Written by **Joe Wolverton, II, J.D.** on October 3, 2012

TrapWire Training Courses Reveal Possible Purpose for its Creation

Although certain people reportedly playing key roles in the web-like leadership structure of TrapWire deny their involvement with the massive surveillance system, there is evidence that the engine driving this global company runs on the ambition of a common core of officers and directors.

Given the potential flood of legal challenges to its constitutionality, the corporation believed to be behind TrapWire is heading for higher ground, denying any association with the surveillance technology.

In a statement published on its website on August 13, Cubic Corporation attempted to sever the ties binding it to TrapWire. "Cubic Corporation (NYSE: CUB) acquired Abraxas Corporation on December 20, 2010. Abraxas Corporation then and now has no affiliation with Abraxas Applications now known as Trapwire, Inc. Erroneous reports have linked the company with Trapwire, Inc.," the company insisted.

Despite such denials, many are rightly worried about any corporate connection — no matter how tenuous — between Cubic and TrapWire given the former's access to the personal data of Americans through its other corporate interests. The synergy of such access with a massive surveillance apparatus could threaten the privacy of millions, as well as the freedom from unwarranted searches and seizures protected by the Fourth Amendment.

As for the scope and significance of TrapWire, the size of it cannot be exaggerated.

TrapWire is a massive and technologically advanced surveillance system that has the capacity to keep nearly the entire population of this country under the watchful eye of government 24 hours a day. Using this network of cameras and other surveillance tools, the federal government is rapidly constructing an impenetrable, inescapable theater of surveillance, most of which is going unnoticed by Americans and unreported by the mainstream media.

Unlike other elements of the central government's cybersurveillance program, word about TrapWire was not leaked by Obama administration insiders. The details of this nearly unbelievable surveillance scheme were made public by WikiLeaks, the anti-secrecy group founded by Julian Assange. The TrapWire story percolated from the millions of e-mails from the Austin, Texas-based private intelligence-gathering firm Stratfor, published this year by WikiLeaks. Covering correspondence from mid-2004 to 2011, these documents expose Stratfor's "web of informers, pay-off structure, payment-laundering techniques and psychological methods."

This coterie of Stratfor co-conspirators is apparently angry about the leaks, considering that the WikiLeaks servers have been under near-constant Distributed Denial of Service (DDoS) attacks since the TrapWire revelations began attracting the notice of alternative journalists. Some outlets report that the cyberattacks are being carried out by agents of the American intelligence community determined to

prevent the full depth of this scandal from being explored by reporters.

Exactly what is TrapWire? According to one description of the program, from Russia Today:

> Former senior intelligence officials have created a detailed surveillance system more accurate than modern facial recognition technology — and have installed it across the US under the radar of most Americans, according to emails hacked by Anonymous.
>
> Every few seconds, data picked up at surveillance points in major cities and landmarks across the United States are recorded digitally on the spot, then encrypted and instantaneously delivered to a fortified central database center at an undisclosed location to be aggregated with other intelligence.

Although many of the details remain undisclosed, it is known that the infrastructure of TrapWire was designed and deployed by Abraxas, an intelligence contractor based in northern Virginia headed and run by dozens of former American surveillance officers. As one article described it: "The employee roster at Abraxas reads like a who's who of agents once with the Pentagon, CIA and other government entities according to their public LinkedIn profiles, and the corporation's ties are assumed to go deeper than even documented."

The network is believed to be immense. An article published by transparency advocacy group Public Intelligence claims that Stratfor e-mails suggest that TrapWire is in use by the U.S. Secret Service, the British security service MI5, the Royal Canadian Mounted Police, as well as counterterrorism divisions in both the Los Angeles and New York Police Departments and the LA fusion center. The e-mails also suggest that TrapWire is in use at military bases around the country. A July 2011 e-mail from a "Burton" to others at Stratfor describes how the U.S. Army, Marine Corps, and Pentagon have all begun using TrapWire and are "on the system now." Burton described the Navy as the "next on the list."

A survey of WikiLeaks e-mails containing information about TrapWire reveals another facet of this ever-expanding tool for tracking and targeting individuals.

In a report filed by online news gathering site darkernet.in, a list of the training courses offered to end users shines a little light on the otherwise purposefully obscured goals of this global monitoring behemoth.

The first course listed in the darkernet article is called the Surveillance Awareness Workshop. This class is reportedly "designed to instruct network and security personnel to use and navigate the TrapWire software system to familiarize themselves with the indicators of surveillance, terrorist surveillance methodologies, facility vulnerabilities, and the identification of probable surveillance zones that exist within each facility."

The goal is that those with their fingers on the buttons and eyes on the consoles will learn to "view their facility the same way as would a terrorist, and then to be alert to the indicators of pre-attack surveillance."

Pre-attack is a statist way of saying "guilty until proven innocent." These agents — typically law enforcement or federal intelligence officers — reportedly will learn to spot suspicious behavior that points to the target's propensity for participation in illegal activities.

This sort of advance profiling is eerily similar to the philosophy undergirding the signature strike that is becoming the go-to tactic in the Obama administration's drone war.

A signature strike is not a strike on a particular suspect, but rather an attack on a person or group of

people demonstrating behavior that is typical of those who might be associated with terror.

Perhaps the TrapWire "pre-attack surveillance" and the drone war "signature strike" are just two identifiable examples of a wider, more insidious government movement toward a society where one can be found guilty in advance of any crime based solely on one's likelihood to act unlawfully and then be summarily executed based on that probability alone.

The second class offered by the makers of TrapWire according to the Internet investigation is designed along similar lines. It is called the Terrorist Pre-Attack Operations Course (TPOC).

Darkernet reports that participation in TPOC "will enhance overall security awareness and improve participants' understanding of terrorist and criminal pre-attack surveillance and intelligence collection operations."

Once again, the watchers are taught to better understand "terrorists" and what behavior they display just prior to the commission of a crime.

Unlike actual laws, these technologies and the courses improving their capabilities in the hands of users do not offer definitions of "terrorist" or "criminal." One is left to one's own understanding, it would seem, in the matter of conceiving of who is and is not a terrorist.

Today, the typical target might be a Muslim seen frequenting a subway station, for example. However, as the gulf separating the rulers and the ruled widens, perhaps a future TrapWire operator will target a gun-owner or attendant at a rally opposing a government policy as a potential threat and will initiate the requisite "intelligence collection operations." The end result of those operations may be indefinite detention or death by Hellfire missile.

Finally, the last class listed in the darkernet article is called the Deception Detection and Eliciting Responses (DDER) course. This class will "teach students to detect deception and elicit responses in individuals including those which have been identified by TrapWire as having been engaged in suspicious behavior."

So, once the target's image pops up on one of the myriad cameras tracking the movements of every citizen (all are targets and potential terrorists, apparently) and the intelligence officers are called in to begin building a dossier on the target, the responding agents will use their newly-acquired interrogation skills to get the truth out of the target. "We have ways of making you talk," in other words.

Given the aversion of the wizards running the surveillance state to allowing the curtain to be pulled back exposing the incredible extent of its domestic surveillance activities, it is more likely than not that TrapWire's use in the tracking of Americans is wider and more institutional than most of us would like to believe.

A link to a complete listing of all TrapWire courses and the associated material is found here.