GlobalResearch
Center for Research on Globalization

The Pentagon's Cyber Command: Civilian Infrastructure is a "Legitimate" Target

By Tom Burghardt
Global Research, April 18, 2010
Antfascist Calling... 18 April 2010

Region: USA
Theme: Police State & Civil Rights, US NATO War Agenda

When U.S. Secretary of Defense Robert M. Gates launched Cyber Command (CYBERCOM) last June, the memorandum authorizing its stand-up specified it as a new "subordinate unified command" under U.S. Strategic Command (STRATCOM), one that "must be capable of synchronizing warfighting effects across the global security environment as well as providing support to civil authorities and international partners."

As Antifascist Calling reported at the time, Gates chose Lt. General Keith Alexander, the current Director of the National Security Agency (NSA), to lead the new DOD entity. The agency would be based in Ft. Meade, Maryland, where NSA headquarters are located and the general would direct both organizations.

In that piece I pointed out that STRATCOM is the successor organization to Strategic Air Command (SAC). One of ten Unified Combatant Commands, STRATCOM's brief includes space operations (military satellites), information warfare, missile defense, global command and control, intelligence, surveillance and reconnaissance (ISR), as well as global strike and strategic deterrence, America's first-strike nuclear arsenal.

Designating CYBERCOM a STRATCOM branch all but guarantees an aggressive posture. As an organization that will unify all military cyber operations from various service branches under one roof, CYBERCOM will coordinate for example, Air Force development of technologies to deliver what are called "D5 effects" (deceive, deny, disrupt, degrade and destroy).

Ostensibly launched to protect military networks against malicious attacks, the command's offensive nature is underlined by its role as STRATCOM's operational cyber wing. In addition to a defensive brief to "harden" the "dot-mil" domain, the Pentagon plan calls for an offensive capacity, one that will deploy cyber weapons against imperialism's adversaries.

As a leading growth sector in the already-massive Military-Industrial-Security-Complex, the cyberwar market is hitting the corporate "sweet spot" as the Pentagon shifts resources from Cold War "legacy" weapons' systems into what are perceived as "over-the-horizon" offensive capabilities.

In association with STRATCOM, the Armed Forces Communications and Electronics Association (AFCEA), will hold a Cyberspace Symposium, "Ensuring Commanders' Freedom of Action in Cyberspace," May 26-27 in Omaha, Nebraska.

Chock-a-block with heavy-hitters in the defense and security world such as Lockheed Martin, HP, Booz Allen Hamilton, CACI, Cisco, CSC, General Dynamics, QinetiQ, Raytheon and the

spooky MITRE Corporation, the symposium seeks to foster "innovation and collaboration between the private sector and government to delve into tough cyber issues." The shin-dig promises to "feature defense contractors and government agencies showcasing their solutions to cyberspace and cyber warfare issues."

During pro forma hearings before the Senate Armed Services Committee (SASC) April 15, Alexander's testimony was short on specifics, as were his written responses to "Advance Questions" submitted to the general by the SASC.

During Thursday's testimony, Alexander told the Senate panel that the command "isn't about efforts to militarize cyberspace," but rather "is about safeguarding the integrity of our military's critical information systems."

"If confirmed" Alexander averred, "I will operate within applicable laws, policies and authorities. I will also identify any gaps in doctrine, policy and law that may prevent national objectives from being fully realized or executed."

What those "national objectives" are and how they might be "executed" are not publicly spelled out, but can be inferred from a wealth of documents and statements from leading cyberwar proponents.

As we will explore below, despite hyperbole to the contrary, CYBERCOM represents long-standing Pentagon plans to militarize cyberspace as part of its so-called "Revolution in Military Affairs" and transform the internet into an offensive weapon for waging aggressive war.

"Switching Cities Off"

While we do not know how Pentagon assets will be deployed, we can be certain their destructive potential is far-reaching. We can infer however, that CYBERCOM possesses the capacity for inflicting irreparable harm and catastrophic damage on civilian infrastructure, and that power grids, hospitals, water supply systems, financial institutions, transportation hubs and telecommunications networks are exquisitely vulnerable.

The potential for catastrophic violence against cities and social life in general, has increased proportionally to our reliance on complex infrastructure. Indeed, most of the networks relied upon for sustaining social life, particularly in countries viewed as adversaries by the United States would be susceptible to such attacks.

In densely populated cities across Africa, Asia, Latin American and the Middle East, even a small number of directed attacks on critical infrastructural hubs could cause the entire network to collapse. The evidence also suggests that the Pentagon fully intends to field weapons that will do just that.

As the National Journal reported in November, in May 2007, "President Bush authorized the National Security Agency, based at Fort Meade, Md., to launch a sophisticated attack on an enemy thousands of miles away without firing a bullet or dropping a bomb."

According to investigative journalist Shane Harris, during the Iraq "surge" Director of National Intelligence Mike McConnell, requested and received an order from President Bush for an "NSA cyberattack on the cellular phones and computers that insurgents in Iraq were using to plan roadside bombings."

While corporate media, the Pentagon and the security grifters who stand to make billions of dollars hyping the "cyberwar threat" to gullible congressional leaders and the public, the DOD, according to Harris, "have already marshaled their forces."

Bob Gourley, who was the chief technology officer for the Defense Intelligence Agency told Harris: "We have U.S. warriors in cyberspace that are deployed overseas and are in direct contact with adversaries overseas," and that these experts already "live in adversary networks."

While the specter of a temporary "interruption of service" may haunt modern cities with blackout or gridlock, a directed attack focused on bringing down the entire system by inducing technical malfunction across the board, would transform "the vast edifices of infrastructure" according to geographer and social critic Stephen Graham, into "so much useless junk."

In his newly-published book, Cities Under Siege, Graham discusses the effects of post-Cold War U.S./NATO air bombing campaigns in Iraq, Afghanistan and the former Yugoslavia as a monstrous instrumentality designed to inflict maximum damage and thereby coerce civilian populations into abandoning resistance to the imperialist hyperpower: the United States.

Much the same can be said of America's "stationary aircraft carrier" in the Middle East, Israel, during its murderous bombing campaign and ground invasion of Gaza during 2008-2009, which similarly targeted civilian infrastructure, reducing it to rubble.

"The effects of urban de-electrification" Graham writes, "are both more ghastly and more prosaic: the mass death of the young, the weak, the ill, and the old, over protracted periods of time and extended geographies, as water systems and sanitation collapse and water-borne diseases run rampant. No wonder such a strategy has been called a 'war on public health,' an assault which amounts to 'bomb now, die later'."

Although critics such as James Der Derian (see: Virtuous War) argue that "new forms of control and governance" are made possible by the modern surveillance state and that "the speed of interconnectivity that the computer enables has, more than any other innovation in warfare from the stirrup to gunpowder to radar to nukes, shifted the battlefield away from the geopolitical to the electromagnetic," exactly the opposite is the case.

Searching for "clean," "sanitized" modes of waging high-tech, low casualty war (for the aggressors), U.S. Cyber Command has been stood-up precisely to deliver the means that enable America's corporate and political masters to "switch cities off" at will, as a tool of economic-political domination.

In this respect, the "electromagnetic" is fully the servant of the "geopolitical," or as Guy Debord reminds us in The Society of the Spectacle: "The current destruction of the city is thus merely one more reflection of humanity's failure, thus far, to subordinate the economy to historical consciousness; of society's failure to unify itself by reappropriating the powers that have been alienated from it."

Part of that "alienation" resides in the chimerical nature of imperialism's quest for high-tech "silver bullets" to assure its continued domination of the planet, despite evidence to contrary in the form of the slow-motion meltdown and collapse of the capitalist economy. The fact is, despite the decidedly "low-tech," though highly-effective, resistance of the

people of Iraq, Palestine and Afghanistan, our masters will continue to pour billions of dollars into such weapons systems to stave off their "rendezvous with history."

While Pentagon Press Secretary Geoff Morrell went to great lengths last year to downplay the offensive role envisaged for Cyber Command, others within the defense bureaucracy are far more enthusiastic.

In a 2008 piece published by Armed Forces Journal, Col. Charles W. Williamson wrote that "America needs a network that can project power by building an af.mil robot network (botnet) that can direct such massive amounts of traffic to target computers that they can no longer communicate and become no more useful to our adversaries than hunks of metal and plastic. America needs the ability to carpet bomb in cyberspace to create the deterrent we lack."

Alexander's equivocal written responses were hardly comforting, nor did they blunt criticism that the Pentagon fully intends to stand-up an electromagnetic equivalent of Strategic Air Command. While promising that CYBERCOM would be "sensitive to the ripple effects from this kind of warfare," as The New York Times delicately put it, Alexander sought to blunt criticism by averring that the Pentagon "would honor the laws of war that govern traditional combat in seeking to limit the impact on civilians."

In written responses to Senate, Alexander went to great lengths to assure the SASC that military actions would comply with international laws that require conformity with principles of military necessity and proportionality.

However, as the Times pointed out, Alexander agreed with a question submitted by the Senate that "the target list would include civilian institutions and municipal infrastructure that are essential to state sovereignty and stability, including power grids, banks and financial networks, transportation and telecommunications."

During questioning by SASC Chairman Carl Levin (D-MI) Thursday, how CYBERCOM would respond to an attack "through computers that are located in a neutral country," Alexander was far more ambiguous. He responded that would "complicate" matters, particularly when it came to the critical question of "attribution."

Despite matters being "complicated" by the fog of war, Alexander didn't rule out an attack on a presumably "neutral" country, even one that unwittingly serves as a "path through."

"Offensive cyber weapons" Alexander wrote, "would only be authorized under specific lawful orders by the [Defense Secretary] and the president and would normally come with supplemental rules of engagement."

While true as far as it goes (which isn't very far!) Alexander's boss, General Kevin Chilton, STRATCOM's commander suggested last year that "the White House retains the option to respond with physical force–potentially even using nuclear weapons–if a foreign entity conducts a disabling cyber attack against U.S. computer networks." (emphasis added)

According to Global Security Newswire, during a Defense Writers Group breakfast last May Chilton told journalists, "I think you don't take any response options off the table from an attack on the United States of America. Why would we constrain ourselves on how we respond?"

Chilton went on to say that “I think that’s been our policy on any attack on the United States of America. And I don’t see any reason to treat cyber any differently. I mean, why would we tie the president’s hands? I can’t. It’s up to the president to decide.”

Hardly comforting words.

In response to an SASC query, Alexander wrote that as Commander his duties include “executing the specified cyberspace missions” to “secure our freedom of action in cyber space.”

Among other things, those duties entail “integrating cyberspace operations and synchronizing warfighting effects across the global security environment.” According to it’s charter, the command will “direct global information grid operations and defense” and execute “full-spectrum military cyberspace operations.”

The command will serve “as the focal point for deconfliction of DOD offensive cyberspace operations;” in other words, it will coordinate and act as the final arbiter amongst the various armed branches which possess their own offensive cyber capabilities.

In the Pipeline

Contemporary military doctrine in the United States, but also in Israel, has emphasized the use of overwhelming force as a means to eradicate civilian infrastructure and break a population’s resistance, what Graham has called “the systematic demodernization and immobilization of entire societies classified as adversaries.”

Whether such force is applied through “traditional” means, aerial bombing preceded or followed by crippling economic sanctions as in Iraq and Palestine, or by the deployment of more “modern” means, cyberwar, state terror has as its primary target the civilian population and crafts its tactics so as to ensure maximal levels of psychological coercion.

This is fully consonant with the Pentagon’s goal to transform cyberspace into an offensive military domain. In a planning document, since removed from the Air Force web site, theorists averred:

> Cyberspace favors offensive operations. These operations will deny, degrade, disrupt, destroy, or deceive an adversary. Cyberspace offensive operations ensure friendly freedom of action in cyberspace while denying that same freedom to our adversaries. We will enhance our capabilities to conduct electronic systems attack, electromagnetic systems interdiction and attack, network attack, and infrastructure attack operations. Targets include the adversary’s terrestrial, airborne, and space networks, electronic attack and network attack systems, and the adversary itself. As an adversary becomes more dependent on cyberspace, cyberspace offensive operations have the potential to produce greater effects. (Air Force Cyber Command, “Strategic Vision,” no date, emphasis added)

U.S. campaigns in Afghanistan, Iraq and Yugoslavia and Israeli aggressive wars against Gaza, the West Bank and Lebanon, demonstrate forcefully that contemporary military doctrine now strives to develop the capacity to systematically degrade, as a means of controlling through threats or actual attacks, the infrastructural “glue” that bind entire nations together. There can be no doubt that the Air Force’s “Strategic Vision” is now fully

integrated into CYBERCOM.

As well, with increasing reliance by the state and its military on high-tech methods of waging war for economic-political-social domination, the self-same methods are appropriated and deployed within heimat societies themselves. Hence, escalating securitization schemes (warrantless wiretapping, watch listing and indexing of "suspect" citizens) are the handmaidens of a generalized militarization of daily life.

What then, are some of the features and future weapons systems being explored by CYBERCOM and their corporate partners? The SASC as part of its confirmation process of General Alexander, has provided a useful summary, Building Cyberwarfare Capabilities in Public Documents.

If anything, the examples cited below clearly demonstrate that CYBERCOM is quietly seeing to it that the "mismatch between our technical capabilities to conduct operations and the governing laws and policies," as Alexander wrote to the SASC, for waging aggressive cyberwar will soon be resolved.

Dominant Cyber Offensive Engagement and Supporting Technology
BAA-08-04-RIKA [BAA, Broad Agency Announcement]
Agency: Department of the Air Force
Office: Air Force Materiel Command
Location: AFRL [Air Force Research Laboratory]-Rome Research Site
Posted on fbo.gov: June 13, 2008

"Solutions to basic and applied research and engineering for the problems relating to Dominant Cyber Offensive Solutions to basic and applied research and engineering for the problems relating to Dominant Cyber Offensive Engagement and Supporting Technology are sought. This includes high risk, high payoff capabilities for gaining access to any remotely located open or closed computer information systems; these systems enabling full control of a network for the purposes of information gathering and effects based operations."

"Also, we are interested in technology to provide the capability to maintain an active presence within the adversaries information infrastructure completely undetected. Of interest are any and all techniques to enable stealth and persistence capabilities on an adversaries infrastructure. This could be a combination of hardware and/or software focused development efforts. Following this, it is desired to have the capability to stealthily exfiltrate information from any remotely-located open or closed computer information systems with the possibility to discover information with previously unknown existence. Any and all techniques to enable exfiltration techniques on both fixed and mobile computing platforms are of interest. Consideration should be given to maintaining a 'low and slow' gathering paradigm in these development efforts to enable stealthy operation. Finally, this BAA's objective includes the capability to provide a variety of techniques and technologies to be able to affect computer information systems through Deceive, Deny, Disrupt, Degrade, Destroy (D5) effects."

Air Force PE 0602788F: Dominant Information Technology

FY 2011 Base Plans: "Continue development of information system access methods and development of propagation techniques. Continue development of stealth and persistence technologies. Continue development of the capability to exfiltrate information from

adversary information systems for generation of actionable CybINT. Continue technology development for preparation of the battlefield and increased situational awareness and understanding. Continue development of technology to deliver D5 effects. Continue development of autonomic technologies for operating within adversary information systems. Continue development of techniques for covert communication among agents operating within adversary information systems. Continue analysis of proprietary hardware and software systems to identify viable means of access and sustained operations within the same. Continue development of a publish/subscribe architecture for exchange and exfiltration of information while operating within development of a publish/subscribe architecture for exchange and exfiltration of information while operating within adversary information systems. Initiate development of techniques to deliver PsyOps via cyber channels. Develop deception techniques to allow misdirection and confusion of adversary attempts to probe and infiltrate AF systems."

As Washington Technology reported in February, "Lockheed Martin Corp. will continue to work with the Defense Advanced Research Projects Agency to help develop a governmentwide cybersecurity initiative under a $30.8 million contract."

That initiative, the National Cyber Range will "provide a revolutionary, safe, fully automated and instrumented environment for U.S. cybersecurity research organizations to evaluate leap-ahead research, accelerate technology transition, and enable a place for experimentation of iterative and new research directions," according to DARPA.

Target, acquired...

Articles by: Tom Burghardt
http://antifascist-calling.blogspot.com/