporters of Al-Assad) retaliate against the US?
  3. Should the US, Russia and Iran join forces and retaliate against Syria and Al-Assad?

French Kissing

- In 2013, TV5 Monde's screens were switched to display messages from a 'cyber caliphate,' ostensibly in retaliation for the French army's involvement in Syria and Iraq
- At first, it seemed that an ISIL-linked group was targeting the station
- However, investigators found that the hacks appeared to originate in Russia, with a Kremlin-linked group, possibly in support of the Assad regime
- Again, who gets to retaliate, and against whom? And how do you know you got the right one?

Be Afraid

- "People are afraid of things that are invisible and things they don't understand" (Stohl, 2006)
- Cyber fear is generated by what could happen, not by what has happened, or is likely to happen
- Press releases by governments, large corporations and major players in the security industry stress "threats" and "critical needs," paying little attention to actual events (largely because they don't exist)

The European Legacy, 2014
Vol. 19, No. 5, 606–621, http://dx.doi.org/10.1080/10848770.2014.943495

Routledge
Taylor & Francis Group

Crossing the Rubicon: Understanding Cyber Terrorism in the European Context

EMERALD M. ARCHER

Cyber Exploitation	Disruptive Cyber Activities	Destructive Cyber Activity
Cyber piracy	Network disruption	e.g., Stuxnet Worm
Cyber stalking	Denial of service	Damage physical targets
Online fraud		
Data theft