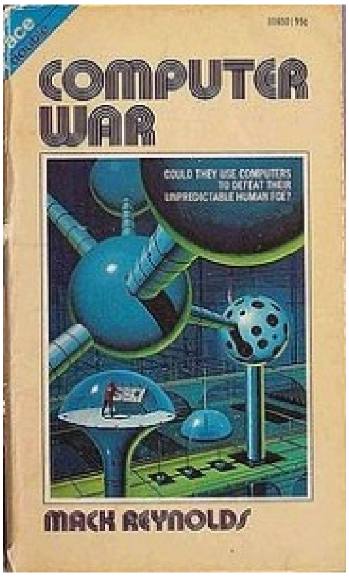
FEAR, UNCERTAINTY, AND DOUBT: THE REAL CYBER ATTACK ON THE TRUTH [UPDATE]


ace
COMPUTER WAR
COULD THEY USE COMPUTERS TO DEFEAT THEIR UNPREDICTABLE HUMAN FOE?
MACK REYNOLDS

[photo: cdrummbks via Flickr]

[*UPDATE — see end of article.*]

One weaselly senator—with long-identified agendas and a pathetically thin understanding of technology—takes to the microphone. Suddenly, by virtue of wrapping his senatorial lips around a few scary words on topics about which he knows little, we citizens are supposed to quake in fear and plead for salvation.

Screw that noise. This is textbook "fear, uncertainty, and doubt" — more commonly referred to as FUD in the information technology industry.

Since the 1970s, FUD tactics have used to suppress competition in the computer marketplace, targeting both hardware and software. Roger Irwin explained,

> …It is a marketing technique used when a competitor launches a product that is both better than yours and costs less,

> i.e. your product is no longer competitive. Unable to respond with hard facts, scare-mongering is used via ‘gossip channels’ to cast a shadow of doubt over the competitors offerings and make people think twice before using it.In general it is used by companies with a large market share, and the overall message is ‘Hey, it could be risky going down that road, stick with us and you are with the crowd. Our next soon-to-be-released version will be better than that anyway’. …

FUD has non-technology applications as well; one need only look at product and service brands that encourage doubts about using any product other than their own, in lieu of actually promoting the advantages their product or service might have.

So what’s the FUD about? Senator Joe Lieberman spouted off about cyber attacks in September last year, claiming Iran was behind disruptive efforts targeting U.S. banks.

Right. Uh-huh. Predictable, yes?

But FUD is used in situations where there is competition, one might point out. Yes, exactly; in September 2012, the case for support of unilateral attacks against Iran was up against the news cycle crush, powered by the post-Benghazi fallout and the drive toward the November general election, followed by the terror that was the “fiscal cliff.” That’s a lot of powerful, compelling competition for both attention, votes, and tax dollars, when members of a reliable but lame duck Congress could be mounting up a pre-emptive cyber war without the headwind of public awareness and resistance, or the too-inquisitive pushback from newbies in the next seated Congress.

The pressure was on; our intrepid weaselly senator speedily whipped out some FUD!
The problem, though, is that no respectable

consultant in the IT security industry picked up the flaming bag of smelly FUD. Take a gander through Kaspersky or Langner websites and look for panicked reports of DDoS assaults on banking—you won’t find them. RSA’s blog never mentions Iran last year at all; F-Secure makes an oblique comment about nation-state cyberwarfare, implicitly critical of U.S. with regard to its deployment of cyberweapons. Kaspersky mentions Iran exactly once, in relation to the “Ma(h)di incident” last year, and not at all in a forecast of 2013. Langner mentions the difficulty of providing adequate cybersecurity, noting Secretary of Defense Leon Panetta’s October 11 speech—again, no reference to Iran.

Intentionally or otherwise, Panetta furthered the FUD with his speech in a way that the mainstream media easily distorted:

> …Let me give you some examples of the kinds of attacks that we have already experienced.
>
> In recent weeks, as many of you know, some large U.S. financial institutions were hit by so-called Distributed Denial of Service attacks. These attacks delayed or disrupted services on customer websites. While this kind of tactic isn’t new, the scale and speed with which it happened was unprecedented.
>
> But even more alarming is an attack that happened two months ago when a very sophisticated virus called Shamoon infected computers in the Saudi Arabian State Oil Company Aramco. Shamoon included a routine called a ‘wiper’, coded to self-execute. This routine replaced crucial systems files with an image of a burning U.S. flag. But it also put additional garbage data that overwrote all the real data on the machine. More than 30,000 computers that it infected were rendered useless

> and had to be replaced. It virtually destroyed 30,000 computers.
>
> Then just days after this incident, there was a similar attack on RasGas of Qatar, a major energy company in the region. All told, the Shamoon virus was probably the most destructive attack that the private sector has seen to date.
>
> Imagine the impact an attack like that would have on your company or your business.
>
> These attacks mark a significant escalation of the cyber threat and they have renewed concerns about still more destructive scenarios that could unfold.
> …

Notice Panetta never actually says U.S. banks suffered Iranian-based DDoS attacks? He segues over to attacks on Saudi machines that might affect oil production, never mentioning what entity was likely responsible. Panetta mentions Iran exactly once—approximately 2184 words after beginning his 3898 word speech—and 861 words after the excerpt above, quite a distance from the examples he cited.

In contrast, he mentions Russia and China in a sentence directly ahead of the mention of Iran; he notes Russia once, and China three times in the same speech.

How are we supposed to infer from this speech that cyber attacks using DDoS on banks were imminent, if not already underway? Mainstream media solved that problem for us, by repeatedly claiming Panetta said in his speech that Iran was a cyber threat to banks.

It didn’t help that Panetta was preoccupied and didn’t step up to demand corrections about reporting on his speech.

Less-than-happy journalism has been too common on this topic. The September 21 Washington Post article that spawned Lieberman’s FUD refers to “U.S. officials.”

> …“I don’t believe these were just hackers who were skilled enough to cause disruption of the Web sites,” said Lieberman in an interview taped for C-SPAN’s “Newsmakers” program. “I think this was done by Iran and the Quds Force, which has its own developing cyberattack capability.” The Quds Force is a special unit of Iran’s Revolutionary Guard Corps, a branch of the military.
>
> Lieberman said he believed the efforts were in response to “the increasingly strong economic sanctions that the United States and our European allies have put on Iranian financial institutions.”
>
> **U.S. officials** suspect Iran was behind similar cyberattacks on U.S. and other Western businesses here and in the Middle East, some dating as far back as December. A conservative Web site, the Washington Free Beacon, reported that the intelligence arm of the Joint Chiefs of Staff said in an analysis Sept. 14 that the cyberattacks on financial institutions are part of a larger covert war being carried out by Tehran. …
>
> [emphasis mine—R.]

Gee, why not name them? Is this just our favorite weaselly senator again, and a mouse in his pocket? Or perhaps these nameless officials were Senators Lieberman, Collins, Rockefeller, and Feinstein, who sponsored the Cybersecurity Act of 2012, up for a vote less than ten days after the election?

Or are these “U.S. officials” part of another government group airing these suspicions without offering any substantive support? Why is the WaPo quoting the cyber attacks claim made by a tiny, little conservative outlet like the Washington Free Beacon? The outlet stated a secret report by “intelligence arm of the Joint Chiefs of Staff” revealed Iran’s anticipated DDoS assault on U.S. banking. Why would anybody affiliated with J-2 disclose anything at all from a secret report to a puny right-wing rag?

It appears there’ve been a number of folks who are allegedly close to the issue and unauthorized to speak to media who’ve been chattering away. Um, why wasn’t Senator Feinstein puling about intelligence leaks, especially when a bill she’s co-sponsored may be directly affected?

It all smells like old fashioned FUD; there’s a lot of fear being pushed, but nothing to remove uncertainty and doubt. Others have criticized the FUD as well as proliferation through distortion and inaccuracies. Computerworld reports experts are not all in agreement about attacks’ origins; see also this excerpt from Digital Dao’s Sept. 28 post, pushing back at Lieberman and media alike:

> **Bloomberg:** “The initial planning for the assault pre-dated the video controversy, making it less likely that it inspired the attacks, according to (Dmitri) Alperovitch and (Rodney) Joffe, both of whom have been tracking the incidents. A significant amount of planning and preparation went into the attacks, they said. “The ground work was done to infect systems and produce an infrastructure capable of launching an attack when it was needed,” Joffe said.”
>
> **CNN:** “To get hold of all the servers necessary to launch such huge attacks, the organizers needed to plan for months, Alperovitch said. The servers had to be compromised and linked together into a network called a “botnet.”
>
> ***FALSE.*** *This attack did not take months*

> *to plan for two reasons: 1) This was a crowd-sourced opt-in botnet commonly used in social activism (aka hacktivist) attacks, and 2) No one needs to create a botnet from scratch anymore. You can find them to rent on pretty much any hacker forum world-wide.*

While all scaremongering proliferates—without any credible information documenting the claims that a nation-state is behind DDoS attacks on banks—more realistic threats to U.S. banking emerged nearly in tandem with the allegations about Iran's cyber assault. Note the stories published by information security journalist Brian Krebs, FastCompany, and other IT news outlets about Project Blitzkrieg, a criminal program targeting 30 U.S. banks with the intent to steal money while tying up the banks' systems with DDoS attacks. How does the public not know that trojans and viruses launched in late summer/early autumn weren't proof-of-concept efforts in advance of real attacks? Skype in particular experienced a widespread virus spread within its community in late September—oddly enough, just before news reports about Project Blitzkrieg—and reporting to date on Project Blitzkrieg indicates that Skype will be a component of the attack.

There's more than one issue that could underpin concerted FUD using the mythos of Iranian cyberwarfare, including the conflicts between the U.S. and the E.U. on surveillance, or tensions over the puzzling inadequate response by the U.S. banking system with regard to their persistent laxity on authentication standards compared to EU banks. (The U.S. has used a single factor while the EU has relied on a two-factor standard. While the EU is more secure, both are inadequate according to security expert Bruce Schneier.)

Whatever the truth, whatever drives the FUD, know this:

— The Cybersecurity Act of 2012 died in

November, though it may be resurrected under the newly seated Congress, or the White House could choose to implement all desired features through an executive order;

– Don’t let the FUD distort your perceptions. “…Some in (IT) industry say DDoS attacks are pretty common. …” They are. They are not the exclusive domain of cyberwarfare, are far more frequently generated by criminal or hacktivist activity.

– Lastly, practice safe computing and safe banking. 1) Run antivirus and anti-malware applications frequently, using more than one antivirus package; 2) Don’t assume Mac OS and iOS are immune, as criminals go where there’s money, not operating systems; 3) If you bank online, use Linux–see Brian Krebs for an overview.

UPDATE – 8:10 PM EST – Check out this interesting report from ProPublica just today, How a Government Report Spread a Questionable Claim About Iran, by Justin Elliott. Notice anything familiar in this article? Looks like a classic dispersion of FUD and at least one familiar outlet. Huh.