Obama's Cyber Nuke Dream, Petraeus' Love Child:
Plus Message for US Congressman Hunter

by John Stanton

"Cyber Warfare, Cyber Security and massive Cyber Attacks are alarmist and vastly overrated. Look at what is going on in Cyprus. 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." ***Source***

"The US Army Secretary [McHugh] states that the program converted to DA Civilian and military positions. That was true up till a year ago but now the program is back to being filled by contractors. Why is that? Likely due to having so many legal problems getting rid of people - good and bad. If the separate commands want a social science capability they can build their own team like CENTCOM did. They can provide the funding and the oversight. So many less issues that way and quite the savings! Though I agree with the intent of McHugh's letter - to save an HTS type capability, I disagree with the saving the HTS program. McHugh sites 'commanders' assessments' as reason to save the program. I doubt these assessments or at least their true value.

The House Armed Services Committee should have one of their educated staffers send a request to the team's in theater requesting them to send in the products they have provided their current units for the last six months. A review of such products would show that a majority of such are just regurgitation's of other products and lack any real operationally relevant info that was used in the day-to-day business of the units. The reason is very few, if any, HTS members have left their forward operating bases in the last 6-12 months to do what the program was designed to do. And now that US forces are handing over battle space to their Afghan partners, HTS work is for the most part limited to data-mining the internet and creating what the commanders ask for to support their desired course of action." ***Source***

"I can tell you CGI runs around talking about its $250 million contract with the US Army."

Source

And they rave about the performances on New York City's Broadway?

The critics of theater should aim their witty minds at the actors and plots on the civil-military stage in Washington, DC. The actors there in the capital of the American nation—political, military, corporate, media and academia/think tanks--are in deadly serious roles but they are all trained as comedians it seems. And not very good ones at that. Two plots and the actors involved make the point.

The first is the never ending story of the US Army's Human Terrain System (HTS), a Big Army intelligence program run out of the US Army's G-2 intelligence function. On 15 March 2013 a letter ostensibly written by US Army Secretary John McHugh to Congressman Duncan Hunter (R-CA)--in response to two articles by Tom Vanden Brook of USA Today critical of HTS—seems to have been written by an autonomous software program. Instead, it was likely written by pro-HTS staff members in the US Army's G-2 shop under orders to do so.

HTS, alas, is now viewed by those in the know as an assemblage of things: a toy for the general purpose US Big Army; an intelligence support function whose information is used for targeting rebels in insurgent populations, not understanding them; a chunk of funding that should have been given over to US Army Civil Affairs; and as a corporate money-trough and bureaucratic pit to be avoided by the special forces community. "You can't meddle with the indigenous condition if you do not understand it. We respect the intentions of HTS but when you hand it to corporate America it becomes a pocketbook game or simply putting butts to seats rather than getting and using experienced and qualified individuals in the project...we had success with it is because we respect the boundaries. These [HTS] guys tweak the cultural information gathered to fit policy instead of molding policy to the information. Intelligence types screw it up all the time..." said a veteran member of the special forces community.

Love Child: Never Meant to Be?

A number of sources asked to review McHugh's letter to Hunter indicated that, as one did, "BDE Commanders knew this program was a Petraeus 'Love Child', so of course they aren't going to bad mouth it The team I was on provided nothing beneficial to our command." The General's reach is still in the minds of many in the US Army and his groupies are legion in Washington, DC.

One source had this commentary. "I would ask these commanders to show the research produced by their HTS team that produced the results they are shoveling praise on, and ask if there were no other resources he had available, that could have produced the same results. I remain highly skeptical and contend that HTS devolved into a highly lucrative cash cow for BAE, third-tier academics and marginally effective military personnel. While the concept of HTS is sound, the program was poorly managed, generated a large percentage of useless reports, experienced a high turnover of personnel, and was not cost efficient. To deny that HTS was an intelligence gathering program is perplexing, since, at the end of the day, the information collected, at the behest of the commander, was processed, and used, like intelligence. Furthermore, to say that commanders could not have benefited from more regional subject matter experts and linguists, is as absurd, as saying that an HTS

research report on Pashtun homosexuality has tactical or operational relevance. I guarantee you that within two years, much of the information collected will find its way into Social Science journals, but will be dismissed or heavily criticized as amateurish and irrelevant.

One final point. As the auditors and bean counters review the myriad of programs rushed into Iraq and Afghanistan, you will begin to notice a familiar pattern. High praise for every gadget, initiative, program, and dog and pony show shoved into the fray, all under the auspices of saving lives. From a historical perspective, every single one of these gadgets and programs failed to live up to their expectations. That's why we study history. The only thing that saves lives, is a change in operational tempo, or a change in tactics. Unfortunately, this pattern will repeat itself in the next conflict, as we rush to substitute drones for pilots, lining the pockets of defense contractors and deluding ourselves into thinking we can substitute cold steel for humanism and remote control."

Hey! Congressman Hunter! A Source is Talking Directly to You

"I can tell you that CGI talks about the program as having a $250 million budget, and of course they are aiming for more than that. If I had Duncan Hunter's ear, I would tell him that HTS has no plans to create an infrastructure for dynamic, "game changing," social research, despite having exclusive access to two separate research institutions. The HTS training focuses on teaching the students how to find out what their commander wants to know, then figure out ways to get the information. The teams are not trained for, nor provided with, any research methods to collaborate with other teams. HTS does not employ or work with anybody who can combine multiple sources of data to provide aggregated bigger picture analysis of the work done by HTS teams. The HTS leadership neither recognizes nor values such abilities. If the HTS program is to be valued, that value should be defined as providing commanders with HTS teams that gather sociocultural information specifically for the informational needs of that commander. For anybody who believes HTS teams provide capacities beyond a commander's stated needs, such as preventing a Cold Start," they will be disappointed to find out that HTS does not have any experience with, nor infrastructure for, providing a sociocultural Starting Point.

If the military values HTS for what it actually does, that's fine with me. I do not want people getting the false impression that HTS is providing social researchers with an opportunity to use their skills to avert socioeconomic conflicts and improve long-term relations across cultures. The program has neither the leadership nor infrastructure to do such work. Many staff members like to suggest that HTS is doing such work, but if it did, the HTS leadership and staff would be eagerly collaborating with outside research programs in order to show these results to the public."

Obama's Cyber Aim: Limit Public Access Internet/WWW

So what, exactly, does the public know about HTS in 2013? If one is to believe the US Secretary of the Army, Army G-2, and US Army public affairs, HTS has cleaned its house and all's well now. One can hear them talking: "It's alright, trust us Congressman Hunter and you too, you pesky journalists. And Joyce and John Q Public, have no doubt, because we up here in the lofty heights of leadership—we can see all, know the score and what's best for you." This can also be heard--"Now get out there and find out who those sources are and where the Internet traffic is coming from and

going to. Those &^%$#@! whistle blowers and websites that post this *&^%. We are going to nail them to a barn door and heal and hide 'em. Where is that 1917 Espionage Act in all this! We need a 2013 Cyber Espionage Act to deal with this crap. Call Holder!"

And so President Obama had a nightmare in 2009 in which the Internet, World Wide Web--and the public that takes full advantage of those technologies to bypass the official civilian and military narrative—were like nuclear weapons. In that horrible dream Wikileaks/Julian Assange tortured Obama with bit by bit of information from a lowly US Army private, Bradly Manning, who both appeared in biblical, apocalyptic forms. Even the Washington Post and New York Times, so collusive with the President and his minions, seemed to be riding the horses of doom aiming to trample the pre-Internet/WWW system in which information flows to the public could be nicely controlled. And then he awoke.

Between 2009 and 2013 there has been a tremendous push by President Obama, Big Mainstream Media, the Pentagon and Defense Industrial Base, and businesses large and small, to pound the Cyber security, Cyber Safety threat into the consciousness of the American public. The verbiage and theater used in this process is nearly the same as that used for pushing other threats and, subsequently, waging war at an incredible cost in lives and treasure. Terrorism, Weapons of Mass Destruction and Iraq, Iran; and illicit drugs come to mind. The US is already at war with Iran having inserted computer viruses into the SCADA's of Iran's industrial equipment and assisting in the murders of Iranian scientists. Who knows where other US created Cyber Weapons will create havoc.

Popular thinking is that Cyber War hit the big time in the October 2012 to March 2013 and that the Chinese, Russians, Teenagers, Industrial Espionage Goons, Anonymous, or, say, a Jihad Amok in Cyberspace are the actors that *are in the system* and *are* the cause for the development and deployment of Cyber War strategies, operations and tactics. History is thorny though.

Actually Cyber Thinking began in earnest on 30 September 1993 with the release by the National Communication System of *The Electronic Intrusion Threat to National Security and Emergency Preparedness* and then a second edition on 4 December 1994 (same title). A fascinating visit back to the future can be found in a compendium of conference briefings from 12-13 June 1995 titled *Information Warfare: Addressing the Revolutionary New Paradigm for Modern Warfare.* The conference was co-sponsored by the Technical Marketing Society of America. Even back then, a critical issue was who would control the flow of information in the USA and abroad, In particular, acceptable whistle blowing/trial ballooning; or, more to the point, insider information meant only for insider trades (CIA exchanging information with the New York Times or Washington Post, for example). Information Warriors of old recognized that the Internet/WWW would destabilize the standard operating procedure for leaks making it easier for whistle blowers and the public to work together. Worse still, the spread of information on civilian, military and corporate programs gone wrong/rogue could no longer be confined to one specific area. How to corral independent thinkers? How to stop the spread of news indicting leaders from all sectors of, say, the US crticial infrastructure?

It has taken a full 20 years to push the Cyber Noodle into public prominence. And with the public in a state of Cyber Fear, there is an attempt by government and industry to get back to some sort of

pre-Internet/WWW days through classification and prosecution of those who leak, who aide, somehow, those whose interests are inimical to American national security interests so broadly defined as to make everyone guilty of overtly supporting the Bill of Rights. President Obama's legacy—and that of those who advise him--will be one of collective vengeance against the sun, the light of day.

It was in 2009 when Wikileaks started to seriously upset the information control system in the USA that once allowed relatively few to comfortably controlled the flow of information to the public. In 2009 it published US senatorial campaign documents, Barclay's Bank data and procedures for POW's in Guantanamo Bay, Cuba. By 2010 Wikileaks published US gunship videos and US state department cables which humiliated the Executive and Legislative branches of the US government and with it the many organizations that shape civilian and military life in America. As an example, the State Department cables gave insight into classification practices. Suggested classification/release dates from dates of original publication were laughable. Obama has already sentenced Assange and Manning by public statement. And Assange was merely the reporter of the information as was the New York Times.

In late January of 2013, the New York Times reported that its data had been trawled and compromised by hackers. A few days later on 1 February 2013, the New York news organization pumped more air into the Cyber Bubble with this report: "*After The New York Times reported on Wednesday that its computers as well as those of Bloomberg News had been attacked by Chinese hackers, The Wall Street Journal said on Thursday that it too had been a victim of Chinese cyberattacks. According to people with knowledge of an investigation at The Washington Post, its computer systems were also attacked by Chinese hackers in 2012*." Since budgets are defended in the US Congress during Winter-Spring of each year, this, with remarkable coincidence, set the stage for US government officials who in US Congressional testimony--along with Cyber Defense Contractors civilian and military alike bloated the threat. A Cyber Defense Contractor named Mandiant surfaced and confirmed that the menace behind this enterprise was the Chinese, in Shanghai to be exact. Earlier in January 2013 the head of the US Department of Homeland Security said a Cyber Attack was "immanent."

In March 2013 the Director of National Intelligence said Cyber Crime was a key threat to the US intelligence community. Corporations (banks and financial) went public with their weaknesses. On 28 March 2013 the New York Times had this headline, "Cyberattacks Seem Meant to Destroy, Not Just Disrupt" with this comment *"Security experts who studied the attacks said that it was part of the same campaign that took down the Web sites of JPMorgan Chase, Wells Fargo, Bank of America and others over the last six months. A group that calls itself the Izz ad-Din al-Qassam Cyber Fighters has claimed responsibility for those attacks."*

So in a year or so, Cyber War has apparently become "real." With the nation's critical infrastructure at risk, particularly Big Corporate Media (Walt Disney, News Corporation, WAPO-Kaplan Education), Finance and Banking (JP Morgan, American Express, Bank of America) under electronic attack, the rubber has finally met the road. Coincidentally in March 2013 the *Tallinn Manual on the*

International Law Applicable to Cyber Warfare was produced by NATO. Talk about Cyber Synergy!!

"We are a nation at war" and the post-911 national state of emergency, renewed by Obama each year, has finally found its eternal anchor. Nowhere is this more evident than in the outrageous *Final Report of the Defense Science Board (DSB) Task Force on Resilient Military Systems*. No one doubts that Cyber Security and Physical Security should be improved, considered more seriously in civilian and military budgets. This is particularly true with the problem of counterfeit software, hardware and telecommunications gear. But why does the US government allow corporations to outsourcing the manufacture of such critical gear to foreign countries? At any rate these matters are responsibilities that fall on the human, not the machine as the latter is just a tool. But to equate an existential Nuclear Attack on the USA with an existential Cyber Attack is, well, comedy. ARPANET, which the Internet is based on, was designed for heavy duty military communications redundancy. The Internet is far more robust and adaptable that the 1960's ARPANET ever was. The bad guys need it functioning as much as the good and neutral parties.

"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."

Who can say how many acrid HTS programs there are in government? How many Cyber Terrain, Cyber Counterinsurgency projects are in the works that will be managed incompetently? Who knows where on the Cyber Continent the US national security apparatus will be roaming and collecting information?

It deserves repeating: "Unfortunately, this pattern will repeat itself in the next conflict, as we rush to substitute drones for pilots, lining the pockets of defense contractors and deluding ourselves into thinking we can substitute cold steel for humanism and remote control."

And lives will be shattered or lost.

John Stanton is a Virginia based writer specializing in national security matters. His recent book the Raptor's Eye is at Amazon. Reach him at cioran123@yahoo.com