

I just sent this story to acquaintances who disclosed a fair amount of these scenarios to me several years ago. In his team's penetration studies, all roads pointed to Beijing, but I was under NDA not to tell, names, etc. But, the short sanitized version from Feb 2005 is:

- Major utility companies POWNED!
- Banks...you, too.
- Communications companies cannot fathom the concept of security much less spell it.
- Airlines owned, and the series of ATC problems in the last 18 months are the Chinese cyber equivalent of U2 flights testing the response mechanisms and capabilities of Soviet radar detection and military/policy reactions. Several of the power outages we have all seen in the news are similarly "tests" by the Chinese of our detection and response systems. (Read "Time Based Security" for the analysis on how to measure this aspect of security.

The private companies (CIs), some of them, have been in touch with the Feds about these attacks, and both of them have wanted to keep it quiet for many obvious reasons, including the Olympic Games.

I have to assume the folks I know have been briefing the right folks in DC about this. I tend to believe that we are also being Psyop'd with cover stories, claimed ignorance or partial truths to disguise what is clearly, IMHO, a potentially devastating first strike capability.

Tie this to Chinese satellite ambitions and their space program, I think we are seeing the first cyber-implementation of Sun Tzu at a truly national, Class III Information Warfare scale. (A couple of chapters in IW1 were dedicated on how to build a cyberforce/cyber-army and what to do. When I look at what has been happening at the CI level, it certainly appears that someone read it. :-))))))

I have talked a bit about this in some fora, but if the analyses I was privy to are accurate, we have a whole lot of catching up to do.

More importantly, I urge us to revisit a question that I asked in 1990 in my first novel: What do we do if we know our CIs are penetrated and owned by adversaries? I came up with one possible scenario/response. I believe it's certainly time to revisit, and perhaps InfowarCon could provide the impetus to address unpopular ideas such as this.

- What is war?
- What is cyber-war?
- Escalation from cyber to kinetic

etc. as we did for so many years at IWC.

Do we know if anyone at the Federal level is currently seriously examining this issue? CI collapse, graceful degradation, reconstitution and such? We have a pretty good feel that the here-to-fore defensive methods are failures.

I guess it's time for me to write a proper article on this now that there is some 'official' recognition of the potential gravity of the situation.