

افغانستان آزاد – آزاد افغانستان

AA-AA

چو کشور نیاشد تن من مباد بدین بوم ویر زنده یک تن مباد
همه سر به سر تن به کشتن دهیم از آن به که کشور به دشمن دهیم

www.afgazad.com

afgazad@gmail.com

European Languages

زبان های اروپایی

M. Mandl

The Global Intelligence Files

2/27/2012

WikiLeaks began publishing The Global Intelligence Files – more than five million emails from the Texas-headquartered "global intelligence" company Stratfor. The emails date from 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 Defense Intelligence Agency. The emails show Stratfor's web of informers, pay-off structure, payment-laundering techniques and psychological methods, for example :

"[Y]ou have to take control of him. Control means financial, sexual or psychological control... This is intended to start our conversation on your next phase" – CEO George Friedman to Stratfor analyst Reva Bhalla on 6 December 2011, on how to exploit an Israeli intelligence informant providing information on the medical condition of the President of Venezuela, Hugo Chavez.

The material contains privileged information about the US government's attacks against Julian Assange and WikiLeaks and Stratfor's own attempts to subvert WikiLeaks. There are more than 4,000 emails mentioning WikiLeaks or Julian Assange. The emails also expose the revolving door that operates in private intelligence companies in the United States. Government and diplomatic sources from around the world give Stratfor advance knowledge of global politics and events in exchange for money. The Global Intelligence Files exposes how Stratfor has recruited a global network of informants who are paid via Swiss banks accounts and pre-paid credit cards.

Stratfor has a mix of covert and overt informants, which includes government employees, embassy staff and journalists around the world.

The material shows how a private intelligence agency works, and how they target individuals for their corporate and government clients. For example, Stratfor monitored and analysed the online activities of Bhopal activists, including the "Yes Men", for the US chemical giant Dow Chemical. The activists seek redress for the 1984 Dow Chemical/Union Carbide gas disaster in Bhopal, India. The disaster led to thousands of deaths, injuries in more than half a million people, and lasting environmental damage.

Stratfor has realised that its routine use of secret cash bribes to get information from insiders is risky. In August 2011, Stratfor CEO George Friedman confidentially told his employees : "We are retaining a law firm to create a policy for Stratfor on the Foreign Corrupt Practices Act. I don't plan to do the perp walk and I don't want anyone here doing it either."

Stratfor's use of insiders for intelligence soon turned into a money-making scheme of questionable legality. The emails show that in 2009 then-Goldman Sachs Managing Director Shea Morenz and Stratfor CEO George Friedman hatched an idea to "utilise the intelligence" it was pulling in from its insider network to start up a captive strategic investment fund. CEO George Friedman explained in a confidential August 2011 document, marked DO NOT SHARE OR DISCUSS : "What StratCap will do is use our Stratfor's intelligence and analysis to trade in a range of geopolitical instruments, particularly government bonds, currencies and the like". The emails show that in 2011 Goldman Sach's Morenz invested "substantially" more than \$4million and joined Stratfor's board of directors. Throughout 2011, a complex offshore share structure extending as far as South Africa was erected, designed to make StratCap appear to be legally independent. But, confidentially, Friedman told StratFor staff : "Do not think of StratCap as an outside organisation. It will be integral... It will be useful to you if, for the sake of convenience, you think of it as another aspect of Stratfor and Shea as another executive in Stratfor... we are already working on mock portfolios and trades". StratCap is due to launch in 2012.

The Stratfor emails reveal a company that cultivates close ties with US government agencies and employs former US government staff. It is preparing the 3-year Forecast for the Commandant of the US Marine Corps, and it trains US marines and "other government intelligence agencies" in "becoming government Stratfors". Stratfor's Vice-President for Intelligence, Fred Burton, was formerly a special agent with the US State Department's Diplomatic Security Service and was their Deputy Chief of the counterterrorism division. Despite the governmental ties, Stratfor and similar companies operate in complete secrecy with no political oversight or accountability. Stratfor claims that it operates "without ideology, agenda or national bias", yet the emails reveal private intelligence staff who align themselves closely with US government policies and channel tips to the Mossad – including through an information mule in the Israeli newspaper Haaretz, Yossi Melman, who conspired with Guardian journalist David Leigh to secretly, and in violation of WikiLeaks' contract with the Guardian, move WikiLeaks US diplomatic cables to Israel.

Ironically, considering the present circumstances, Stratfor was trying to get into what it called the leak-focused "gravy train" that sprung up after WikiLeaks' Afghanistan disclosures :

"[Is it] possible for us to get some of that 'leak-focused' gravy train ? This is an obvious fear sale, so that's a good thing. And we have something to offer that the IT security companies don't, mainly our focus on counter-intelligence and surveillance that Fred and Stick know better than anyone on the planet... Could we develop some ideas and procedures on the idea of 'leak-focused' network security that focuses on preventing one's own employees from leaking sensitive information... In fact, I'm not so sure this is an IT problem that requires an IT solution."

Like WikiLeaks' diplomatic cables, much of the significance of the emails will be revealed over the coming weeks, as our coalition and the public search through them and discover connections. Readers will find that whereas large numbers of Stratfor's subscribers and clients work in the US military and intelligence agencies, Stratfor gave a complimentary membership to the controversial Pakistan general Hamid Gul, former head of Pakistan's ISI intelligence service, who, according to US diplomatic cables, planned an IED attack on international forces in Afghanistan in 2006. Readers will discover Stratfor's internal email classification system that codes correspondence according to categories such as 'alpha', 'tactical' and 'secure'. The correspondence also contains code names for people of particular interest such as 'Hizzies' (members of Hezbollah), or 'Adogg' (Mahmoud Ahmedinejad).

Stratfor did secret deals with dozens of media organisations and journalists – from Reuters to the Kiev Post. The list of Stratfor's "Confederation Partners", whom Stratfor internally referred to as its "Confed Fuck House" are included in the release. While it is acceptable for journalists to swap information or be paid by other media organisations, because Stratfor is a private intelligence organisation that services governments and private clients these relationships are corrupt or corrupting.

WikiLeaks has also obtained Stratfor's list of informants and, in many cases, records of its payoffs, including \$1,200 a month paid to the informant "Geronimo" , handled by Stratfor's Former State Department agent Fred Burton.

WikiLeaks has built an investigative partnership with more than 25 media organisations and activists to inform the public about this huge body of documents. The organisations were provided access to a sophisticated investigative database developed by WikiLeaks and together with WikiLeaks are conducting journalistic evaluations of these emails. Important revelations discovered using this system will appear in the media in the coming weeks, together with the gradual release of the source documents.