Stratfor or Stratagainst

Hal Berghel
University of Nevada, Las Vegas

Based on what you know about WikiLeaks and Stratfor, which group seems to be the greater threat to society?

Nearly one year has passed since WikiLeaks released Stratfor's internal email via the hacktivist group, Anonymous. By now, this story should have inspired public discussions on any number of fronts: journalistic ethics, whether private intelligence-gathering companies that use bribery to gain privileged information from politically exposed persons (PEPs) should fall under the Foreign Corrupt Practices Act, and whether governments and their employees should be held accountable for supporting such activities, to name but a few. Yet the current crop of thought leaders appears to be avoiding any potentially important policy issues that might underlie this incident.

BLACK OPS NGOs

Stratfor illustrates the post-9/11 wave of private cybermercenaries—for-profit organizations that sell cyberservices to risk-averse and fearful businesses and governments. Although the psychology behind this mindset may be the more interesting topic and will likely be the subject of social science treatises, essays, and monographs for decades, we'll limit our present discussion to the cyber side of things.

The missions behind the current crop of cybermercenaries seem to fit within the following continuum:

1. *intelligence gathering*—basically the same investigation plus analysis activities usually associated with law enforcement, perhaps with an increased level of sophistication in real-time reporting and analysis, just-in-time briefings of impending events, back-end data mining, and so forth. This activity may involve illegal behavior such as the bribery, extortion, and blackmail of PEPs.
2. *cyberespionage and cybersurveillance*—again, basically what law enforcement does, only privately and with neither oversight nor court orders.
3. *cyberweapons manufacturing or deployment*—either licensed to clients or used offensively by developer.

From what I can tell from the WikiLeaks documents, Stratfor is primarily in the first group—along with HBGary Federal (now part of ManTech) and Palantir on their best behavior. The third group is also easy to populate (thanks again to the Anonymous folks). Players in this space include HBGary and the Gamma Group. The second group is harder to define because it draws talent from the other groups. For example, as the "URL Pearls" sidebar describes, some of the software developed by HBGary and the Gamma Group was designed for cyberespionage and cybersurveillance, and some of the activities of Stratfor, HBGary, and Palantir under such innocuous-sounding rubrics as "predictive policing" involve surveillance.

It should be noted that the activities in (1) and (2) fall within the domain of statutory investigative agencies such as the police and FBI. I note here that accurate classification of cybermercenaries is difficult for outsiders because of the secrecy under which they operate—well outside the sphere of statutory authority and beyond the reach of the media—kind of like a National Security Agency but without the tax support.

This parallels the proliferation of corporate mercenaries—private armies, private military contractors, private security contractors—such as Academi (formerly Xe Services, Blackwater) and Triple Canopy. For the moment, the cyber side seems to remain largely decoupled, but I predict that, in time, these interests will converge into one-size-fits-all, general-purpose private army/police/intelligence-for-hire concerns. Experiments at such integration have already occurred—see the Computer Sciences Corporation, which owned the private military contractor DynCorp from 2003 to 2005. Not surprisingly, as Figure 1 indicates, some of these companies have been known to target WikiLeaks.

Published by the IEEE Computer Society

The Stratfor website states that "Stratfor is a subscription-based provider of geopolitical analysis. … Unlike traditional news outlets, Stratfor uses a unique, intelligence-based approach to gathering information via rigorous open-source monitoring and a global network of human sources." Founded in 1996 by George Friedman, this Austin, Texas, company "publishes analysis via … website and customized email updates." It isn't clear that much of what Stratfor does with its "intelligence" is particularly interesting or controversial, but the way that it gets its "intelligence" is both interesting and controversial, as is evident from the WikiLeaks revelations.

As the press release from Stratfor's founder, shown in Figure 2, indicates, Stratfor's expressed objection to the Anonymous/WikiLeaks exposé is that it was "illegal" and a "breach of privacy." Let's see if we have this right: Stratfor is claiming that there's something wrong with illegal breaches of privacy or the dissemination of information that has been obtained without the information owner's permission.

Ponder that for a while. It seems to me to be a clear case of pots and kettles, snakes and crabs, or brambles and pomegranates. Let's try to put it into some sort of meaningful perspective.

While the mainstream press has extensively covered WikiLeaks for several years now, Stratfor has operated largely in the dark. Many of us had never heard of Stratfor before the Anonymous hack of December 2011, so I offer the following short review for the benefit of the uninitiated.

Stratfor's avowed goal is to become "the world's leading private intelligence organization." This is expressly stated in one of CEO George Friedman's leaked emails (5 September 2011, with the subject line "Labor Day Review of Where We Are"). This is also the email in which Friedman announced to Stratfor employees the StratCAP partnership with Shea Morentz, then managing director of Goldman Sachs, who invested several million dollars in Stratfor to create actionable intelligence useful to investors in exchange for a Stratfor board seat. Apparently this deal soured.

Stratfor uses global informants. According to some media reports, at least some of these informants are paid via Swiss bank accounts and prepaid debit cards.

Stratfor serves global corporations and agencies. A quick review of the "GB Master Client List" spreadsheet dated 3-15-07 is a who's who of financial institutions, government contractors, technology companies, and Forbes 1,000 companies, including Coke, Wexford Capital, Perot Systems, Dow Chemical, and Northrup Grumman.

According to Friedman, Stratfor is not above innovative means to con-

URL PEARLS

Bruce Schneier refers to HBGary Federal as a "cyberweapons arms manufacturer." (http://gizmodo.com/5888440/wikileaks-reveals-private-cias-dirty-laundry-updating-live). HBGary has been associated with a variety of software that would qualify as either, including FastDump and FDPro Windows memory-capturing utilities and the Windows rootkit project, Magenta (http://cyberwarzone.com/cyberwarfare/hbgarys-rootkit-project-magenta?page=4). The Gamma Group is associated with FinFisher, a general-purpose snoop tool that offers screen scraping, Skype session capture, keylogging, decryption, and rootkit capabilities (http://bits.blogs.nytimes.com/2012/08/13/elusive-finspy-spyware-pops-up-in-10-countries). Some interesting analysis of the FinFisher product can be found at https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed.

Wikileaks refers to the 5 million or so Stratfor email messages that it released as "The Global Intelligence Files" (wikileaks.org/gifiles/releases.html). WikiLeaks has the entire Palantir/HBGary/Berico slide presentation in PDF format online at http://wikileaks.org/IMG/pdf/WikiLeaks_Response_v6.pdf. Forbes.com has the complete statement from Palantir CEO Alex Carp online at www.forbes.com/sites/andygreenberg/2011/02/11palantir-apologizes-for-wikileaks-attack-proposal-cuts-ties-with-hbgary.

The PayPal book-banning story has been well covered (www.huffingtonpost.co.uk/bernard-oleary/paypal-banned-books-the-books-banned-by-paypa_b_1314953.html). In reaction to the outcry from anticensorship groups, PayPal has since lifted the ban (www.abffe.org/news/86299/).

Palantir

Potential Proactive Tactics

- Feed the fuel between the feuding groups. Disinformation. Create messages around actions to sabotage or discredit the opposing organization. Submit fake documents and then call out the error.
- Create concern over the security of the infrastructure. Create exposure stories. If the process is believed to not be secure they are done.
- Cyber attacks against the infrastructure to get data on document submitters. This would kill the project. Since the servers are now in Sweden and France putting a team together to get access is more straightforward.
- Media campaign to push the radical and reckless nature of wikileaks activities. Sustained pressure. Does nothing for the fanatics, but creates concern and doubt amongst moderates.
- Search for leaks. Use social media to profile and identify risky behavior of employees.

Figure 1. A slide taken from Palantir's presentation "The WikiLeaks Threat." (The CEO of Palantir has since apologized for this.)

STRATFOR
GLOBAL INTELLIGENCE

George Friedman on Email Theft and the Wikileaks Release

—Visit Stratfor.com/hacking-news to watch this video message from George Friedman

Transcript:

I'm George Friedman, founder and CEO of Stratfor.

As most of you know, in December thieves hacked into Stratfor data systems and stole a large number of company emails, as well as private information of Stratfor subscribers and friends. Today Wikileaks is publishing the emails that were stolen in December. This is a deplorable, unfortunate -- and illegal -- breach of privacy.

Some of the emails may be forged or altered to include inaccuracies. Some may be authentic. We will not validate either, nor will we explain the thinking that went into them. Having had our property stolen, we will not be victimized twice by submitting to questions about them.

Figure 2. Stratfor CEO's announcement of the WikiLeaks revelations.

trol its sources: "If this is a source you suspect may have value, you have to take control od [sic] him. Control means financial, sexual or psychological control to the point where he would reveal his sourcing and be tasked." This email is dated 6 December 2011 and went to a Stratfor intelligence analyst regarding an informant's report on the health of Hugo Chavez.

Regarding relationships with the media, Stratfor works with media organizations and journalists whom it refers to as (among other things) "confederation partners." It's not at all obvious that a private intelligence organization's close relation with the media satisfies the standards of journalistic ethics taught in the academy.

With those few clarifications in mind, I offer for your consideration Table 1 as a modest comparison of Stratfor and WikiLeaks in terms of their operations and objectives.

I've based Table 1 on information available from mainstream media reports and analysis of the WikiLeaks documents. Assuming that this is a fair characterization, and based on what you know about WikiLeaks and

Table 1. Comparison of WikiLeaks and Stratfor operations.

Activity	WikiLeaks	Stratfor
Revenue model	Not for profit	For profit
Primary constituency served	Media/individuals	Corporations/agencies
Seeks access to nonpublic, proprietary, or classified information, for which the owner does not authorize access	Under dispute	Yes
Relies on a leak-centric communication network	Yes	Yes
System built on paid informants	No	Yes
Uses active intelligence systems: leakers, spies, whistleblowers	Yes	Yes
Willing to corrupt media resources	Perhaps	Yes
Partners with media to inform public	Yes	No
Provides intelligence to media/public	Yes	Limited
Provides actionable intelligence to partners in military industrial complex	No	Yes
Black ops	No	Yes
Uses third-party contractors (spies)	No	Yes
Controls sources via money, sex, blackmail, extortion	No	Yes
Nature of risks to society	Overt	Covert

Stratfor, which group seems to you to be the greater threat to society?

THE BRIGHT SIDE

Good journalists are always concerned about the possibility of accidentally disseminating erroneous information. At this point, I haven't seen a single report from any source that I deem credible that claims the WikiLeaks Stratfor emails are bogus. I encourage everyone to look into these leaked documents, and the concomitant media coverage, and come to their own conclusion.

The Stratfor revelations are alarming for at least two reasons. First, I'm not convinced that Stratfor's approach to intelligence analytics will lead to significantly better decision making than we've come to expect from the military industrial complex, and I'm fearful that unenlightened leadership may be lulled into overreliance on such analyses. That might in turn lead to even more ill-advised decisions. Second, I'm bothered by the lack of oversight and transparency in the process. From the email, it appears that Stratfor has introduced a corrupting influence on the process of intelligence gathering.

The question that informed world citizens should ask is whether they feel comfortable with their governments supporting such things. It should be emphasized that there is a reason why governments and businesses outsource this kind of work. Is it due to the fact that dedicated private companies are so much better at it? Or do the customers and clients want to maintain distance from, and deniability of, putatively illegal activity.

There is no obvious Fourth Amendment protection against private shadow intelligence agencies, just as there is no First Amendment protection against PayPal banning books.

While the constitutional lawyers argue the legality, the public should be discussing whether or to what extent Stratfor's activities are consistent with democratic values and the rule of law, and whether government agencies should be tolerating it, much less encouraging it. I'm not sure that a "trust us" defense should be any more compelling to society in this case than when it was used to defend flawless efficient markets before the most recent economic meltdown.

One final observation: it's unlikely that any of this would have become public were it not for Anonymous. But that's a topic for another column.

***Hal Berghel**, Out of Band column editor, is a professor of computer science at the University of Nevada, Las Vegas, where he is the director of the Identity Theft and Financial Fraud Research and Operations Center (itffroc.org). Contact him at hlb@computer.org.*