CYBER Hustlers Atlantic Council, New York Times: Americans Stupid, Military Incompetent

by John Stanton

"There is an inverse relationship between public access to the Internet and the inability of governments and institutions to control information flow and hence state allegiance, ideology, public opinion, and policy formulation. Increase in public access to the Internet results in an equivalent decrease in government and institutional power. Indeed, after September 11, 2001, Internet traffic statistics show that many millions of Americans have connected to alternative news sources outside the continental United States. The information they consume can be and often is contrary to US government statements and US mainstream media reporting. Recognizing this, terrorists will coordinate their assaults with an adroit use of cyberspace for the purpose of manipulating perceptions, opinion, and the political and socioeconomic direction of many nation-states." *Terrorists Will Exploit and Widen the Gap* between Governing Structures and the Public, American Behavioral Scientist, 2002

Information is a strategic resource vital to national security. US Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of USG interests, policies, and objectives through coordinated programs, plans, themes, messages, and products synchronized with the actions of all elements of national power: Diplomacy, Intelligence, Military, Economic, Finance, Law Enforcement, Information… The DOD must also support and participate in USG Strategic C communications activities to understand, inform, and influence relevant foreign audiences, including the DOD's transition to and from hostilities, security, military forward presence, and stability operations. US Army *Unconventional Warfare Manual,* 2008

In the early 1990s scores of studies were conducted by the US government, think tanks, consulting firms, defense contractors, futurists and military thinkers on the likely threats to the US military's electronic communications systems. Those analyses often encompassed commercial networked systems.

For example, in May 1993 Security Measures for Wireless Communications was released under the auspices of the US National Communications System. Not long after, the same office published *The Electronic Intrusion Threat to National Security and Emergency Preparedness* in December 1994. During June 1995 a conference, co-sponsored by the Technical Marketing Society of America, was held. That event was titled *Information Warfare: Addressing the Revolutionary New Paradigm for Modern Warfare.*

Then as now the most pernicious and non-life threatening cyber-attacks normally resulted in the theft of identities and, perhaps, intellectual property to which 'experts' would assign dollar values. Other network, computer assaults were visited upon databases containing personal information producing headaches for the individuals who had to get new credit cards or revise

identities. Embarrassment was the penalty for commercial organizations too cheap to invest in robust electronic security systems.

I Love New York

Information Operations have not taken place (yet) resulting in large scale, life-threatening fallout, but the 1977 New York City blackout provides some clues as to what might result from a successful cyber assault on a power grid. Those initially responsible for the Black Out were bolts of lightning from a thunderstorm that repeatedly struck a Consolidated Edison facility. Redundancies built into the grid that did not function and aging equipment and operator error led to the loss of power. Observers were already thinking about rudimentary network centric themes even then as The Trigger Effect from the 1978 series Connections by James Burke demonstrates.

It is difficult to say with any certainty if, over the last 23 years, competently secured US military networks have been successfully compromised by electronic intrusions by noted Information Warfare nations Russia, China and Israel seeking to steal classified, compartmented data or Intelligence, Surveillance and Reconnaissance technologies. That information is not likely to ever see the light of day, classified as it should be.

Certainly, US military websites and other government organizations have been hacked successfully over the years resulting in detrimental data spills and website defacement. But these do not rise to the level of national security threat; instead, they are clear cut cases of robbery and vandalism and should be viewed from a civilian law enforcement perspective.

Insiders Have Done More Damage to US National Security

It is worth noting that, to date, the most serious breaches of US national and military security have come at the hands of disillusioned US citizens like Jonathan Pollard (US Navy) and Richard Hansen (FBI) who lifted paper documents from secure facilities, and Edward Snowden (NSA & Booz Allen) who downloaded electronic files to his storage devices.

As far as anyone knows, the electromagnetic waves emanating from a computer display have not been remotely manipulated by a state or non-state actor to kill or maim a person looking at the display. But transmitting retroviral software at some distance, or using an intelligence operative to insert destructive code via a flash drive, is known to have been successful in the US-led operation against Iran as the Stuxent case demonstrated.

Recent electronic intrusions and theft of data/images from the non-secured private accounts of former NATO commander General Phillip Breedlove, USAF (Ret.); Andrew Weiner (sexting former politician from New York) or General Colin Powell, USA (Ret.) are generally served up by hackers and then picked up as news by US Big Media and Social Media. Humiliating as it is for the individuals involved, this nefarious CYBER-vandalism is not a national security matter,

but it is used, gleefully, by any number of political interest groups and businesses for their own ends.

In like manner, the Sony, Democratic National Committee and Yahoo electronic break-ins, for example, are not national security incidents by any stretch of the imagination. Were they criminal actions and embarrassing for the victims? Yes. Did the information peddled by the hackers influence the public in some fashion? Sure. If sponsors of the hackers are from Russia, China, Iran, DPRK, Daesh, Israel or any other cyber-suspect, should they be exposed and brought to justice? Yes.

Should we nuke them or carpet bomb them? No.

It is problematic that politico-military strategists and tacticians, spurred on by any number of think tanks and CYBER hustlers in Washington, DC and New York (Atlantic Council, New York Times), have pushed the robbery of data/information and vandalism, or defacement of main-page websites into a crisis that threatens the nation's stability. More's the pity, they have pasted CYBER over Information Warfare and have meshed it with Asymmetric Warfare and Unconventional Warfare not recognizing the differences and nuances.

CYBER Influence Peddlers: Pest Control Needed

CYBER enthusiasts at the Atlantic Council and the New York Times see foreign news agencies like Xinhua/People's Daily, Press TV, RT, Sputnik News and Hezbollah, which all broadcast news and information with their brand of spin, as demonic CYBER influence peddlers who are corrupting the American national consciousness by engaging in perception management techniques in an attempt to electronically captivate American audiences and turn them, well, to the "dark side."

Iran's Press TV Internet traffic statistics show it is ranked 26,598 with 28 percent of its visits coming from the United States. RT is ranked 446 in the world with 18 percent of its visitors from the US. Sputnik News is 1410 with 8 percent of its visitors from the US. Xinhua is ranked 25,000 with about 3 percent visiting from the US and the People's Daily does not even rank.

In this dark CYBER world, the unemployed and disaffected youth bulges (but why are they jobless and disenchanted), social miscreants and American citizens will populate evil foreign websites and after viewing assorted marketing/propaganda they will by Pepsi instead of Coke; whoops, I meant to say join the Islamic State or the Chinese Communist Party; move to Russia; or take in the Hezbollah website (no ranking on the Internet).

What this says, in part, is that those pushing CYBER fear have unwittingly indicted the United States and its people of idiocy. They seem to be saying that the American people have been ill served by the Constitution and the Bill of Rights, educational institutions and the government and the citizenry is but a collective of dolts incapable of sorting through information pushed out

of non-Western media outlets. In the United States, the First Amendment makes sure that all-points of view can be aired on the premise that the American people have the ability to harvest information and distinguish between info-crap and 'actionable' info that can be turned into positive knowledge for civil good.

What is there to fear from comparatively small state backed-foreign news outlets? So they spin news or publish opinions contrary to the US narrative. So what? How is that any different from left and right wing publications in the United States that take down US civilian and military institutions? The American public can handle all of this. The CYBER Fear pushers further display their ignorance by assuming that the US national security machinery has not done enough to protect the enfeebled American public from opinions emanating from non-Western sources. The CYBER chicken-littles believe too, that the US military and those in charge of America's critical infrastructure sets do not understand the gravity of the CYBER Danger.

Nonsense.

Sleep Well

As the US Army's Unconventional Warfare Manual and scores of US military CYBER commands, and doctrinal publications make clear, the US national security community has been pushing the CYBER matter hard. It has engaged in the less public relations friendly issues like mathematics and encryption, physically securing communications nodes and networks, creating honeypots to attract hackers, digital forensics (breaking into secure hard drives, software) and working with civilian counterparts, sometimes controversially, to secure communications networks.

For those worried about the US government's ability to listen to adversaries, allies, the public, whomever, the Snowden document dumps show just how deep the National Security Agency's wormhole goes. Either you're of the mind that this grossly oversteps the US government's authority, or maybe the nation is better off with the NSA playing God, or, like most, you just don't care.

The US capabilities to tap transoceanic communications cables or satellite communications are well known.

The seriousness with which the US national security community views CYBER can be noted in this comment from a *Defense Science Board* study on CYBER Existentialism

"While the manifestation of a nuclear and cyber attack are very different, in the end, the existential impact to the United States is the same. Existential Cyber Attack is defined as an attack that is capable of causing sufficient wide scale damage for the government potentially to lose control of the country, including loss or damage to significant portions of military and

critical infrastructure: power generation, communications, fuel and transportation, emergency services, financial services, etc."

And just a quasi authoritative US government body claims there is a real danger of an existential CYBER attack, the First Amendment allows a rapier like response from a former government official musing on the fallout from the collapse of electronically connected networks whether by CYBER Attack, lightening bolts or human error.

"Cyber Warfare, Cyber Security and massive Cyber Attacks are alarmist and vastly overrated. Look at what went on in Cyprus in 2013. What could trigger a run on the banks in the United States? Something as simple as shutting down all the ATM's for three days. The resulting panic and long bank lines could irrevocably shake confidence in banks and financial institutions, as Americans find out the significance of all the paperwork they signed when they established their banks accounts, fed by direct deposits. Since many in the country know what the country was like before personal computers and the Internet, they'll do fine. Those people who have exchanged their hearts and brains for computer chips manufactured in Vietnam, and are tethered to Smart Phones and the Cloud, are due for a very rude awakening. You've heard of sleeper agents and moles haven't you? I wonder how many sleeper programs are in the millions of computer chips that are now in every single facet of our lives."

John Stanton can be reached at jstantonarchangel@gmail.com