RFID: Surveillance-Beacon warfare soon to be imposed on YOU!

by Tom Burghardt via Kismo - Antifascist Calling... *Thursday, Jun 11 2009, 8:38am*
international / peace/war / other press

CIA and Pentagon Deploy RFID "Death Chips."

> What Pentagon theorists describe as a "Revolution in Military Affairs" (RMA) leverages information technology to facilitate (so they allege) command decision-making processes and mission effectiveness, i.e. the waging of aggressive wars of conquest.

RFID chip embedded in new Oz passport

It is assumed that U.S. *technological* preeminence, referred to euphemistically by *Airforce Magazine* as "compressing the kill chain," will assure American *military* hegemony well into the 21st century. Indeed a 2001 study, *Understanding Information Age Warfare*, brought together analysts from a host of Pentagon agencies as well as defense contractors Boeing, Booz Allen Hamilton and the MITRE Corporation and consultants from ThoughtLink, Toffler Associates and the RAND Corporation who proposed to do just.

As a result of this and other Pentagon-sponsored research, military operations from Afghanistan to Iraq and beyond aim for "defined effects" through "kinetic" and "non-kinetic" means: leadership decapitation through preemptive strikes combined with psychological operations designed to pacify (terrorize) insurgent populations. This deadly combination of high- and low tech tactics is the dark heart of the Pentagon's Unconventional Warfare doctrine.

In this respect, "network-centric warfare" advocates believe U.S. forces can now dominate entire societies through ubiquitous surveillance, an always-on "situational awareness" maintained by cutting edge sensor arrays as well as by devastating aerial attacks by armed drones, warplanes and Special Forces robosoldiers.

Meanwhile on the home front, urbanized RMA in the form of ubiquitous CCTV systems deployed on city streets, driftnet electronic surveillance of private communications and radio-frequency identification (RFID) chips embedded in commodities are *all* aspects of a control system within securitized societies such as ours.

As *Antifascist Calling* has written on more than one occasion, contemporary U.S. military operations are conceived as a branch of capitalist management theory, one that shares more than a passing resemblance to the organization of corporate entities such as Wal-Mart.

Similar to RMA, commodity flows are mediated by an ubiquitous surveillance of products--and consumers--electronically. Indeed, Pentagon theorists conceive of "postmodern" warfare as just another manageable network enterprise.

The RFID (Counter) Revolution

Radio-frequency identification tags are small computer chips connected to miniature antennae that can be fixed to or implanted within physical objects, including human beings. The chip itself contains an Electronic Product Code that can be read each time a reader emits a radio signal.
The chips are subdivided into two distinct categories, passive or active. A passive tag doesn't contain a battery and its read range is variable, from less than an inch to twenty or thirty feet. An active tag on the other hand, is self-powered and has a much longer range. The data from an active tag can be sent directly to a computer system involved in inventory control--or weapons targeting.

It is hardly surprising then, that the Pentagon and the CIA have spent "hundreds of millions of dollars researching, developing, and purchasing a slew of 'Tagging tracking and locating' (TTL) gear," *Wired* reports.

Long regarded as an urban myth, the military's deployment of juiced-up RFID technology along the AfPak border in the form of "tiny homing beacons to guide their drone strikes in Pakistan," has apparently moved out of the laboratory. "Most of these technologies are highly classified" *Wired* reveals,

> But there's enough information in the open literature to get a sense of what the government is pursuing: laser-based reflectors, super-strength RFID tags, and homing beacons so tiny, they can be woven into fabric or into paper.
>
> Some of the gadgets are already commercially available; if you're carrying around a phone or some other mobile gadget, you can be tracked--either through the GPS chip embedded in the gizmo, or by triangulating the cell signal. Defense contractor EWA Government Systems, Inc. makes a radio frequency-based "Bigfoot Remote Tagging System" that's the size of a couple of AA batteries. But the government has been working to make these terrorist tracking tags even smaller. (David Hambling and Noah Shachtman, "Inside the Military's Secret Terror-Tagging Tech," *Wired*, June 3, 2009)

Electronic Warfare Associates, Inc. (EWA) is a little-known Herndon, Virginia-based niche company comprised of nine separate operating entities "each with varying areas of expertise," according to the firm's website. Small by industry standards, EWA has annual revenue of some $20 million, *Business First* reports. According to *Washington Technology*, the firm provides "information technology, threat analysis, and test and evaluation applications" for the Department of Defense. The majority of the company's products are designed for signals intelligence and surveillance operations, including the interception of wireless communications. According to EWA, its Bigfoot Remote Tagging System is "ideal" for "high-value target" missions and intelligence operations.

EWA however, isn't the only player in this deadly game. The Defense Advanced Research Projects Agency (DARPA), the Pentagon's geek-squad, has been developing "small, environmentally robust, retro reflector-based tags that can be read by both handheld and airborne sensors at significant

ranges," according to a presentation produced by the agency's Strategic Technology Office (STO).

Known as "DOTS," Dynamic Optical Tags, DARPA claims that the system is comprised of a series of "small active retroreflecting optical tags for 2-way data exchange." The tags are small, 25x25x25 mm with a range of some 10 km and a two month shelf-life; far greater than even the most sophisticated RFID tags commercially available today. Sold as a system possessing a "low probability of detection," the devices can be covertly planted around alleged terrorist safehouses--or the home of a political rival or innocent citizen--which can then be targeted at will by Predator or Reaper drones.

The Guardian revealed May 31 that over the last 18 months more than 50 CIA drone attacks have been launched against "high-value targets." The Pentagon claims to have killed nine of al-Qaeda's top twenty officials in north and south Waziristan. "That success" *The Guardian* avers, "is reportedly in part thanks to the mysterious electronic devices, dubbed 'chips' or 'pathrai' (the Pashto word for a metal device), which have become a source of fear, intrigue and fascination."

According to multiple reports by Western and South Asian journalists, CIA paramilitary officers or Special Operations commandos pay tribesmen to plant the devices adjacent to farmhouses sheltering alleged terrorists. "Hours or days later" *The Guardian* narrates, "a drone, guided by the signal from the chip, destroys the building with a salvo of missiles. 'There are body parts everywhere,' said Wazir, who witnessed the aftermath of a strike."

> It is a high-tech assassination operation for one of the world's most remote areas.
>
> The pilotless aircraft, Predators or more sophisticated Reapers, take off from a base in Baluchistan province.
>
> But they are guided by a joystick-wielding operator half a world away, at a US air force base 35 miles north of Las Vegas. (Declan Walsh, "Mysterious 'chip' is CIA's latest weapon against al-Qaida targets hiding in Pakistan's tribal belt," *The Guardian*, May 31, 2009)

But while American operators may get their kicks unloading a salvo of deadly missiles on unsuspecting villagers thousands of miles away, what happens when CIA "cut-outs" get it wrong?

According to investigative journalist Amir Mir, writing in the Lahore-based newspaper *The News*, "of the sixty cross-border Predator strikes...between January 14, 2006 and April 8, 2009, only 10 were able to hit their actual targets, killing 14 wanted al-Qaeda leaders, besides perishing 687 innocent Pakistani civilians. The success percentage of the US Predator strikes thus comes to not more than six percent."

So much for "precision bombing." But as CIA Director Leon Panetta recently told Congress, continued drone attacks are "the only game in town."

A "game" likely to reap tens of millions of dollars for enterprising corporate grifters. According to *Wired*, Sandia National Laboratories are developing "Radar Responsive" tags that are "a long-range version of the ubiquitous stick-on RFID tags used to mark items in shops."

A Sandia "Fact Sheet" informs us that "Radar-tag applications include battlefield situational awareness, unattended ground sensors data relay, vehicle tracking, search and recovery, precision targeting, special operations, and drug interdiction." Slap a tag on the car or embed one of the devilish devices in the jacket of a political dissident and bingo! instant "situational awareness" for

Pentagon targeting specialists.

As Sandia securocrats aver, Radar Responsive tags can light up and locate themselves from twelve miles away thus providing "precise geolocation of the responding tag independent of GPS." But "what happens in Vegas" certainly won't stay there as inevitably, these technologies silently migrate into the *heimat*.

Homeland Security: Feeding the RFID Beast

One (among many) firms marketing a spin-off of Sandia's Radar Responsive tags is the Washington, D.C.-based Gentag. With offices in The Netherlands, Brazil and (where else!) Sichuan, China, the world capital of state-managed surveillance technologies used to crush political dissent, Gentag's are a civilian variant first developed for the Pentagon.

According to Gentag, "the civilian version (which still needs to be commercialized) is a lower power technology suitable for commercial civilian applications, including use in cell phones and wide area tracking." Conveniently, "Mobile reader infrastructure can be set up anywhere (including aircraft) or can be fixed and overlaid with existing infrastructure (e.g. cell phone towers)."

One member of the "Gentag Team" is Dr. Rita Colwell, the firm's Chief Science Advisor. Headquartered at the University of Maryland, College Park and the Johns Hopkins Bloomberg School of Public Health, according to a blurb on Gentag's website "Colwell will lead development of detection technologies that can be combined with cell phones for Homeland Security applications."

Another firm specializing in the development and marketing of RFID surveillance technologies is Inkode. The Vienna, Virginia-based company specializes in the development of low power devices "for integration into all types of products." According to a 2003 article in the *RFID Journal*, the firm has developed a method for "embedding very tiny metal fibers in paper, plastic and other materials that radio frequency waves can penetrate. The fibers reflect radio waves back to the reader, forming what Inkode calls a 'resonant signature.' These can be converted into a unique serial number."

Indeed, the fibers can be embedded in "paper, airline baggage tags, book bindings, clothing and other fabrics, and plastic sheet," *Wired* reported. "When illuminated with radar, the backscattered fields interact to create a unique interference pattern that enables one tagged object to be identified and differentiated from other tagged objects," the company says.
"For nonmilitary applications, the reader is less than 1 meter from the tag. For military applications, the reader and tag could theoretically be separated by a kilometer or more." The perfect accoutrement for a drone hovering thousands of feet above a target.

More recently, the *RFID Journal* reports that Queralt, a Wallingford, Connecticut-based start-up, received a Department of Homeland Security grant to design "an intelligent system that learns from data collected via RFID and sensors."

Tellingly, the system under development builds on the firm's "existing RFID technology, as well as an integrated behavioral learning engine that enables the system to, in effect, learn an individual's or asset's habits over time. The DHS grant was awarded based on the system's ability to track and monitor individuals and assets for security purposes," the *Journal* reveals.

And with a booming Homeland Security-Industrial-Complex as an adjunct to the defense industry's monetary black hole, its no surprise that Michael Queralt, the firm's cofounder and managing director told the publication, "The reason this development is interesting to us is it is very close to our heart in the way we are going with the business. We are developing a system that converges

physical and logical, electronic security."

> The core of Queralt's system is the behavioral engine that includes a database, a rules engine and various algorithms. Information acquired by reading a tag on an asset or an individual, as well as those of other objects or individuals with which that asset or person may come into contact, and information from sensors (such as temperature) situated in the area being monitored, are fed into the engine. The engine then logs and processes the data to create baselines, or behavioral patterns. As baselines are created, rules can be programmed into the engine; if a tag read or sensor metric comes in that contradicts the baseline and/or rules, an alert can be issued. Development of the behavioral engine is approximately 85 percent done, Queralt reports, and a prototype should be ready in a few months. (Beth Bacheldor, Queralt Developing Behavior-Monitoring RFID Software," *RFID Journal*, April 23, 2009)

Creating a "behavior fingerprint," Queralt says the technology will have a beneficial application in monitoring the elderly at home to ensure their safety. Homes are laced with humidity, temperature and motion-sensing tags that can for example, "sense when a medicine cabinet has been opened, or if a microwave oven has been operated." In other words, the Orwellian "behavioral engine" can learn what a person is doing on a regular basis.

But given the interest--and a $100,000 DHS grant, chump change by current Washington standards to be sure--corporate and intelligence agency clients have something far different in mind than monitoring the sick and the elderly!

Indeed, the *RFID Journal* reports that "a company could use the system, for instance, to monitor the behavior of employees to ensure no security rules are breached."

Want to surveil workers for any tell-tale signs of "antisocial behavior" such as union organizing? Then Queralt may have just the right tool for you! "The workers could be issued RFID-enabled ID badges that are read as they arrive at and leave work, enter and exit various departments, and log onto and off of different computer systems," the *RFID Journal* informs us. "Over time, the system will establish a pattern that reflects the employee's typical workday."

And if a worker "enters the office much earlier than normal on a particular occasion," or "goes into a department in which he or she does not work," perhaps to "coerce" others into joining "communist" unions opposed let's say, to widespread surveillance, the ubiquitous and creepy spy system "could send an alert."
Queralt is currently designing an application programming interface to "logical security and identity-management systems" from Microsoft and Oracle that will enable corporations to "tie the RFID-enabled behavioral system to their security applications."

The Future Is Now!

This brief survey of the national security state's deployment of a literally murderous, and privacy-killing, surveillance technology is not a grim, dystopian American *future* but a quintessentially American *present*.

The technological fetishism of Pentagon war planners and their corporate enablers masks the deadly realities for humanity posed by the dominant world *disorder* that has reached the end of the line as capitalism's long death-spiral threatens to drag us all into the abyss.

The dehumanizing rhetoric of RMA with its endless array of acronyms and "warfighting tools" that reduce waging aggressive imperialist wars of conquest to the "geek speak" of a video game, must be unmasked for what it actually represents: state killing on a massive scale.

Perhaps then, the victims of America's "war on terror," at home as well as abroad, will cease to be "targets" to be annihilated by automated weapons systems or ground down by panoptic surveillance networks fueled by the deranged fantasies of militarists and the corporations for whom product development is just another deadly (and very profitable) blood sport.

http://antifascist-calling.blogspot.com/2009/06/cia-and-pentagon-deploy-rfid-death.html

---