



TrapWire's Alleged Corporate and Government Connections Grow

As TrapWire searches out and scrubs all references in the mainstream media to its global surveillance system, new connections between it and other tracking technologies are being uncovered.

[Tartan is software designed by Ntrepid Corporation](#) that “exposes and quantifies key influencers and hidden connections in social networks using mathematical algorithms for objective, un-biased output. Our analysts, mathematicians and computer scientists are continually exploring new quantification, mining and visualization techniques in order to better analyze social networks.”

[According to RT](#), Tartan “aims to track down alleged anarchists by specifically singling out Occupy Wall Street protesters and the publicly funded media — all with the aid of federal agents.”

The [Tartan website](#) proudly admits this use of its technology. “Tartan was used to reveal a hidden network of relationships among anarchist leaders of seemingly unrelated movements,” the website reads. “The study exposed the affiliations within this network that facilitate the viral spread of violent and illegal tactics to the broader protest movement in the United States.”

As [The New American recently reported](#), 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 are 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 notice of alternative journalists. Some outlets report that the cyberattacks are being carried out by agents of the American intelligence community determined to





Written by [Joe Wolverton, II, J.D.](#) on August 28, 2012

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.”

Just how expansive is the TrapWire network believed to be? 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 Department and the LA fusion center. The e-mails also suggest that TrapWire is in use at military bases around the country. A [July 2011 email 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.”

One e-mail in a set stolen from global intelligence firm Stratfor by hactivists Anonymous and leaked via WikiLeaks states:

We have an agreement in principle with Abraxas [TrapWire] to provide “streaming sitreps” to their clients via their desktop/homepage by the end of July. Their clients include Scotland Yard, #10 Downing, the White House, and many MNC’s [multinational corporations].

In what is likely an uncomfortable discovery for the company behind TrapWire, several common board members link TrapWire to Tartan. First, Margaret A. Lee is listed as secretary of the board of directors of Ntrepid. Also on the board are Director Richard Helms, CFO Wesley R. Husted, and President Michael Martinka.

Compare this information with the Commonwealth of Virginia’s State Corporation Commission website where [Margaret A. Lee registered a company named TrapWire](#) Inc. on March 7, 2009. Other business databases available on the Web reveal that in the past, Wesley Husted served as the CFO of TrapWire, Inc. and a Richard H. Helms was the CEO.

RT reports that Helms is a former CIA agent “that once ran the agency’s European division.” The same article claims that Helms has since “severed ties with TrapWire,” but the other significant links between TrapWire and Tartan developer Ntrepid are unchanged. All three of these individuals are also named in documents filed by Ntrepid with the Florida Department of State, Division of Corporations.

Recently, however, in a comment to [Project PM’s Barrett Brown](#), Cubic Corp. Communication Director



Written by [Joe Wolverton, II, J.D.](#) on August 28, 2012

Tim Hall repeats his company's denial of the relationship. "There is no connection at all with Abraxas Applications and Trapwire and or Ntrepid," Hall reportedly said in [an audio file posted to YouTube](#). Project PM counters by claiming to have a copy of Cubic's 2010 tax returns where Ntrepid and Abraxas are listed as being companies "wholly owned" by Cubic.

For its part, Cubic Corporation denies being involved in anything related to TrapWire. In a [press release](#) Cubic stated, "Abraxas Corporation then and now has no affiliation with Abraxas Applications now known as Trapwire, Inc."

That claim doesn't square with the information revealed in [a story covering the latest in the ongoing TrapWire revelations](#):

According to [a 2007 report in the Washington Business Journal](#), though, that as well is a full-on fib. "Abraxas Corp., a risk-mitigation technology company, has spun out a software business to focus on selling a new product," the article reads. "The spinoff — called Abraxas Applications — will sell TrapWire, which predicts attacks on critical infrastructure by analyzing security reports and video surveillance."

It is unclear how or if Cubic Corporation will explain this apparent discrepancy.

While all this corporate intermingling is certainly suspicious, especially in light of the adamant denials of such on the part of the companies allegedly involved, an important question remains: What ties these two surveillance schemes to the government of the United States?

Several organizations and individuals are digging deeper into the corporate connection between TrapWire and Tartan and how these twin terrors might be implemented by U.S. intelligence.

[The British newspaper Guardian reported](#) last year that Ntrepid was working on an "online personal management" tool useful in the influence of "regional and international audiences to achieve U.S. Central Command strategic objectives."

Additionally, the Guardian's research uncovered a \$2.76-million contract awarded by U.S. Central Command to Ntrepid Corporation. The money was earmarked, the *Guardian* reports, for the creation of "false online personalities" that would drum up support for the American foreign policy overseas. The *Guardian* writes that Centcom would accomplish this goal by enabling:

US service personnel, working around the clock in one location, to respond to emerging online conversations with any number of co-ordinated messages, blogposts, chatroom posts and other interventions. Details of the contract suggest this location would be MacDill air force base near Tampa, Florida, home of US Special Operations Command.

All this should be done, the story continues, without revealing the wizards behind the cyber curtain. Interestingly, RT claims that this identity-guarding gambit was supported by a timely software purchase by Cubic Corporation — the company that created TrapWire. The article alleges that through a corporate buyout, Cubic Corporation gained control of "an online identity masking tool called Anonymizer."

Despite the apparent similarities between Centcom's project and Anonymizer, there is nothing proving a connection between them.



Subscribe to the New American

Get exclusive digital access to the most informative, non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.

[Subscribe](#)