()

The GiFiles,
Files released: 5543061

The GiFiles (https://www.wikileaks.org/the-gifiles.html)

(//wikileaks.org/the-gifiles.html)

On Monday February 27th, 2012, WikiLeaks began publishing *The Global Intelligence Files*, over five million e-mails from the Texas headquartered "global intelligence" company Stratfor. The e-mails date between July 2004 and late December 2011. They reveal the inner workings of a company that fronts as an intelligence publisher, but provides confidential intelligence services to large corporations, such as Bhopal's Dow Chemical Co., Lockheed Martin, Northrop Grumman, Raytheon and government agencies, including the US Department of Homeland Security, the US Marines and the US Defence Intelligence Agency. The emails show Stratfor's web of informers, pay-off structure, payment laundering techniques and psychological methods.

Re: [CT] [SUSPECTED SPAM] Fw: [OS] US/CT/TECH - Palantir, the War on Terror's Secret Weapon

Released on 2013-03-04 00:00 GMT

Email-ID	5499887
Date	2011-11-29 01:52:58
From	colby.martin@stratfor.com
To	ct@stratfor.com

somebody is making the money, it isn't like they give it back. it is what i always loved about NGO work - volunteers do all the work - the Director makes 300,000 a year and doesn't pay taxes (or anything else for that matter).

On 11/28/11 6:14 PM, Sean Noonan wrote:

The company Fred was asking about a couple weeks ago. Very good article. The hypothetical sounds too good to be true, but even if its half way there, that's pretty impressive. Stick, note the assigned reading. All the good stuff is in the article, here are some problems:
1. It all depends on the inputs. But what this tells me is not only is the software helpful, but the inputs have gotten a lot better.
2. Thiel is probably fucking nuts. (I usually wouldn't get worked up about privacy concerns, but some of his work scares me)
3. I get the salary cap thing, but only to a point. Its like working for the govt, but as they point out all these engineers went to CA instead of DC in the first place for a reason.
4. "There is only one trilogy"

From: Morgan Kauffman <morgan.kauffman@stratfor.com>
Sender: os-bounces@stratfor.com
Date: Mon, 28 Nov 2011 17:48:36 -0600 (CST)
To: OS<os@stratfor.com>
ReplyTo: The OS List <os@stratfor.com>

Subject: [OS] US/CT/TECH - Palantir, the War on Terror's Secret Weapon
http://www.businessweek.com/printer/magazine/palantir-the-vanguard-of-cyberterror-security-11222011.html

Palantir, the War on Terror's Secret Weapon
A Silicon Valley startup that collates threats has quietly become indispensable to the U.S. intelligence community

By Ashlee Vance and Brad Stone

In October, a foreign national named Mike Fikri purchased a one-way plane ticket from Cairo to Miami, where he rented a condo. Over the previous few weeks, he'd made a number of large withdrawals from a Russian bank account and placed repeated calls to a few people in Syria. More recently, he rented a truck, drove to Orlando, and visited Walt Disney World by himself. As numerous security videos indicate, he did not frolic at the happiest place on earth. He spent his day taking pictures of crowded plazas and gate areas.

None of Fikri's individual actions would raise suspicions. Lots of people rent trucks or have relations in Syria, and no doubt there are harmless eccentrics out there fascinated by amusement park infrastructure. Taken together, though, they suggested that Fikri was up to something. And yet, until about four years ago, his pre-attack prep work would have gone unnoticed. A CIA analyst might have flagged the plane ticket purchase; an FBI agent might have seen the bank transfers. But there was nothing to connect the two. Lucky for counterterror agents, not to mention tourists in Orlando, the government now has software made by Palantir Technologies, a Silicon Valley company that's become the darling of the intelligence and law enforcement communities.

The day Fikri drives to Orlando, he gets a speeding ticket, which triggers an alert in the CIA's Palantir system. An analyst types Fikri's name into a search box and up pops a wealth of information pulled from every database at the government's disposal. There's fingerprint and DNA evidence for Fikri gathered by a CIA operative in Cairo; video of him going to an ATM in Miami; shots of his rental truck's license plate at a tollbooth; phone records; and a map pinpointing his movements across the globe. All this information is then displayed on a clearly designed graphical interface that looks like something Tom Cruise would use in a Mission: Impossible movie.

As the CIA analyst starts poking around on Fikri's file inside of Palantir, a story emerges. A mouse click shows that Fikri has wired money to the people he had been calling in Syria. Another click brings up CIA field reports on the Syrians and reveals they have been under investigation for suspicious behavior and meeting together every day over the past two weeks. Click: The Syrians bought plane tickets to Miami one day after receiving the money from Fikri. To aid even the dullest analyst, the software brings up a map that has a pulsing red light tracing the flow of money from Cairo and Syria to Fikri's Miami condo. That provides local cops with the last piece of information they need to move in on their prey before he strikes.

Fikri isn't real-he's the John Doe example Palantir uses in product demonstrations that lay out such hypothetical examples. The demos let the company show off its technology without revealing the sensitive work of its clients. Since its founding in 2004, the company has quietly developed an indispensable tool employed by the U.S. intelligence community in the war on terrorism. Palantir technology essentially solves the Sept. 11 intelligence problem. The Digital Revolution dumped oceans of data on the law enforcement establishment but provided feeble ways to make sense of it. In the months leading up to the 2001 attacks,

the government had all the necessary clues to stop the al Qaeda perpetrators: They were from countries known to harbor terrorists, who entered the U.S. on temporary visas, had trained to fly civilian airliners, and purchased one-way airplane tickets on that terrible day.

An organization like the CIA or FBI can have thousands of different databases, each with its own quirks: financial records, DNA samples, sound samples, video clips, maps, floor plans, human intelligence reports from all over the world. Gluing all that into a coherent whole can take years. Even if that system comes together, it will struggle to handle different types of data-sales records on a spreadsheet, say, plus video surveillance images. What Palantir (pronounced Pal-an-TEER) does, says Avivah Litan, an analyst at Gartner (IT), is "make it really easy to mine these big data sets." The company's software pulls off one of the great computer science feats of the era: It combs through all available databases, identifying related pieces of information, and puts everything together in one place.

Depending where you fall on the spectrum between civil liberties absolutism and homeland security lockdown, Palantir's technology is either creepy or heroic. Judging by the company's growth, opinion in Washington and elsewhere has veered toward the latter. Palantir has built a customer list that includes the U.S. Defense Dept., CIA, FBI, Army, Marines, Air Force, the police departments of New York and Los Angeles, and a growing number of financial institutions trying to detect bank fraud. These deals have turned the company into one of the quietest success stories in Silicon Valley-it's on track to hit $250 million in sales this year-and a candidate for an initial public offering. Palantir has been used to find suspects in a case involving the murder of a U.S. Immigration and Customs Enforcement special agent, and to uncover bombing networks in Syria, Afghanistan, and Pakistan. "It's like plugging into the Matrix," says a Special Forces member stationed in Afghanistan who requested anonymity out of security concerns. "The first time I saw it, I was like, `Holy crap. Holy crap. Holy crap.' "

Palantir's engineers fill the former headquarters of Facebook along University Avenue in the heart of Palo Alto's main commercial district. Over the past few years, Palantir has expanded to four other nearby buildings as well. Its security people-who wear black gloves and Secret Service-style earpieces-often pop out of the office to grab their lunch, making downtown Palo Alto feel, at times, a bit like Langley.

Inside the offices, sweeping hand-drawn murals fill the walls, depicting tributes to Care Bears and the TV show Futurama. On one floor, a wooden swing hangs from the ceiling by metal chains, while Lord of the Rings knickknacks sit on desks. T-shirts with cutesy cartoon characters are everywhere, since the engineers design one for each new version of their software. Of late, they've run out of Care Bears to put on the shirts and moved on to My Little Ponies.

The origins of Palantir go back to PayPal, the online payments pioneer founded in 1998. A hit with consumers and businesses, PayPal also attracted criminals who used the service for money laundering and fraud. By 2000, PayPal looked like "it was just going to go out of business" because of the cost of keeping up with the bad guys, says Peter Thiel, a PayPal co-founder.

The antifraud tools of the time could not keep up with the crooks. PayPal's engineers would train computers to look out for suspicious transfers-a number of large transactions between U.S. and Russian accounts, for example-and then have human analysts review each flagged

deal. But each time PayPal cottoned to a new ploy, the criminals changed tactics. The computers would miss these shifts, and the humans were overwhelmed by the explosion of transactions the company handled.

PayPal's computer scientists set to work building a software system that would treat each transaction as part of a pattern rather than just an entry in a database. They devised ways to get information about a person's computer, the other people he did business with, and how all this fit into the history of transactions. These techniques let human analysts see networks of suspicious accounts and pick up on patterns missed by the computers. PayPal could start freezing dodgy payments before they were processed. "It saved hundreds of millions of dollars," says Bob McGrew, a former PayPal engineer and the current director of engineering at Palantir.

After EBay (EBAY) acquired PayPal in 2002, Thiel left to start a hedge fund, Clarium Capital Management. He and Joe Lonsdale, a Clarium executive who'd been a PayPal intern, decided to turn PayPal's fraud detection into a business by building a data analysis system that married artificial intelligence software with human skills. Washington, they guessed, would be a natural place to begin selling such technology. "We were watching the government spend tens of billions on information systems that were just horrible," Lonsdale says. "Silicon Valley had gotten to be a lot more advanced than government contractors, because the government doesn't have access to the best engineers."

Thiel, Lonsdale, and a couple of former colleagues officially incorporated Palantir in 2004. Thiel originally wanted to hire a chief executive officer from Washington who could navigate the Byzantine halls of the military-industrial complex. His co-founders resisted and eventually asked Alex Karp, an American money manager living in Europe who had been helping raise money for Clarium, to join as temporary CEO.

It was an unlikely match. Before joining Palantir, Karp had spent years studying in Germany under Ju:rgen Habermas, the most prominent living representative of the Frankfurt School, the group of neo-Marxist philosophers and sociologists. After getting a PhD in philosophy from the University of Frankfurt-he also has a degree from Stanford Law School-Karp drifted from academia and dabbled in stocks. He proved so good at it that, with the backing of a handful of European billionaires, he set up a money management firm called the Caedmon Group. His intellect, and ability to solve a Rubik's Cube in under a minute, commands an awed reverence around the Palantir offices, where he's known as Dr. Karp.

In the early days, Palantir struggled to sell its message and budding technology to investors. Big-name venture capital firms such as Kleiner Perkins Caufield & Byers, Sequoia Capital, and Greylock Partners all passed. Lonsdale says one investor, whom he won't name, actually started laughing on the phone at Karp's nonbusiness academic credentials. Overlooked by the moneyed institutions on Sand Hill Road, Thiel put up the original funds before enticing In-Q-Tel, the investment arm of the CIA, to invest as well. Karp says the reason VC firms "passed was that enterprise technology was not hot. And the government was, and still is, anti-hot."

Michael E. Leiter, the former head of the National Counterterrorism Center, recalls being skeptical when Karp arrived to sell Palantir's system to the NCTC, created by President George W. Bush after the attacks. "There's Karp with his hair and his outfit-he doesn't look like me or the other people that work for me," he says. But Leiter soon discovered that Palantir's software cost a fraction of competing products and actually worked. Palantir not only made the connections

between the data sets but also drew inferences based on the clues and empowered the analysts. Leiter is now a Palantir consultant.

At 44, Karp has a thin, sinewy physique-the result of a strict 1,200-calorie-a-day diet-and an angular face that gives way to curly brown, mad-scientist hair. On a November visit at Palantir's headquarters, he's wearing purple pants and a blue and orange athletic shirt. As he does every day, he walked to work. "I never learned to drive because I was busy reading, doing things, and talking to people," he says. "And I'm coordinated enough to bike, but the problem is that I will start dreaming about the business and run into a tree."

During the era of social networks, online games, and Web coupons, Karp and his engineers have hit on a grander mission. "Our primary motivation," Karp says, "is executing against the world's most important problems in this country and allied countries." That's an unusual pitch in Silicon Valley, where companies tend to want as little to do with Washington as possible and many of the best engineers flaunt their counterculture leanings.

Palantir's name refers to the "seeing stones" in Lord of the Rings that provide a window into other parts of Middle-earth. They're magical tools created by elves that can serve both good and evil. Bad wizards use them to keep in touch with the overlord in Mordor; good wizards can peer into them to check up on the peaceful, innocent Hobbits of the Shire. As Karp explains with a straight face, his company's grand, patriotic mission is to "protect the Shire."

Most of Palantir's government work remains classified, but information on some cases has trickled out. In April 2010, security researchers in Canada used Palantir's software to crack a spy operation dubbed Shadow Network that had, among other things, broken into the Indian Defense Ministry and infiltrated the Dalai Lama's e-mail account. Palantir has also been used to unravel child abuse and abduction cases. Palantir "gives us the ability to do the kind of link-and-pattern analysis we need to build cases, identify perpetrators, and rescue children," says Ernie Allen, CEO of the National Center for Missing and Exploited Children. The software recently helped NCMEC analysts link an attempted abduction with previous reports of the suspect to the center's separate cyber-tip line-and plot that activity on a map. "We did it within 30 seconds," Allen says. "It is absolutely a godsend for us."

In Afghanistan, U.S. Special Operations Forces use Palantir to plan assaults. They type a village's name into the system and a map of the village appears, detailing the locations of all reported shooting skirmishes and IED, or improvised explosive device, incidents. Using the timeline function, the soldiers can see where the most recent attacks originated and plot their takeover of the village accordingly. The Marines have spent years gathering fingerprint and DNA evidence from IEDs and tried to match that against a database of similar information collected from villagers. By the time the analysis results came back, the bombers would be long gone. Now field operatives are uploading the samples from villagers into Palantir and turning up matches from past attacks on the spot, says Samuel Reading, a former Marine who works in Afghanistan for NEK Advanced Securities Group, a U.S. military contractor. "It's the combination of every analytical tool you could ever dream of," Reading says. "You will know every single bad guy in your area."

Palantir has found takers for its data mining system closer to home, too. Wall Street has been particularly receptive. Every year, the

company holds a conference to promote its technology, and the headcount swelled from about 50 people at past events to 1,000 at the most recent event in October. "I saw bankers there that don't go to any other conferences," says Gartner's Litan. The banks have set Palantir's technology loose on their transaction databases, looking for fraudsters, trading insights, and even new ways to price mortgages. Guy Chiarello, chief information officer for JPMorgan Chase (JPM), says Palantir's technology turns "data landfills into gold mines." The bank has a Palantir system for fraud detection and plans to use the technology to better tailor marketing campaigns to consumers. "Google (GOOG) unlocked the Internet with its search engine," Chiarello says. "I think Palantir is on the way to doing a similar thing inside the walls of corporate data."

One of the world's largest banks has used Palantir software to break up a popular scam called BustOut. Criminals will steal or purchase access to thousands of people's online identities, break into their bank and credit-card accounts, then spend weeks watching. Once they spot a potential victim purchasing a plane ticket or heading out on a holiday, they siphon money out of the accounts as fast as they can while the mark is in transit. The criminals hide their trails by anonymizing their computing activity and disabling alert systems in the bank and credit-card accounts. When the bank picks up on a few compromised accounts, it uses Palantir to uncover the network of thousands of other accounts that have to be tapped.

A Palantir deal can run between $5 million and $100 million. The company asks for 20 percent of that money up front and the rest only if the customer is satisfied at the end of the project. Typically, it's competing against the likes of Raytheon (RTN), Lockheed Martin (LMT), Northrop Grumman (NOC), and IBM (IBM), along with a scattering of less prominent data mining startups. "We can be up and running in a bank in eight weeks," Karp says. "You will be getting results right away instead of waiting two to three years with our competitors."

Palantir has been doubling headcount every year to keep up with business. To get a job at the company, an applicant must pass a gauntlet of brain teasers. An example: You have 25 horses and can race them in heats of 5. You know the order the horses finished in, but not their times. How many heats are necessary to find the fastest? First and second? First, second, and third? (Answers: six, seven, and seven.) If candidates are able to prove themselves as what Karp calls "a software artist," they're hired. The company gives new arrivals some reading material, including a guide to improvisational acting, a lecture by the entrepreneur Steve Blank on Silicon Valley's secret history with the military, and the book The Looming Tower: Al-Qaeda and the Road to 9/11. They're also rewarded with a low wage by Silicon Valley standards: Palantir caps salaries at $127,000.

Instead of traditional salespeople, Palantir has what it calls forward deployed engineers. These are the sometimes awkward computer scientists most companies avoid putting in front of customers. Karp figures that engineers will always tell the truth about the pros and cons of a product, know how to solve problems, and build up a strong reputation with customers over time. "If your life or your economic future is on the line," he says, "and there is one company where people are maybe kind of suffering from Asperger's syndrome, but they have always been accurate, you end up trusting them."

The director of these forward deployed engineers is Shyam Sankar, a Palantir veteran. In his corner office there's a Shamu stuffed animal,

an antique Afghan rifle hanging overhead, and a 150-year-old bed frame decorated with a wild, multicolored comforter. The bed comes in handy during an annual team-building exercise: For one week, employees live in the Palantir offices; the bedless make shantytown houses out of cardboard boxes. Sankar celebrates Palantir's mix of office frivolity and low salaries. "We will feed you, clothe you, let you have slumber parties, and nourish your soul," he says. "But this is not a place to come to get cash compensation."

Like many of the young engineers, Sankar recounts a personal tale that explains his patriotic zeal. When he was young, his parents moved from India to Nigeria, where Sankar's father ran a pharmaceutical plant. One night, burglars broke into their home, pistol-whipped his dad, and stole some valuables. After that traumatic event, the family moved to Florida and started over, selling T-shirts to theme parks. "To come to a place and not have to worry about such bad things instilled a sense of being grateful to America," Sankar says. "I know it sounds corny, but the idea here is to save the Shire."

Karp acknowledges that to outsiders, Palantir's Middle-earth-meets-National Security Agency culture can seem a bit much. "One of my investors asked me, `Is this a company or a cult?' " he says. "Well, I don't seem to be living like a cult leader." Then he begins a discourse on how Palantir's unusual ways serve the business. "I tend to think the critiques are true," Karp says. "To make something work, it cannot be about the money. I would like to believe we have built a culture that is about a higher purpose that takes the form of a company. I think the deep character anomalies of the company are the reasons why the numbers are so strong."

Using Palantir technology, the FBI can now instantly compile thorough dossiers on U.S. citizens, tying together surveillance video outside a drugstore with credit-card transactions, cell-phone call records, e-mails, airplane travel records, and Web search information. Christopher Soghoian, a graduate fellow at the Center for Applied Cybersecurity in the School of Informatics and Computing at Indiana University, worries that Palantir will make these agencies ever hungrier consumers of every piece of personal data. "I don't think Palantir the firm is evil," he says. "I think their clients could be using it for evil things."

Soghoian points out that Palantir's senior legal adviser, Bryan Cunningham, authored an amicus brief three years ago supporting the Bush Administration's position in the infamous warrantless wiretapping case and defended its monitoring domestic communication without search warrants. Another event that got critics exercised: A Palantir engineer, exposed by the hacker collective Anonymous earlier this year for participating in a plot to break into the PCs of WikiLeaks supporters, was quietly rehired by the company after being placed on leave.

Karp stresses that Palantir has developed some of the most sophisticated privacy protection technology on the market. Its software creates audit trails, detailing who has seen certain pieces of information and what they've done with it. Palantir also has a permission system to make sure that workers in agencies using its software can access only the data that their clearance levels allow. "In the pre-Palantir days, analysts could go into file cabinets and read whatever they want," says former NCTC director Leiter. "Nobody had any idea what they had seen." Soghoian scoffs at the privacy-protecting features Palantir builds into its software. "If you don't think the NSA can disable the piece of auditing functionality, you have to be kidding me," he says. "They can do

whatever they want, so it's ridiculous to assume that this audit trail is sufficient."

Thiel, who sits on the board and is an avowed libertarian, says civil liberties advocates should welcome Palantir. "We cannot afford to have another 9/11 event in the U.S. or anything bigger than that," he says. "That day opened the doors to all sorts of crazy abuses and draconian policies." In his view, the best way to avoid such scenarios in the future would be to provide the government the most cutting-edge technology possible and build in policing systems to make sure investigators use it lawfully.

After Washington and Wall Street, Karp says the company may turn its attention to health care, retail, insurance, and biotech. The thinking is that Palantir's technology can illuminate health insurance scams just as well as it might be able to trace the origin of a virus outbreak. Despite all this opportunity, and revenue that is tripling every year, Karp insists that Palantir will remain grounded. An IPO, while not out of the question, "dilutes nonmonetary motivation," he says.

One higher purpose in the coming year will be rescuing strapped companies and government bodies from the brink of financial ruin. Karp lists fraud, Internet security issues, Europe's financial woes, and privacy concerns as possible drivers for Palantir's business. For anyone in peril, the message is clear: Give us a signal and a forward deployed engineer will be at your doorstep. "There are some people out there that don't think to pick up the phone and call us," Karp says. "By next year, many of those people will."

--
Colby Martin
Tactical Analyst
colby.martin@stratfor.com