

American World View is WAR - the Primary cause for its Impending Demise

by Kismo *Friday, Jul 15 2011, 3:01am*

international / mass media / commentary

Internet Declared a War Zone

A recently released Pentagon report has declared the Internet a WAR ZONE -- well, of course it has, it's a POV snapshot from the military, a distorted reality the US Banking/Military/Corporate complex is unsuccessfully attempting to impose on the world population in order to justify and continue on its mass murdering, plundering course. I mean, how could the US even attempt to justify killing millions of civilians, ruining/enslaving European nations and sticking its destructive nose into EVERYBODY'S business without declaring War on almost everything?

It's CLEARLY a pathological world view characteristic of a nation essentially at war with itself!

The plutocrats have plundered the nation and are now plundering government coffers in the form of TARP, bailouts, stimulus loans etc., while the poor eat shit and learn to like it! However, experts and housewives alike are aware it can't go on as there is nothing financially substantial supporting it any longer.

America's policy course has forced it to overprint/supply worthless fiat greenbacks; an insane tactic that will ensure the rapid end to the global economy, which is currently on life support - actually, it is already dead; there is no economy outside brazen economic Imperialism and the parasitic plunder of weaker nations' sovereign wealth. However, the world seems to have had enough bullying from lunatic Corporatists and Uncle Sam, so too the shit-eating American population - slow to wake up but wake they eventually did!

Consider the psychopathic mentality that led to the current situation; the American obsession with declaring WAR on everything from drugs, crime, to in-grown toenails! I would add that America has LOST the wars on drugs and crime for obvious reasons; those nefarious enterprises have supplied Wall St banking interests with an extended life in the form of trillions in cash liquidity which had nowhere to go but back into the system. However, those ill-gotten gains will soon also be targeted by the REAL criminal elite - Corporatists and Wall St. Banksters. Al Capone got it right in the 30's; he described himself as a small fry hoodlum in comparison to the REAL tuxedo-wearing criminals that rule America.

America has lost all its social wars and is now losing military wars against elusive ephemeral enemies it is unable to identify - how much more difficult to identify ghosts in cyber space - IMPOSSIBLE?

The remedy for the Pentagon, as demonstrated almost daily by its CRIMINAL civilian killing Drone attacks, is declaring war on ALL suspects and hope you eventually hit a few real enemies during the missile melee. The obvious problem with that tactic is reflected in the statistics of civilian deaths, which authorities are a pains to HIDE! Nevertheless, the HUGE number of innocent deaths ensures defeat for a much reviled, criminal, pariah nation, which CLEARLY places no value whatsoever on (innocent) human life.

The Pentagon has described various States, groups and 'stateless actors' as hostile, but FAILS to ask WHY people with much better things to do are obliged to defeat the evil scourge that plagues the entire WORLD.

Common sense dictates the USA is following a SELF-DESTRUCTIVE strategy - it forgot that cyber space is the ultimate ASYMMETRICAL 'theatre' and that people value their national and personal SOVEREIGNTY - I'll repeat those words so Pentagon goons can 'legitimately' waste more time analysing the processes involved in their inevitable defeat - 'Asymmetry and Sovereignty,' have you got it now, morons?

It is widely known that Government hackers are fifth rate; the best of the best by nature, instinctively oppose ALL criminal empires and their destructive, JOYLESS world views. Drats, another war lost!

Report from 'The Hill' follows:

Pentagon declares the Internet a war domain

by John T. Bennett

The Pentagon released a long-promised cybersecurity plan Thursday that declares the Internet a domain of war but does not spell out how the U.S. military would use the Web for offensive strikes.

The Defense Department's first-ever plan for cyberspace states that DOD will expand its ability to thwart attacks from other nations and groups, beef up its cybersecurity workforce and expand collaboration with the private sector.

Like major corporations and the rest of the federal government, the military "depends on cyberspace to function," the DOD strategy states. The U.S. military uses cyberspace for everything from carrying out military operations to sharing intelligence data internally to managing personnel assignments.

"The department and the nation have vulnerabilities in cyberspace," the document states. "Our reliance on cyberspace stands in stark contrast to the inadequacy of our cybersecurity."

Other nations "are working to exploit DOD unclassified and classified networks, and some foreign intelligence organizations have already acquired the capacity to disrupt elements of DOD's information infrastructure," the plan states. "Moreover, non-state actors increasingly threaten to penetrate and disrupt DOD networks and systems."

Groups are capable of this largely because "small-scale technologies" that have "an impact disproportionate to their size" are relatively inexpensive and readily available.

The Pentagon plans to focus heavily on three areas under the new strategy: The theft or exploitation of data, attempts to deny or disrupt access to U.S. military networks, and any attempts to "destroy or degrade networks or connected systems."

Another problem highlighted in the strategy is a baked-in threat: "The majority of information technology products used in the United States are manufactured and assembled overseas."

To address those issues, DOD revealed a multi-pronged approach.

As expected and foreshadowed by Pentagon officials' comments in recent years, the plan etches in stone that cyberspace is now an "operational domain" just as land, air, sea and space have been for decades for the military.

"This allows DOD to organize, train and equip for cyberspace" as in those other areas, the plan states. It also notes the 2010 establishment of U.S. Cyber Command to oversee all DOD work in the cyberspace.

By crafting a this strategy, "the Department of Defense is acknowledging what all observers of the IT revolution have known for years: cyberwar is already a reality," Lexington Institute analyst Daniel Goure, a former Army official, wrote recently.

"The publication of the cyberwar strategy may also help jumpstart a long-postponed public debate over the nature of such a war and how it should be deterred, if possible, or fought if necessary," Goure wrote. "The last technology to revolutionize warfare to the same extent as IT is doing was that which led to the creation of nuclear weapons."

The second leg of the plan is to employ new defensive ways of operating in cyberspace, first by enhancing the DOD's "cyber hygiene." That term covers ensuring that data on military networks remains secure, using the Internet wisely and designing systems and networks to guard against cyberstrikes.

The military will continue its "active cyber defense" approach of "using sensors, software and intelligence to detect and stop malicious activity before it can affect DOD networks and systems." It also will look for new "approaches and paradigms" that will include "development and integration ... of mobile media and secure cloud computing."

The plan devotes more than a page to mostly underscore efforts long under way to work with other government agencies and the private sector.

Notably, it calls the Department of Homeland Security the lead for "interagency efforts to identify and mitigate cyber vulnerabilities in the nation's critical infrastructure." Some experts have warned against DOD overstepping on domestic cybersecurity.

The Pentagon also announced a new pilot program with industry designed to encourage companies to "voluntarily [opt] into increased sharing of information about malicious or unauthorized cyber activity."

The strategy calls for a larger DOD cybersecurity workforce.

One challenge, Pentagon experts say, will be attracting top IT talent because the private sector can pay much larger salaries — especially in times of shrinking defense budgets. To that end, "DOD will focus on the establishment of dynamic programs to attract talent early," the plan states.

On IT acquisition, the plan lays out several changes, including: faster delivery of systems; moving to incremental development and upgrading instead of waiting to buy "large, complex systems"; and improved security measures.

Finally, the strategy states an intention to work more closely with “small- and medium-sized business” and “entrepreneurs in Silicon Valley and other U.S. technology innovation hubs.”

The reaction from Capitol Hill in the immediate wake of the plan’s unveiling was mostly muted. Cybersecurity is not a polarizing political issue in the way some defense issues are, like missile defense.

Claude Chafin, a spokesman for House Armed Services Committee Chairman Buck McKeon (R-Calif.), called the strategy “the next step in an important national conversation on securing critical systems and information, one that the Armed Services Committee has been having for some time.”

That panel already has set up its own cybersecurity task force, which Chafin said would “consider this [DOD] plan in its sweeping review of America’s ability to defend against cyber attacks.”

As the Pentagon tweaks its approaches to cybersecurity, Senate Armed Services Committee ranking member John McCain (R-Ariz.) on Wednesday wrote Senate leaders saying that chamber must as well. McCain asked Majority Leader Harry Reid (D-Nev.) and Minority Leader Mitch McConnell (R-Ky.) to establish a temporary Select Committee on Cyber Security and Electronic Intelligence Leaks.

“Cybersecurity proposals have been put forth by numerous Senate committees, the White House and various government agencies; however, the Senate has yet to coalesce around one comprehensive proposal that adequately addresses the government-wide threats we face,” McCain’s office said in a statement. “A select committee would be capable of drafting comprehensive cybersecurity legislation quickly without needing to work through numerous and in some cases competing committees of jurisdiction.”

Copyright applies to external text.

<http://tinyurl.com/5ucgopp>

Cleaves Alternative News. <http://cleaves.lingama.net/news/story-2623.html>