List of Releases

Articles

the gifiles (es)
Stratfor on the Australian Assange
WikiLeaks' Impact is Stratfor's Bottom Line
Stratfor Sydney Based Watch Officer Connection to Woman in Assange Case
Stratfor Emails : US Has Issued Sealed Indictment Against Julian Assange
the gifiles (pt)
the gifiles (de)
the gifiles (se)
the gifiles (fr)
the gifiles

Our Partners

ABC Color - Paraguay
Al Akhbar - Lebanon
Al Masry Al Youm - Egypt
Asia Sentinel - Hong Kong
Bivol - Bulgaria
Carta Capital - Brazil
CIPER - Chile
Dawn Media - Pakistan
L'Espresso - Italy
La Repubblica - Italy
La Jornada - Mexico
La Nacion - Costa Rica
Malaysia Today - Malaysia
McClatchy - United States
Nawaat - Tunisia
NDR/ARD - Germany
Owni - France
Pagina 12 - Argentina
Philip Dorling - Fairfax media contributor - Australia
Plaza Publica - Guatemala
Publica - Brazil
Publico.es - Spain
Rolling Stone - United States
Russian Reporter - Russia
Ta Nea - Greece
Taraf - Turkey
The Hindu - India
The Yes Men - Bhopal Activists
Sunday Star-Times - New Zealand
torrent dumps are available at
wlstorage.net torrent repository
pick newest one available

Community resources

Supporters

Specified Search

Translations
[fr] the gifiles (fr)
[sv] the gifiles (se)
[de] the gifiles (de)
[pt_br] the gifiles (pt)
[es] the gifiles (es)

More articles ...
- Stratfor Emails : US Has Issued Sealed Indictment Against Julian Assange
- Stratfor Sydney Based Watch Officer Connection to Woman in Assange Case
- WikiLeaks' Impact is Stratfor's Bottom Line
- Stratfor on the Australian Assange

LONDON—Today, Monday 27 February, 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 Venezuala, 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.

END

- Public partners in the investigation
- Comment
- Current WikiLeaks status
- How to read the data

Public partners in the investigation:

More than 25 media partners (others will be disclosed after their first publication) :

- Al Akhbar – Lebanon – http://english.al-akhbar.com
- Al Masry Al Youm – Egypt – http://www.almasry-alyoum.com
- Bivol – Bulgaria – http://bivol.bg
- CIPER – Chile – http://ciperchile.cl
- Dawn Media – Pakistan – http://www.dawn.com
- L'Espresso – Italy – http://espresso.repubblica.it
- La Repubblica – Italy – http://www.repubblica.it
- La Jornada – Mexico – www.jornada.unam.mx/
- La Nacion – Costa Rica – http://www.nacion.com
- Malaysia Today – Malaysia – www.malaysia-today.net
- McClatchy – United States – http://www.mcclatchydc.com
- Nawaat – Tunisia – http://nawaat.org
- NDR/ARD – Germany – http://www.ndr.de
- Owni – France – http://owni.fr
- Pagina 12 – Argentina – www.pagina12.com.ar
- Plaza Publica – Guatemala – http://plazapublica.com.gt
- Publico.es – Spain – www.publico.es
- Rolling Stone – United States – http://www.rollingstone.com
- Russian Reporter – Russia – http://rusrep.ru
- Sunday Star-Times – New Zealand - www.star-times.co.nz
- Ta Nea – Greece –- http://www.tanea.gr
- Taraf – Turkey – http://www.taraf.com.tr
- The Hindu – India – www.thehindu.com
- The Yes Men – Bhopal Activists – Global http://theyesmen.org

Comment:

- WikiLeaks – Kristinn Hrafnsson, Official WikiLeaks representative, +35 4821 7121

Other comment :

- Bhopal Medical Appeal (in UK) – Colin Toogood : colintoogood@bhopal.org / +44 (0) 1273 603278/ +44 (0) 7798 845074
- International Campaign for Justice in Bhopal (in India) – Rachna Dhingra : rachnya@gmail.com, +91 98 261 67369
- Yes Men – mike@theyesmen.org / +44 (0) 7578 682321 - andy@theyesmen.org, +1-718-208-0684
- Privacy International – +44 (0) 20 7242 2836

Twitter tag : #gifiles

CURRENT WIKILEAKS STATUS:

An extrajudicial blockade imposed by VISA, MasterCard, PayPal, Bank of America, and Western Union that is designed to destroy WikiLeaks has been in place since December 2010. The EU Commission is considering whether it will open a formal investigation, but two lawsuits have been filed (http://wikileaks.org/Banking-Blocka...). There are also other ways to donate (https://shop.wikileaks.org/donate). It is legal to donate, including in the United States. The US Treasury has publicly stated that that there are no grounds to place WikiLeaks on a US government blacklist.

WikiLeaks Founder and Publisher Julian Assange has not been charged with any crime in any country. Four prosecutors are currently trying to charge him under the Espionage Act of 1917 before a closed Grand Jury in Virginia, in the United States. Julian Assange has been detained for 447 days (10,728 hours) since Dec 7, 2010, without charge, and he is currently awaiting a decision from the UK Supreme Court on extradition to Sweden (http://www.justiceforassange.com/Su...). The decision is expected in March. The decision on whether he will be onwardly extradited to the US lies in the hands of the Swedish Executive, but Sweden's Prime Minister Fredrik Reinfeldt has refused to state whether he will protect Assange from a politically motivated extradition to the United States (http://justice4assange.com/US-Extra...).

The Swedish Foreign Minister Carl Bildt has repeatedly attacked WikiLeaks this week in a bizarre manner

(http://ferrada-noli.blogspot.com/20...).

An alleged WikiLeaks US military source, Bradley Manning, has been in pre-trial detention for 639 days (http://bradleymanning.org/). His arraignment took place on 24 February 2012. In December 2011, Manning's attorney revealed in the preliminary hearing that the US government is attempting to enter a plea deal with Manning in order to "go after" Assange. Manning has 22 charges against him, including violating the Espionage Act of 1917 and aiding the enemy. Manning has deferred entering a plea. Julian Assange and WikiLeaks are legally represented in the Manning hearings by the US Centre for Constitutional Rights (http://ccrjustice.org/). WikiLeaks was denied full access to Manning's hearing after appeal (http://ccrjustice.org/newsroom/pres...). WikiLeaks put out a statement relating to Manning's trial ahead of the Article 32 Hearing : (http://www.wikileaks.org/Statement-...).

The alleged WikiLeaks-supporting hacktivists known as the "PayPal 14" were arrested in 2011 following co-ordinated online demonstrations against the financial services companies that are carrying out the unlawful financial blockade on WikiLeaks (VISA, MasterCard, Paypal, Western Union, Bank of America). They are represented by attorney Stanley Cohen and will go before court in May 2012 (http://www.cyberguerrilla.org/?p=4644).

WikiLeaks is about to launch a distributed, encrypted "Facebook for revolutionaries" (https://wlfriends.org/).

Julian Assange is currently directing interviews, from house arrest, for a programme on the future of the world that is syndicated to various broadcasters. The first show will be broadcast in March (http://www.wikileaks.org/New-Assang...)

HOW TO READ THE DATA

This is a glossary and information on how to understand the internal terms and codes used by Stratfor in their emails. It is not a complete list. We call on the public to add to this list by tweeting #gifind

To see a list of the terms George Friedman considers useful for his staff to know please download this PDF : The Stratfor Glossary of Useful, Baffling and Strange Intelligence Terms.

OPEN SOURCE VS. "COVERT"

As you browse through the content, you will notice that a large set of it is what is classified as "open source" (subject lines which include [OS]). These are basically email threads that start with someone posting a published and accessible source, such as news sites, and follow with commentary by the staff. In one of the emails, Joseph Nye is referenced saying :

"Open source intelligence is the outer pieces of the jigsaw puzzle, without which one can neither begin nor complete the puzzle"

CODES IN SUBJECT LINES

Many of the emails have codes in the subject lines as well as in the body, to make it easier for the staff to "quickly identify when we need to go back and have a look-see." [*] :

Examples : INSIGHT - COUNTRY - Subject - SOURCE CODE INSIGHT - CHINA - Trains and planes - CN1000

Please refer to the glossary for the code names of subject and country tags, as well as mailing list names.

SOURCE CODES

A lot of interesting stuff comes from "sources". Sources are either informal contacts or people they have a formal relationship with. The IDs for sources have the format of CN120 or ME001. In terms of the character part, it refers to a region or a country :

A) Regions ME - Middle East region EU - European Union EE - Eastern Europe LA- South America SA- South Asia

B) Countries or Orgs CN - China PK - Pakistan IN- India ML - Malaysia VN - Vietnam NP- Nepal

US - United States VZ - Venezuela CO- Colombia BR-Brazil NC- Nicaragua MX- Mexico CL/CH- Chile AR-Argentina PY- Paraguay BOL- Bolivia

RU - Russia UA - Ukraine GE - Georgia TJ - Tajikstan MD - Moldova BG -Bulgaria CR/CZ- Czech Republic PT-Portugal

ZA - South Africa AO - Angola SO - Somalia NG- Nigeria CD- DR Congo CI- Cote D'Ivoire ZW- Zimbabwe ZM-Zambia RW- Rwanda KE- Kenya ET- Ethiopia SD -Sudan MA- Morocco SN- Senegal GN- Guinea SL- Sierra Leone

IR - Iran IQ- Iraq IL or IS- Israel SA- Saudi Arabia SY- Syria KU- Kuwait Y or YN - Yemen HZ - Hizbollah TK - Turkey LN- Lebanon LY- Libya UAE- UAE EG- Egypt (etc.)

C) Odd codes OCH - Old China hand, a finance insider. Stick - Scott Stewart, high level employee Z's - Zetas, Mexican drug gang

---

INSIGHTS FORMAT

When "insights" are sent, they usually have the following header information :

SOURCE : The ID of the source, say CN123. Sometimes this is left "no source ID" when it's a new source.

ATTRIBUTION : How the source is to be attributed, i.e. "Source in the pharma distribution industry in China", Stratfor source, etc.

SOURCE DESCRIPTION : Describes the source, for example : "Source works with Mercator Pharmaceutical Solutions, distributing pharma to developing countries." These include concrete details on the source for internal consumption so that there's a better understanding on the source's background and ability to make assessments on the ground.

PUBLICATION : Yes or No. If the option is yes it doesn't mean that it would be published, but rather that it _can_ be published.

SOURCE RELIABILITY : A/B

SOURCE RELIABILITY : A-F, A being the best and F being the worst. This grades the turnaround time of this source in responding to requests.

ITEM CREDIBILITY : 1-10, 1 being the best and 10 being the worst (we may change the range here in the future). this changes a lot based on the info provided. 1 is "you can take this to the bank" and 10 would be an example of maybe - "this is a totally ridiculous rumor but something that is spreading on the ground"

SPECIAL HANDLING : often this is "none" but it may be something like, "if you use this we need to be sure not to mention the part about XXX in the publication" or any other special notes

SOURCE HANDLER : the person who can take follow-up questions and communicate with the source.

MAILING LISTS

alpha@stratfor.com Discussions circulated exclusively among analysts, writers and higher-ups, including 'insights' and discussions about sources and source meetings. secure@stratfor.com Discussions circulated exclusively among analysts and higher-ups, and only for use within continental US (analysts traveling 'overseas' are removed from the list for the duration of their journey). analysts@stratfor.com - Discussion among analysts only, who manage sources, gather and analyze intelligence. ct@stratfor.com Ongoing discussions to collect and analyze counterterrorism intelligence, circulated among select group of analysts. tactical@statfor.com Non-time sensitive discussions for internal training on technical and tactical matters within field of counterterrorism. intelligence@stratfor.com gvalerts@stratfor.com - Related to Gas ventures clients military@stratfor.com Military list for pre-approved staff africa@stratfor.com eastasia@stratfor.com mesa@stratfor.com Middle East/South Asia list for pre-approved staff. eurasia@stratfor.com os@stratfor.com List with information from the public domain circulated and discussed among all employees. adp@stratfor.com List for ADPs. See Glossary. translations@stratfor.com alerts@stratfor.com responses@stratfor.com dialog-list@stratfor.com

GLOSSARY

a) Industry and other misc. tags :

HUMINT - Human intelligence OSINT- Open source intelligence DATA FLU BIRDFLU ECON TECH ENERGY MINING GV - Gas Venture CT - Counterterrorism G1-G4 B2-B4 S1-S4 MILITARY or MIL PENTAGON AQ- Al Qaeda AQAP - Al Qaeda in the Arabia Peninsula SF- Special Forces CONUS- Continental US

b) Special internal codewords :

Hizzies or HZ - Hizbollah Izzies or IZ - Israel A-dogg - Mahmoud Ahmadinajad, Iranian President Baby bashar - Bashar Al-Assad, Syrian President Uncle Mo - Moammar Gaddhafi ADP- Analyst Development Program. Four-month program at STRATFOR from which candidates— mostly recent college graduates— are selected for hire. Strictly protect and protect - Often mentioned in the 'subject', means that the source is protected. Played- A term used for procuring sensitive information from sources. E.g. from one of the secure list messages circulating the 'complete scenario for the Israeli team in Centcom's war game,' the analyst who procured the data wrote : "I played the head of the Mossad which was great fun." Excomm- Appears to be 'executive committee' of STRATFOR.

c) Regions and Orgs

AFRICOM - African countries LATAM - Latin American MERCOSUR NATFA ASEAN APEC FSU - Former Soviet Union countries MESA or MIDDLEEAST - Middle East EASTASIA OPEC EURASIA SA - South Asia FSB- Federal Security Service (Russia)

ATTACHED DOCUMENTS

Attached documents can be searched by Filename or part of the file name. Preliminary searches for filenames using the terms 'lists', 'source lists' or 'insight lists', coupled with the names of source handlers (e.g. Reva for Turkey, Brazil or Venezuela) produced Excel lists of the source names, contact info and source descriptions which correspond to the source codes (e.g. ME1315).

Sourcing Criteria

The following are the proposed criteria for analyzing both sources and insight.

1. Source Timeliness 2. Source Accessibility/Position 3. Source Availability 4. Insight Credibility 5. Insight Uniqueness

Source Timeliness : This is the average grade on how long this particular source turns around tasks and replies to inquiries. It may change but is more of a static indicator.

Source Accessibility : Accessibility weighs the source's position to have certain knowledge in a particular field. So, for example, if we are looking for energy insight and the source is an official in an energy agency, his or her Accessibility would be ranked higher than if s/he was a banker giving insight on energy. While we would welcome a banker giving his/her insight, a good source may not have a high accessibility ranking if they aren't in a position to offer reliable insight on a certain topic. The source's access to decision makers, specific training or education in the desired topic area, specific knowledge of events/situations/incidents can also be considered.

Source Availability : How often can we go to this source ? Are they someone we can tap daily, weekly, monthly, yearly ?

Insight Credibility : This is our assessment of the veracity of the insight offered. Here we need to consider whether or not this is disinformation, speculation, correct data or knowledgeable interpretation. Any bias that the source is displaying or any specific viewpoints or personal background the source is using in the assessment provided should also be considered.

Insight Uniqueness : Is this insight something that could be found in OS ? If it is but the analysis of the information is unique, it would still have a high uniqueness ranking. Or, if it is concrete data, but is something that is only offered to industry insiders, i.e. stats that aren't published but that aren't secret, it would still have a high uniqueness score.

Scoring

All of the above factors will be scored on an A-F scale, with A being exemplary and F being useless.

Source Timeliness : A = turnaround within 24 hours B = turnaround within 48 hours C = turnaround within a week D = turnaround within a month F = lucky to receive a reply at all

Source Accessibility : A = Someone with intimate knowledge of the particular insight B = Someone within the industry but whose knowledge of the topic is not exact (e.g. if we were asking someone in the oil industry about natural gas) C = Someone working close to the industry who doesn't have intimate knowledge of a particular topic but can speak to it intelligently (e.g. a financial consultant asked to gauge the movement of the stock market) D = Someone who may know a country but doesn't have any concrete insight into a particular topic but can offer rumors and discussions heard on the topic F = Someone who has no knowledge of a particular industry at all

Source Availability : A = Available pretty much whenever B = Can tap around once a week C = Can tap about once a month D = Can tap only several times a year F = Very limited availability

Insight Credibility : A = We can take this information to the bank B = Good insight but maybe not entirely precise C = Insight is only partially true D = There may be some interest in the insight, but it is mostly false or just pure speculation. F = Likely to be disinformation

Insight Uniqueness : A = Can't be found anywhere else B = Can only be found in limited circles C = Insight can be found in OS, but the source has an interesting take/analysis D = Insight can be found in OS, but still may not be common knowledge F = Insight is accessible in numerous locations

Daily Insight Scoring

SOURCE : code ATTRIBUTION : this is what we should say if we use this info in a publication, e.g. STRATFOR source/source in the medical industry/source on the ground, etc SOURCE DESCRIPTION : this is where we put the more concrete details of the source for our internal consumption so we can better understand the source's background and ability to make the assessments in the insight. PUBLICATION : Yes or no. If you put yes it doesn't mean that we will publish it, but only that we can publish it. SOURCE RELIABILITY : A-F. A being the best and F being the worst. This grades the source overall - access to information, timeliness, availability, etc. In short, how good is this source ? ITEM CREDIBILITY : A-F. A = we can take this info to the bank ; B = Good insight but maybe not entirely precise ; C = Insight is only partially true ; D = There may be some interest in the insight, but it is mostly false or just pure speculation ; F = Likely to be disinformation. SPECIAL HANDLING : often this is "none" but it may be something like, "if you use this we need to be sure not to mention the part about XXX in thepublication" or any other special notes SOURCE HANDLER : the person who can take follow-up questions and communicate with the source.

Lead journalist: Sarah Harrison