The Intercept_

HOW PETER THIEL'S PALANTIR HELPED THE NSA SPY ON THE WHOLE WORLD

Sam Biddle

February 22 2017, 6:06 a.m.

101

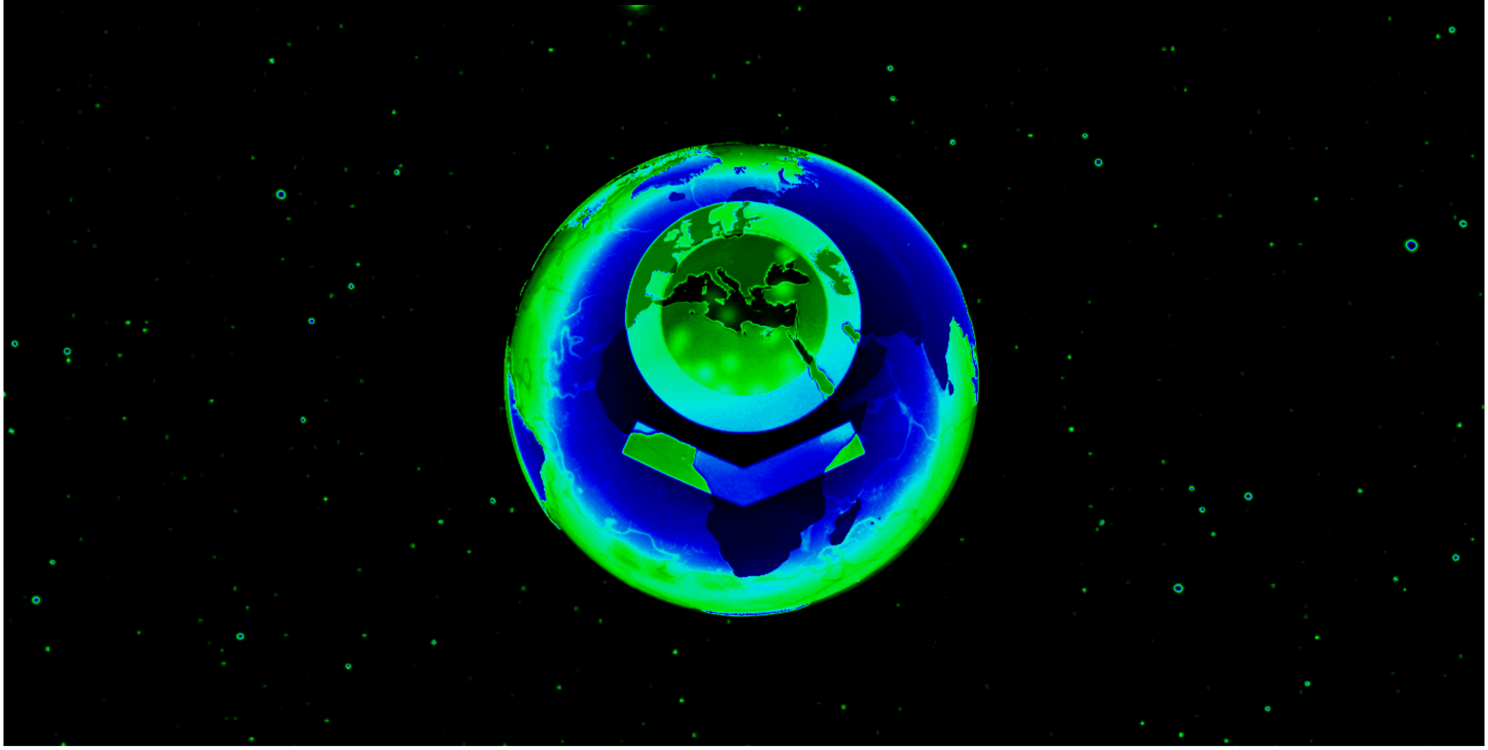


Illustration: Erik Carter for The Intercept

DONALD TRUMP HAS inherited the most powerful machine for spying ever devised. How this petty, vengeful man might wield and expand the sprawling American spy apparatus, already vulnerable to abuse, is disturbing enough on its own. But the outlook is even worse considering Trump's vast preference for private sector expertise and new strategic friendship with Silicon Valley billionaire investor Peter

Thiel, whose controversial (and opaque) company Palantir has long sought to sell governments an unmatched power to sift and exploit information of any kind. Thiel represents a perfect nexus of government clout with the kind of corporate swagger Trump loves. The Intercept can now reveal that Palantir has worked for years to boost the global dragnet of the NSA and its international partners, and was in fact co-created with American spies.

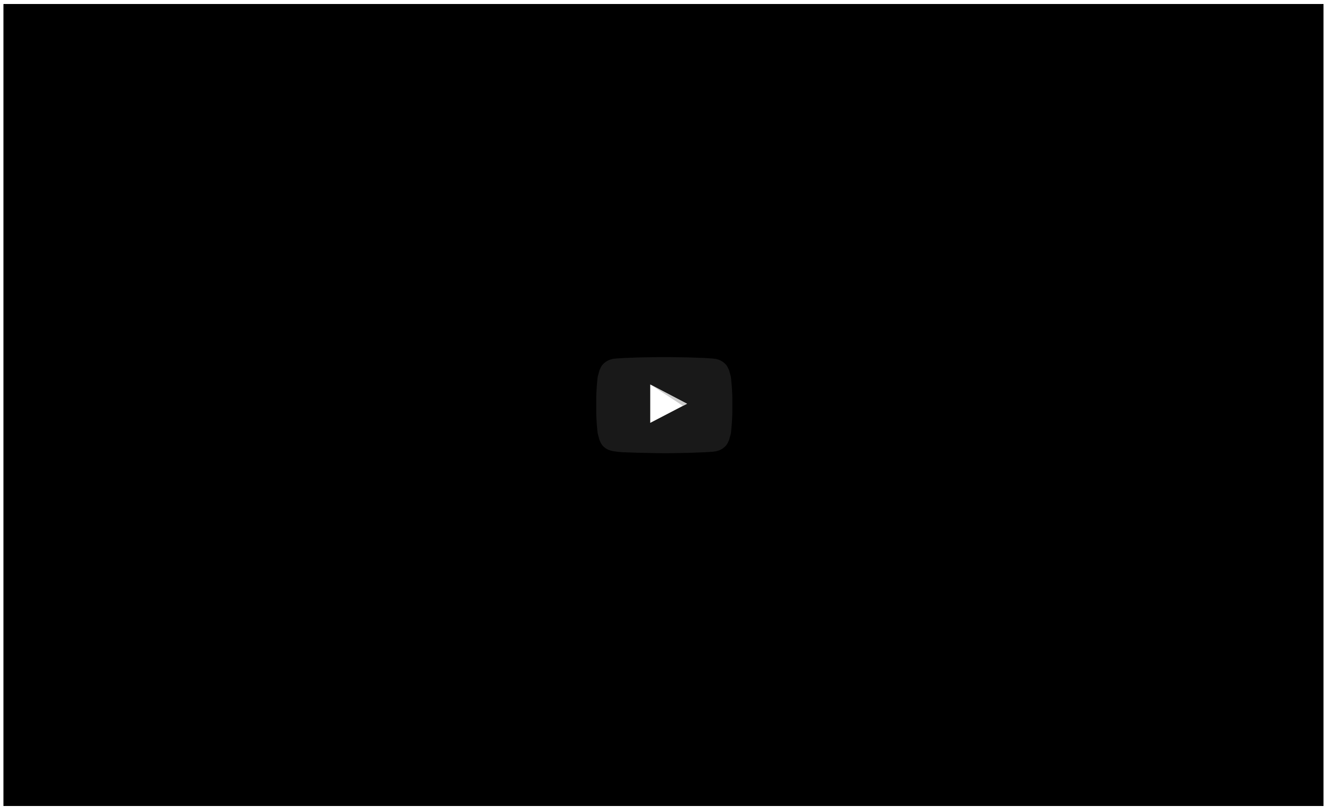
Peter Thiel became one of the American political mainstream's most notorious figures in 2016 (when it emerged he was bankrolling a lawsuit against Gawker Media, my former employer) even before he won a direct line to the White House. Now he brings to his role as presidential adviser decades of experience as kingly investor and token nonliberal on Facebook's board of directors, a Rolodex of software luminaries, and a decidedly Trumpian devotion to controversy and contrarianism. But perhaps the most appealing asset Thiel can offer our bewildered new president will be Palantir Technologies, which Thiel founded with Alex Karp and Joe Lonsdale in 2004.

Palantir has never masked its ambitions, in particular the desire to sell its services to the U.S. government — the CIA itself was an early investor in the startup through In-Q-Tel, the agency's venture capital branch. But Palantir refuses to discuss or even name its government clientele, despite landing "at least $1.2 billion" in federal contracts since 2009, according to an August 2016 report in Politico. The company was last valued at $20 billion and is expected to pursue an IPO in the near future. In a 2012 interview with TechCrunch, while boasting of ties to the intelligence community, Karp said nondisclosure contracts prevent him from speaking about Palantir's government work.

Alex Karp, co-founder and CEO of Palantir Technologies, speaks during the WSJDLive Global Technology Conference in Laguna Beach, Calif., on Oct. 26, 2016. Photo: Patrick T. Fallon/Bloomberg/Getty Images

"Palantir" is generally used interchangeably to refer to both Thiel and Karp's company and the software that company creates. Its two main products are Palantir Gotham and Palantir Metropolis, more geeky winks from a company whose Tolkien namesake is a type of magical sphere used by the evil lord Sauron to surveil, trick, and threaten his enemies across Middle Earth. While Palantir Metropolis is pegged to quantitative analysis for Wall Street banks and hedge funds, Gotham (formerly Palantir Government) is designed for the needs of intelligence, law enforcement, and homeland security customers. Gotham works by importing large reams of "structured" data (like spreadsheets) and "unstructured" data (like images) into one centralized database, where all of the information can be visualized and analyzed in one workspace. For example, a 2010 demo showed how Palantir Government could be used to chart the flow of weapons throughout the

Middle East by importing disparate data sources like equipment lot numbers, manufacturer data, and the locations of Hezbollah training camps. Palantir's chief appeal is that it's not designed to do any single thing in particular, but is flexible and powerful enough to accommodate the requirements of any organization that needs to process large amounts of both personal and abstract data.



A Palantir promotional video.

Despite all the grandstanding about lucrative, shadowy government contracts, co-founder Karp does not shy away from taking a stand in the debate over government surveillance. In a Forbes profile in 2013, he played privacy lamb, saying, "I didn't sign up for the government to know when I smoke a joint or have an affair. … We have to find places that we protect away from government so that we can all be the unique and interesting and, in my case, somewhat deviant people we'd like to be." In that same article, Thiel lays out Palantir's mission with privacy in mind: to "reduce terrorism while preserving civil liberties." After the first wave of revelations spurred by the whistleblower Edward Snowden, Palantir was quick to deny that it had any connection to the

NSA spy program known as PRISM, which shared an unfortunate code name with one of its own software products. The current iteration of Palantir's website includes an entire section dedicated to "Privacy & Civil Liberties," proclaiming the company's support of both:

> Palantir Technologies is a mission-driven company, and a core component of that mission is protecting our fundamental rights to privacy and civil liberties. …
>
> Some argue that society must "balance" freedom and safety, and that in order to better protect ourselves from those who would do us harm, we have to give up some of our liberties. We believe that this is a false choice in many areas. Particularly in the world of data analysis, liberty does not have to be sacrificed to enhance security. Palantir is constantly looking for ways to protect privacy and individual liberty through its technology while enabling the powerful analysis necessary to generate the actionable intelligence that our law enforcement and intelligence agencies need to fulfill their missions.

It's hard to square this purported commitment to privacy with proof, garnered from documents provided by Edward Snowden, that Palantir has helped expand and accelerate the NSA's global spy network, which is jointly administered with allied foreign agencies around the world. Notably, the partnership has included building software specifically to facilitate, augment, and accelerate the use of XKEYSCORE, one of the most expansive and potentially intrusive tools in the NSA's arsenal. According to Snowden documents published by The Guardian in 2013, XKEYSCORE is by the NSA's own admission its "widest reaching" program, capturing "nearly everything a typical user does on the internet." A subsequent report by The Intercept showed that XKEYSCORE's "collected communications not only include emails, chats, and web-browsing traffic, but also pictures, documents, voice calls, webcam photos, web searches, advertising analytics traffic, social media traffic, botnet traffic, logged keystrokes, computer network exploitation targeting, intercepted username and password pairs, file uploads to online services, Skype sessions, and more." For the NSA and its global partners, XKEYSCORE makes all of this as searchable as a hotel reservation site.

But how do you make so much data comprehensible for human spies? As the additional documents published with this article demonstrate, Palantir sold its services to make one of the most powerful surveillance systems ever devised even more powerful, bringing clarity and slick visuals to an ocean of surveillance data.

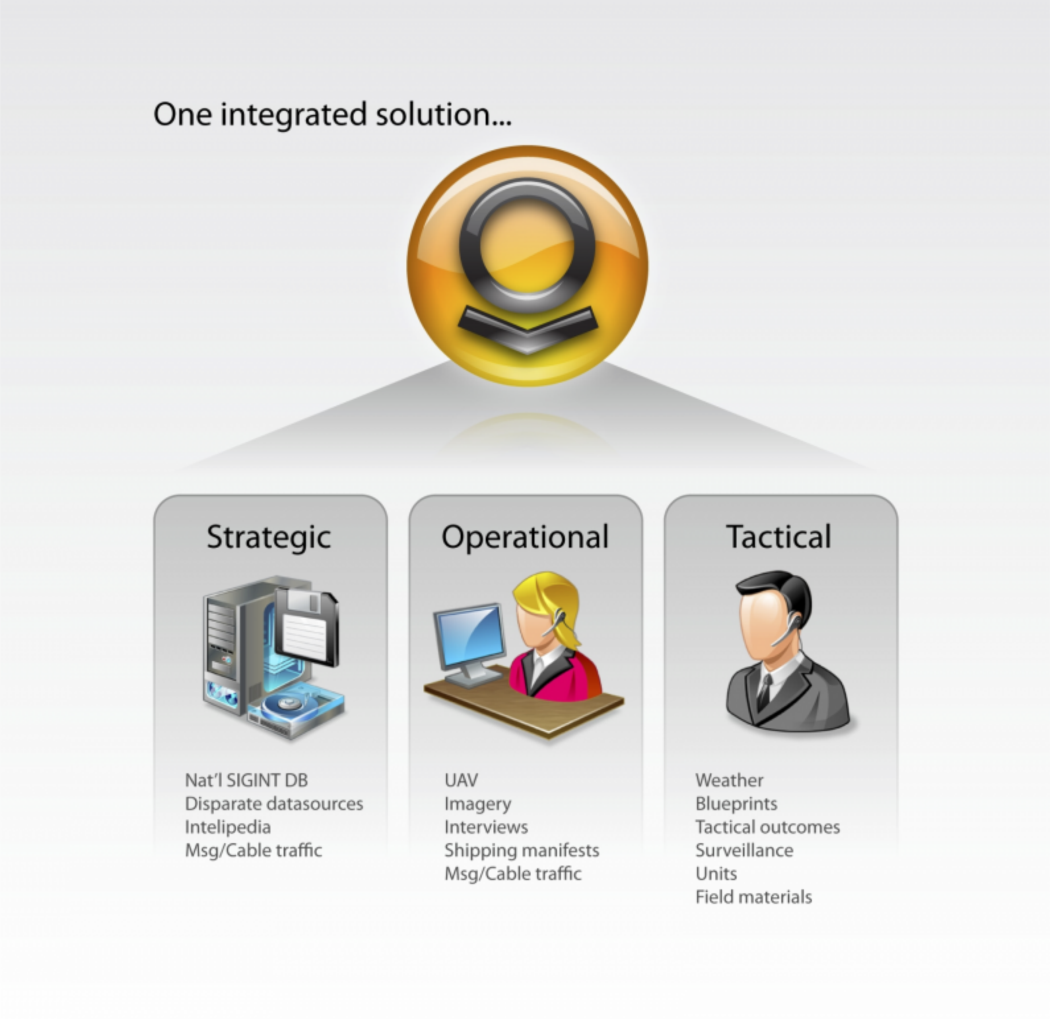
An office building occupied by the technology firm Palantir in McLean, Va., on Oct. 11, 2014.
Photo: Kristoffer Tripplaar/Sipa USA/AP

PALANTIR'S RELATIONSHIP WITH government spy agencies appears to date back to at least 2008, when representatives from the U.K.'s signals intelligence agency, Government Communications Headquarters, joined their American peers at VisWeek, an annual data visualization and computing conference organized by the Institute of Electrical and Electronics Engineers and the U.S. National Institute of Standards and Technology. Attendees from throughout government and academia gather to network with members of the private sector at the event, where they compete in teams to solve hypothetical data-based puzzles as part of the Visual Analytics Science and Technology (VAST) Challenge. As described in a document saved by GCHQ, Palantir fielded a team in 2008 and tackled one such scenario using its own software. It was a powerful marketing opportunity at a conference filled with potential buyers.

In the demo, Palantir engineers showed how their software could be used to identify Wikipedia users who belonged to a fictional radical religious sect and graph their social relationships. In Palantir's pitch, its approach to the VAST Challenge involved using software to enable "many analysts working together [to] truly leverage their collective mind." The fake scenario's target, a cartoonishly sinister religious sect called "the Paraiso Movement," was suspected of a terrorist bombing, but the unmentioned and obvious subtext of the experiment was the fact that such techniques could be applied to de-anonymize and track members of any political or ideological group. Among a litany of other conclusions, Palantir determined the group was prone to violence because its "Manifesto's intellectual influences include 'Pancho Villa, Che Guevara, Leon Trotsky, [and] Cuban revolutionary Jose Martí,' a list of military commanders and revolutionaries with a history of violent actions."

The delegation from GCHQ returned from VisWeek excited and impressed. In a classified report from those who attended, Palantir's potential for aiding the spy agency was described in breathless terms. "Palantir are a relatively new Silicon Valley startup who are sponsored by the CIA," the report began. "They claim to have significant involvement with the US intelligence community, although none yet at NSA." GCHQ noted that Palantir "has been developed closely internally with intelligence community users (unspecified, but likely to be the CIA given the funding)." The report described Palantir's demo as "so significant" that it warranted its own entry in GCHQ's classified internal wiki, calling the software "extremely sophisticated and mature. … We were *very* impressed. You need to see it to believe it."

The report conceded, however, that "it would take an enormous effort for an in-house developed GCHQ system to get to the same level of sophistication" as Palantir. The GCHQ briefers also expressed hesitation over the price tag, noting that "adoption would have [a] huge monetary … cost," and over the implications of essentially outsourcing intelligence analysis software to the private sector, thus making the agency "utterly dependent on a commercial product." Finally, the report added that "it is possible there may be concerns over security — the company have published a lot of information on their website about how their product is used in intelligence analysis, some of which we feel very uncomfortable about."



One integrated solution...

Strategic

Nat'l SIGINT DB
Disparate datasources
Intelipedia
Msg/Cable traffic

Operational

UAV
Imagery
Interviews
Shipping manifests
Msg/Cable traffic

Tactical

Weather
Blueprints
Tactical outcomes
Surveillance
Units
Field materials

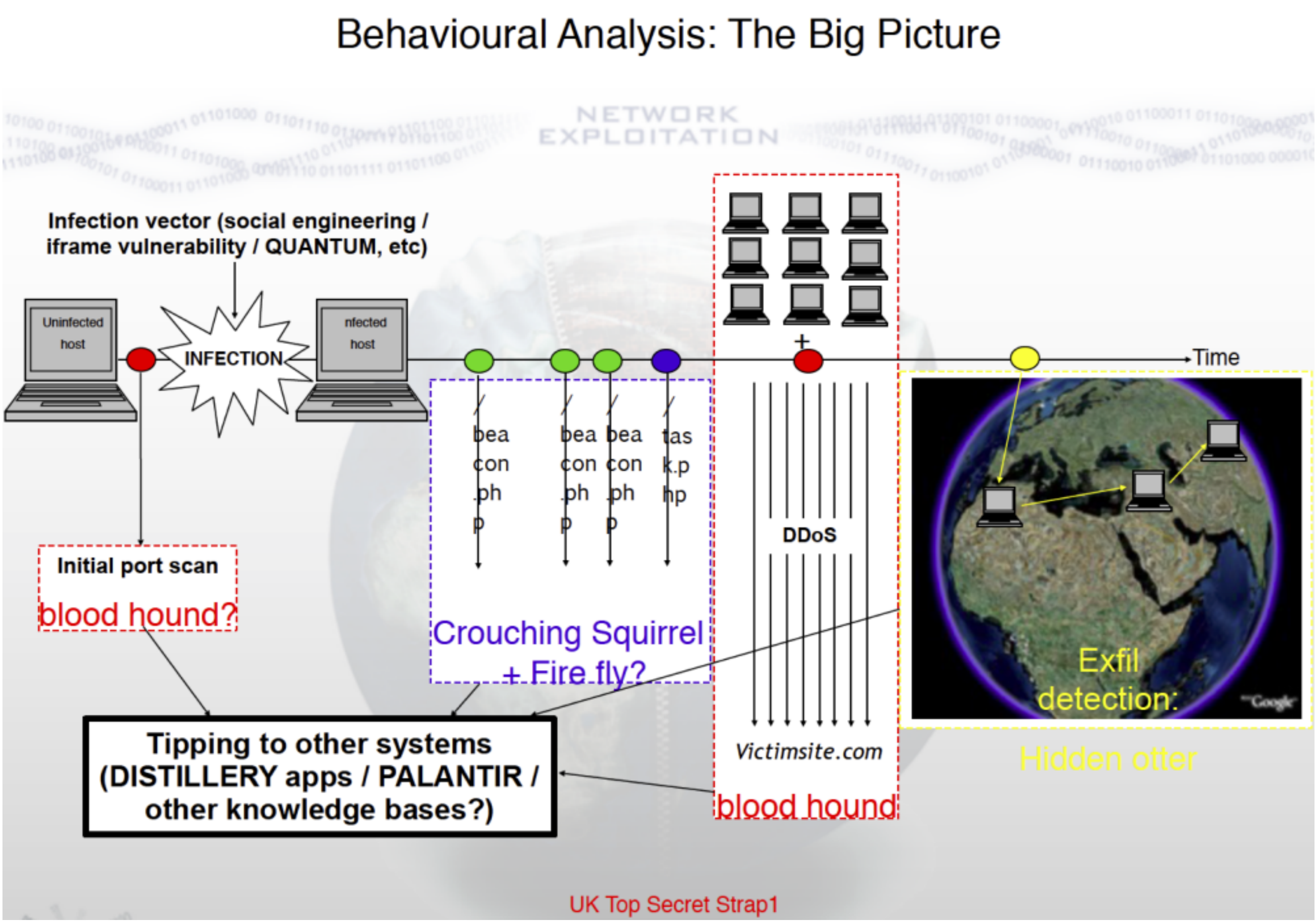
A page from Palantir's "Executive Summary" document, provided to government clients.

However anxious British intelligence was about Palantir's self-promotion, the worry must not have lasted very long. Within two years, documents show that at least three members of the "Five Eyes" spy alliance between the United States, the U.K., Australia, New Zealand, and Canada were employing Palantir to help gather and process data from around the world. Palantir excels at making connections between enormous, separate databases, pulling big buckets of information (call records, IP addresses, financial transactions, names, conversations, travel records) into one centralized heap and visualizing them coherently, thus solving one of the persistent problems of modern intelligence gathering: data overload.

A GCHQ wiki page titled "Visualisation," outlining different ways "to provide insight into some set of data," puts succinctly Palantir's intelligence value:

> Palantir is an information management platform for analysis developed by Palantir Technologies. It integrates structured and unstructured data, provides search and discovery capabilities, knowledge management, and collaborative features. The goal is to offer the infrastructure, or 'full stack,' that intelligence organizations require for analysis.

Bullet-pointed features of note included a "Graph View," "Timelining capabilities," and "Geo View."


Behavioural Analysis: The Big Picture

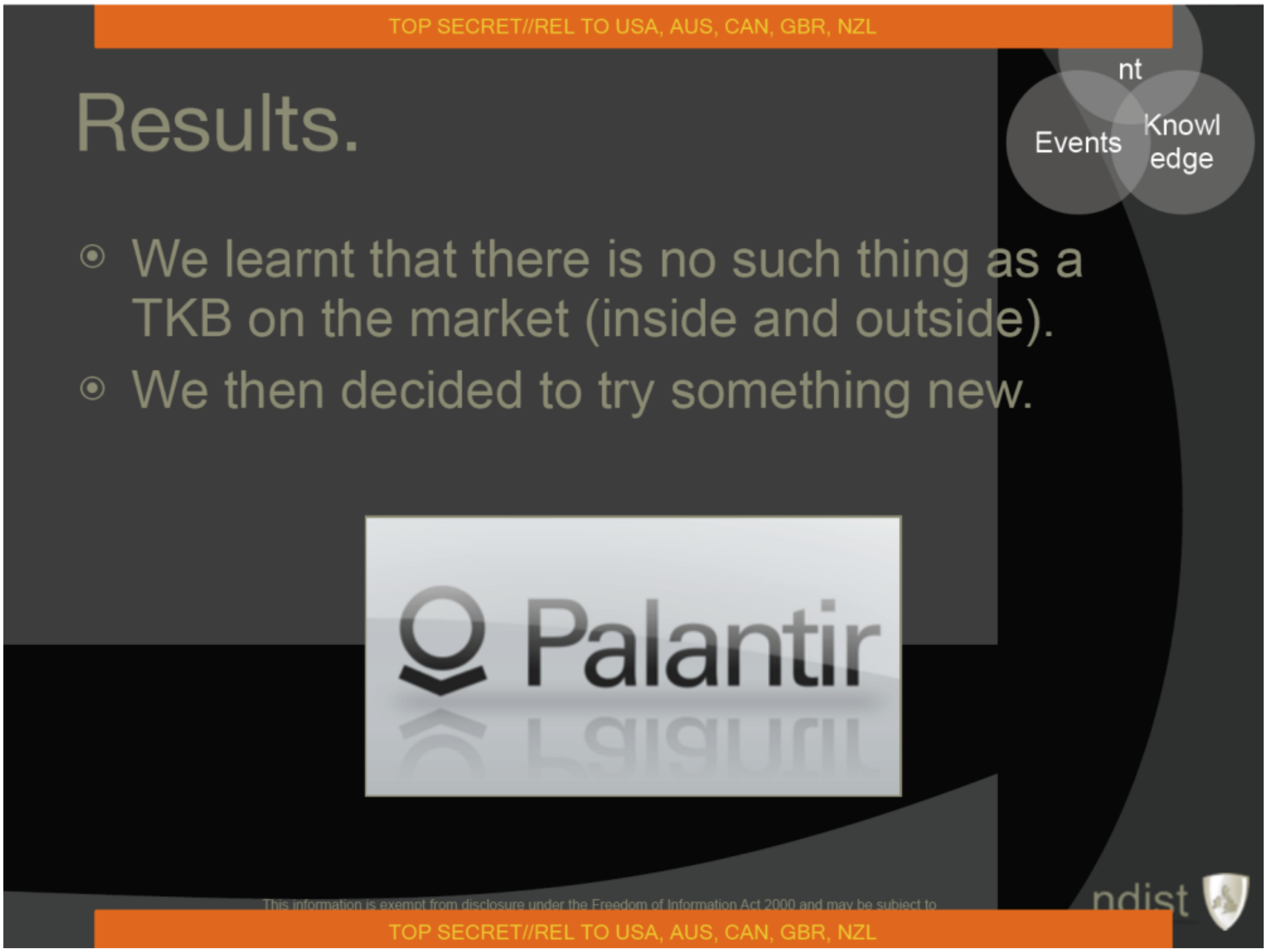
A GCHQ diagram indicates how Palantir could be used as part of a computer network attack.

Under the Five Eyes arrangement, member countries collect and pool enormous streams of data and metadata collected through tools like XKEYSCORE, amounting to tens of billions of records. The alliance is constantly devising (or attempting) new, experimental methods of prying data out of closed and private sources, including by hacking into computers and networks in non-Five Eyes countries and infecting them with malware.

A 2011 PowerPoint presentation from GCHQ's Network Defence Intelligence & Security Team (NDIST) — which, as The Intercept has previously reported, "worked to subvert anti-virus and other security software in order to track users and infiltrate networks" — mentioned Palantir as a tool for processing data gathered in the course of its malware-oriented work. Palantir's software was described as an "analyst workspace [for] pulling together disparate information and displaying it in novel ways," and was used closely in conjunction with other intelligence software tools, like the NSA's notorious XKEYSCORE search system. The novel ways of using Palantir for spying seemed open-ended, even imaginative: A 2010 presentation on the joint NSA-GCHQ "Mastering the Internet" surveillance program mentioned the prospect of running Palantir software on "Android handsets" as part of a SIGINT-based "augmented reality" experience. It's unclear what exactly this means or could even look like.

Above all, these documents depict Palantir's software as a sort of consolidating agent, allowing Five Eyes analysts to make sense of tremendous amounts of data that might have been otherwise unintelligible or highly time-consuming to digest. In a 2011 presentation to the NSA, classified top secret, an NDIST operative noted the "good collection" of personal data among the Five Eyes alliance but lamented the "poor analytics," and described the attempt to find new tools for SIGINT analysis, in which it "conducted a review of 14 different systems that might work." The review considered services from Lockheed

Martin and Detica (a subsidiary of BAE Systems) but decided on the up-and-comer from Palo Alto.



TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL

Results.

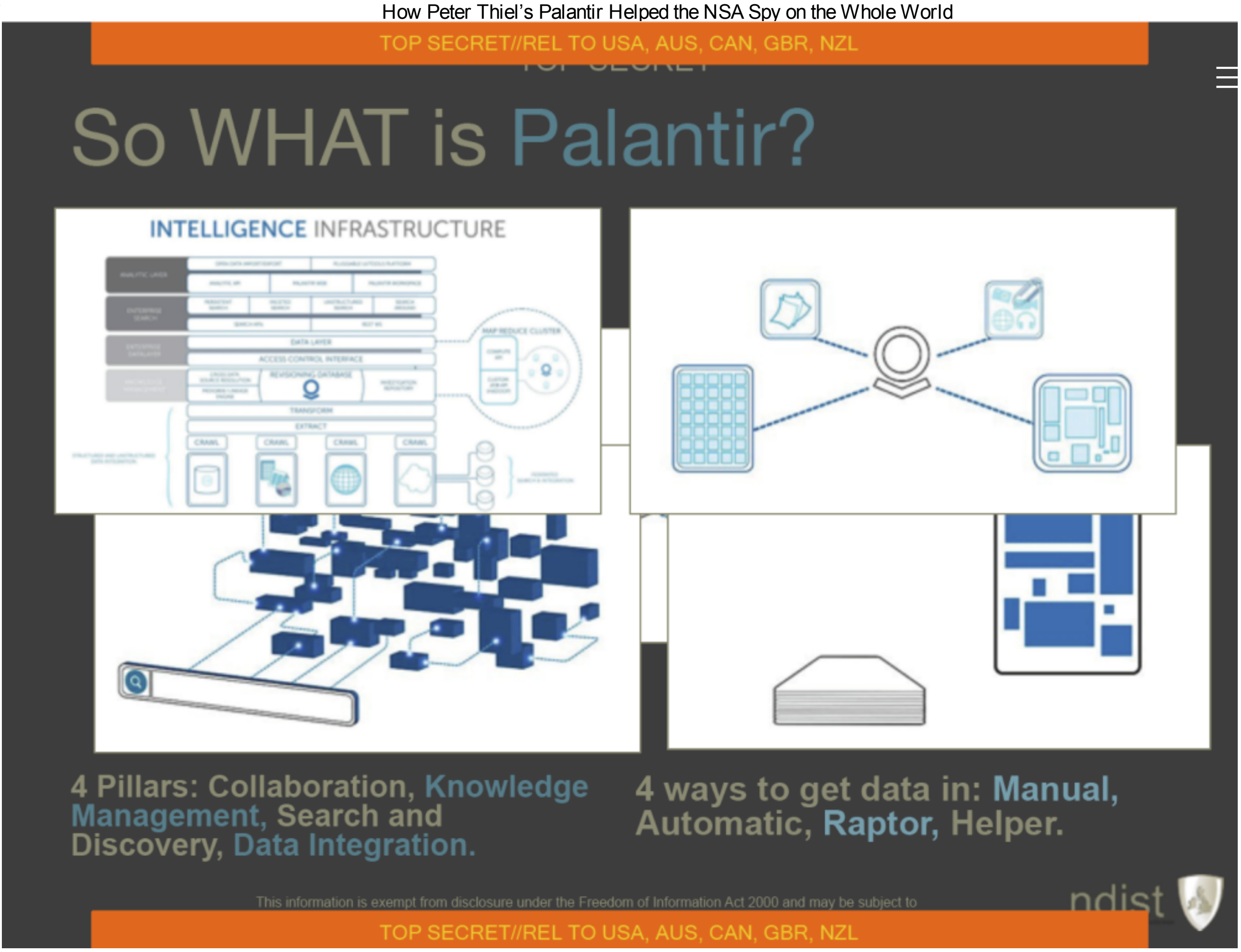
- We learnt that there is no such thing as a TKB on the market (inside and outside).
- We then decided to try something new.

nt
Events
Knowl edge
Palantir
ndist

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to

TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL

Palantir is described as having been funded not only by In-Q-Tel, the CIA's venture capital branch, but furthermore created "through [an] iterative collaboration between Palantir computer scientists and analysts from various intelligence agencies over the course of nearly three years." While it's long been known that Palantir got on its feet with the intelligence community's money, it has not been previously reported that the intelligence community actually helped build the software. The continuous praise seen in these documents shows that the collaboration paid off. Under the new "Palantir Model," "data can come from anywhere" and can be "asked whatever the analyst wants."



TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL

TOP SECRET

So WHAT is Palantir?

INTELLIGENCE INFRASTRUCTURE
ANALYTIC LAYER
ANALYTIC API
PALANTIR WEB
PALANTIR WORKSPACE
ENTERPRISE SEARCH
SEARCH APIs
REST WS
ENTERPRISE DATA LAYER
DATA LAYER
ACCESS CONTROL INTERFACE
KNOWLEDGE MANAGEMENT
REVISIONING DATABASE
INVESTIGATION REPOSITORY
TRANSFORM
EXTRACT
CRAWL
CRAWL
CRAWL
CRAWL
MAP REDUCE CLUSTER
COMPUTE API
STRUCTURED AND UNSTRUCTURED DATA INTEGRATION
FEDERATED SEARCH & INTEGRATION

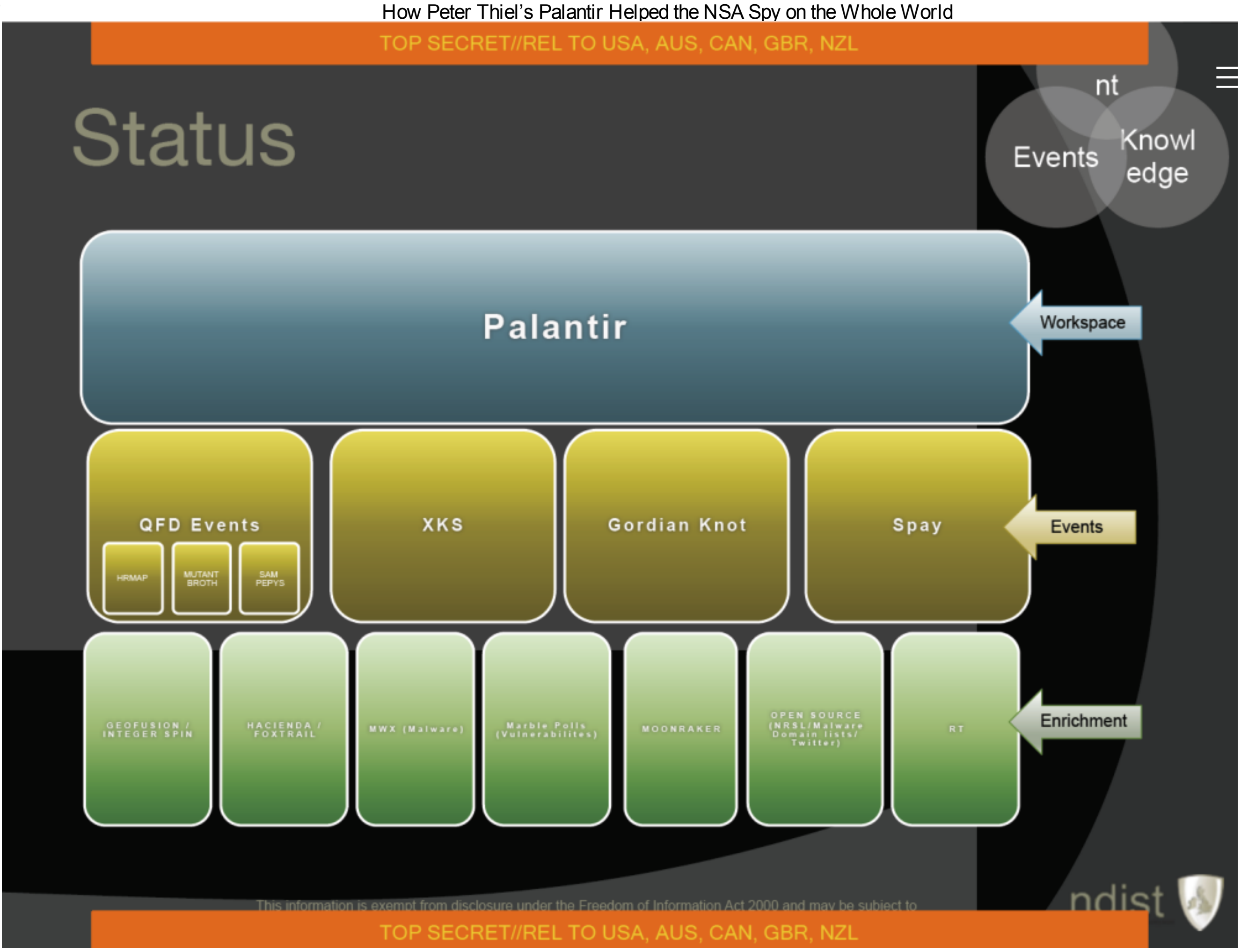
4 Pillars: Collaboration, Knowledge Management, Search and Discovery, Data Integration.

4 ways to get data in: Manual, Automatic, Raptor, Helper.

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to

ndist

TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL



TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL

Status

nt
Events
Knowl
edge

Palantir
Workspace

QFD Events
HRMAP
MUTANT BROTH
SAM PEPYS
XKS
Gordian Knot
Spay
Events

GEOFUSION / INTEGER SPIN
HACIENDA / FOXTRAIL
MWX (Malware)
Marble Polls (Vulnerabilites)
MOONRAKER
OPEN SOURCE (NRSL/Malware Domain lists/ Twitter)
RT
Enrichment

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to

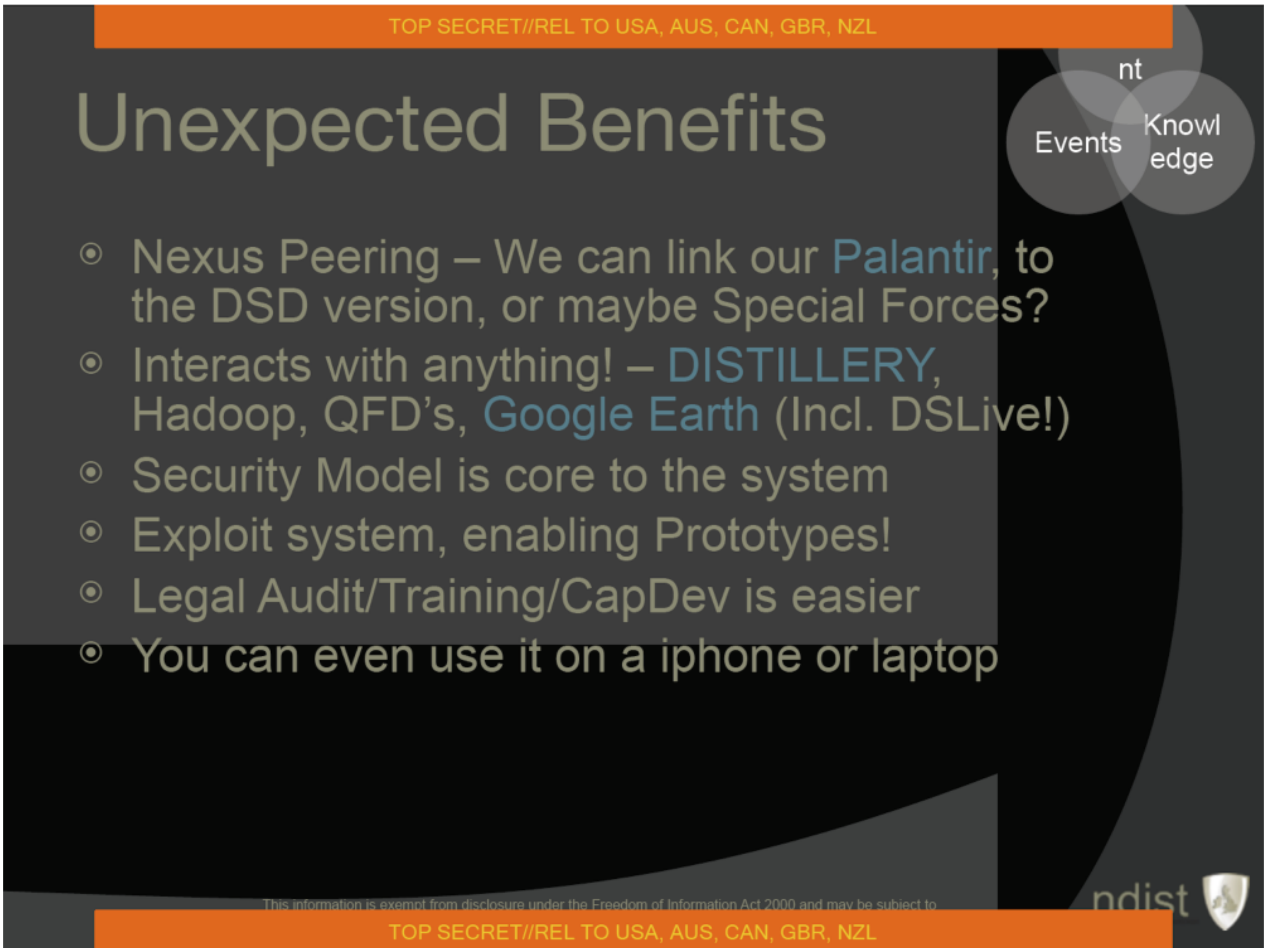
ndist

TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL

Along with Palantir's ability to pull in "direct XKS Results," the presentation boasted that the software was already connected to 10 other secret Five Eyes and GCHQ programs and was highly popular among analysts. It even offered testimonials (TWO FACE appears to be a code name for the implementation of Palantir):

> [Palantir] is the best tool I have ever worked with. It's intuitive, i.e. idiot-proof, and can do a lot you never even dreamt of doing.
>
> This morning, using TWO FACE rather than XKS to review the activity of the last 3 days. It reduced the initial analysis time by at least 50%.

Enthusiasm runs throughout the PowerPoint: A slide titled "Unexpected Benefits" reads like a marketing brochure, exclaiming that Palantir "interacts with anything!" including Google Earth, and "You can even use it on a iphone or laptop." The next slide, on "Potential Downsides," is really more praise in disguise: Palantir "Looks expensive" but "isn't as expensive as expected." The answer to "What can't it do?" is revealing: "However we ask, Palantir answer," indicating that the collaboration between spies and startup didn't end with Palantir's CIA-funded origins, but that the company was willing to create new features for the intelligence community by request.


nt
Events
Knowl edge
ndist

TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL

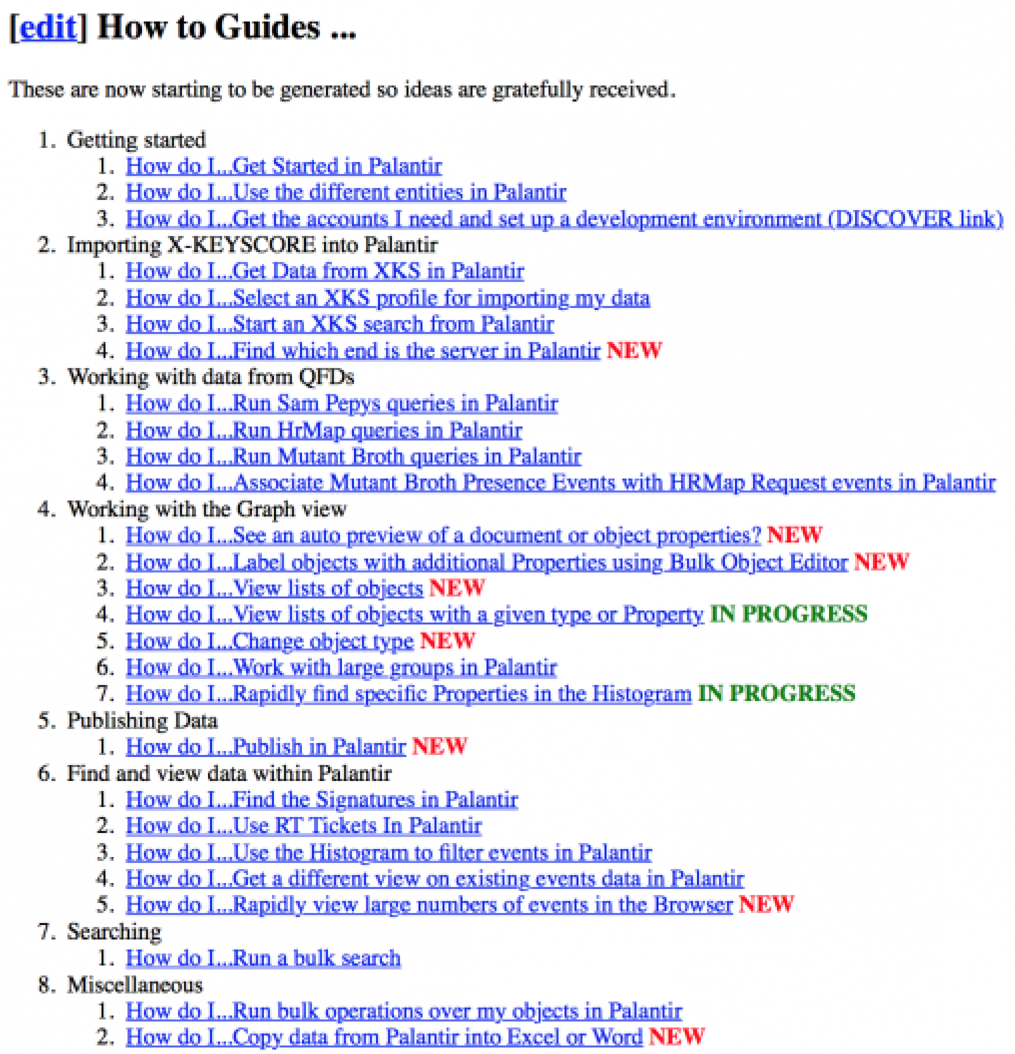
Unexpected Benefits

- Nexus Peering – We can link our Palantir, to the DSD version, or maybe Special Forces?
- Interacts with anything! – DISTILLERY, Hadoop, QFD's, Google Earth (Incl. DSLive!)
- Security Model is core to the system
- Exploit system, enabling Prototypes!
- Legal Audit/Training/CapDev is easier
- You can even use it on a iphone or laptop

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to

TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL

On GCHQ's internal wiki page for TWO FACE, analysts were offered a "how to" guide for incorporating Palantir into their daily routine, covering introductory topics like "How do I … Get Data from XKS in Palantir," "How do I … Run a bulk search," and "How do I … Run bulk operations over my objects in Palantir." For anyone in need of a hand, "training is currently offered as 1-2-1 desk based training with a Palantir trainer. This gives you the opportunity to quickly apply Palantir to your current work task." Palantir often sends "forward deployed engineers," or FDEs, to work alongside clients at their offices and provide assistance and engineering services, though the typical client does not have access to the world's largest troves of personal information. For analysts interested in tinkering with Palantir, there was even a dedicated instant message chat room open to anyone for "informally" discussing the software.



[edit] How to Guides ...

These are now starting to be generated so ideas are gratefully received.

1. Getting started
   1. How do I...Get Started in Palantir
   2. How do I...Use the different entities in Palantir
   3. How do I...Get the accounts I need and set up a development environment (DISCOVER link)
2. Importing X-KEYSCORE into Palantir
   1. How do I...Get Data from XKS in Palantir
   2. How do I...Select an XKS profile for importing my data
   3. How do I...Start an XKS search from Palantir
   4. How do I...Find which end is the server in Palantir **NEW**
3. Working with data from QFDs
   1. How do I...Run Sam Pepys queries in Palantir
   2. How do I...Run HrMap queries in Palantir
   3. How do I...Run Mutant Broth queries in Palantir
   4. How do I...Associate Mutant Broth Presence Events with HRMap Request events in Palantir
4. Working with the Graph view
   1. How do I...See an auto preview of a document or object properties? **NEW**
   2. How do I...Label objects with additional Properties using Bulk Object Editor **NEW**
   3. How do I...View lists of objects **NEW**
   4. How do I...View lists of objects with a given type or Property **IN PROGRESS**
   5. How do I...Change object type **NEW**
   6. How do I...Work with large groups in Palantir
   7. How do I...Rapidly find specific Properties in the Histogram **IN PROGRESS**
5. Publishing Data
   1. How do I...Publish in Palantir **NEW**
6. Find and view data within Palantir
   1. How do I...Find the Signatures in Palantir
   2. How do I...Use RT Tickets In Palantir
   3. How do I...Use the Histogram to filter events in Palantir
   4. How do I...Get a different view on existing events data in Palantir
   5. How do I...Rapidly view large numbers of events in the Browser **NEW**
7. Searching
   1. How do I...Run a bulk search
8. Miscellaneous
   1. How do I...Run bulk operations over my objects in Palantir
   2. How do I...Copy data from Palantir into Excel or Word **NEW**

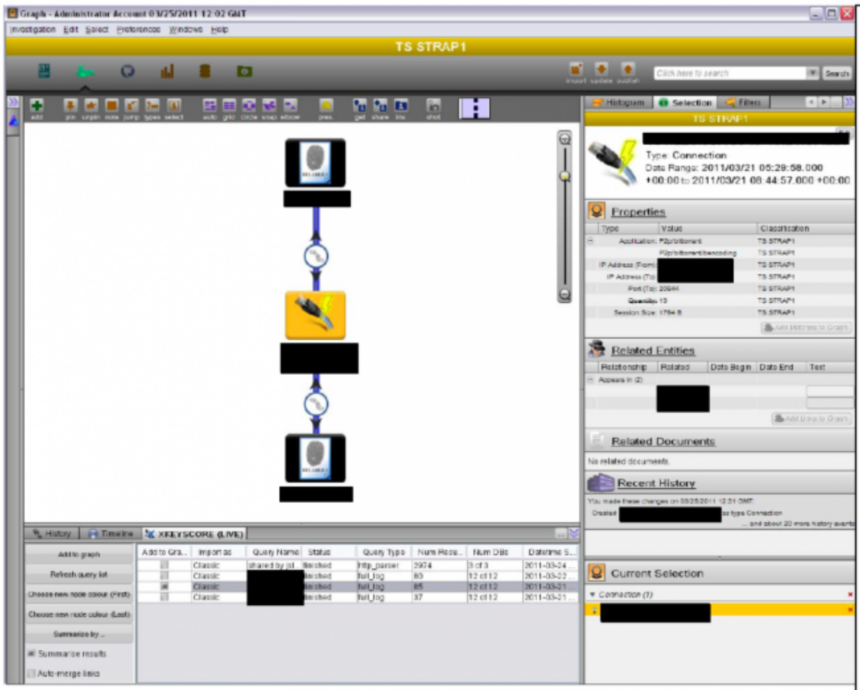
The GCHQ wiki includes links to classified webpages describing Palantir's use by the Australian Defence Signals Directorate (now called the Australian Signals Directorate) and to a Palantir entry on the NSA's internal "Intellipedia," though The Intercept does not have access to copies of the linked sites. However, embedded within Intellipedia HTML files available to The Intercept are references to a variety of NSA-Palantir programs, including "Palantir Classification Helper," "[Target Knowledge Base] to Palantir PXML," and "PalantirAuthService." (Internal Palantir documents obtained by TechCrunch in 2013 provide additional confirmation of the NSA's relationship with the company.)

One Palantir program used by GCHQ, a software plug-in named "Kite," was preserved almost in its entirety among documents provided to The Intercept. An analysis of Kite's source code shows just how much flexibility the company afforded Five Eyes spies. Developers and analysts could ingest data locally using either Palantir's "Workspace" application or Kite. When they were satisfied the process was working properly, they could push it into a Palantir data repository where other Workspace users could also access it, almost akin to a Google Spreadsheets collaboration. When analysts were at their Palantir workstation, they could perform simple imports of static data, but when they wanted to perform more complicated tasks like import databases or set up recurring automatic imports, they turned to Kite.

Kite worked by importing intelligence data and converting it into an XML file that could be loaded into a Palantir data repository. Out of the box, Kite was able to handle a variety of types of data (including dates, images, geolocations, etc.), but GCHQ was free to extend it by writing custom fields for complicated types of data the agency might need to analyze. The import tools were designed to handle a variety of use cases, including static data sets, databases that were updated frequently, and data stores controlled by third parties to which GCHQ was able to gain access.

This collaborative environment also produced a piece of software called "XKEYSCORE Helper," a tool programmed with Palantir (and thoroughly stamped with its logo) that allowed analysts to essentially import data from the NSA's pipeline, investigate and visualize it through Palantir, and then presumably pass it to fellow analysts or Five Eyes intelligence partners. One of XKEYSCORE's only apparent failings is that it's so incredibly powerful, so effective at vacuuming personal metadata from the entire internet, that the volume of information it extracts can be overwhelming. Imagine trying to search your Gmail account, only the results are pulled from every Gmail inbox in the world.

TOP SECRET STRAP 1



[redacted]

Type: Connection
Date Range: 2011/03/21 05:28:58.000 +00:00 to 2011/03/21 08:44:57.000 +00:00

Properties

Type	Value	Classification
Application:	P2p/bittorrent	TS STRAP1
	P2p/bittorrent/bencoding	TS STRAP1
IP Address (From):	[redacted]	TS STRAP1
IP Address (To):		TS STRAP1
Port (To):	20644	TS STRAP1
Quantity:	19	TS STRAP1
Session Size:	1764 B	TS STRAP1

Related Entities

Relationship	Related	Date Begin	Date End	Text
Appears In (2)				
	[redacted]			

Related Documents

No related documents.

Recent History

You made these changes on 03/25/2011 12:31 GMT:
Created [redacted] as type Connection
... and about 20 more history events

Add to Gra...	Import as	Query Name	Status	Query Type	Num Resu...	Num DBs	Datetime S...
☐	Classic	shared by jsl...	finished	http_parser	2974	3 of 3	2011-03-24 ...
☐	Classic	[redacted]	finished	full_log	80	12 of 12	2011-03-22 ...
☒	Classic		finished	full_log	85	12 of 12	2011-03-21 ...
☐	Classic		finished	full_log	37	12 of 12	2011-03-21 ...

In this example, I removed all the other data from the input from the graph.

There are a few things to note from the results of this import:

- Quantity records the number of results which matched that histogram criteria (In this case 19). This matches up with the XKEYSCORE histogram grid
- Session size is a sum of all session sizes for this histogrammed piece of data. This allows you to see the total amount of data being sent from one IP to another, in this case also summarised by destination port.
- "Application" shows the different fingerprints hit on for this summary event. For example, if X contacts Y and it is picked up by fingerprints foo on connection 1 and bar on connection 2, the summarised connection between X and Y will list "foo" and "bar" as applications
- Time metadata is preserved in that you can view the first time this event occurred and the last.

3 of 6

[redacted]

TOP SECRET STRAP 1

MAKING XKEYSCORE MORE intelligible — and thus much more effective — appears to have been one of Palantir's chief successes. The helper tool, documented in a GCHQ PDF guide, provided a means of transferring data captured by the NSA's XKEYSCORE directly into Palantir, where presumably it would be far easier to analyze for, say, specific people and places. An analyst using XKEYSCORE could pull every IP address in Moscow and Tehran that visited a given website or made a Skype call at 14:15 Eastern Time, for example, and then import the resulting data set into Palantir in order to identify additional connections between the addresses or plot their positions using Google Earth.

Palantir was also used as part of a GCHQ project code-named LOVELY HORSE, which sought to improve the agency's ability to collect so-called open source intelligence — data available on the public internet, like tweets, blog posts, and news articles. Given the "unstructured" nature of this kind of data, Palantir was cited as "an enrichment to existing [LOVELY HORSE] investigations … the content should then be viewable in a human readable format within Palantir."

Palantir's impressive data-mining abilities are well-documented, but so too is the potential for misuse. Palantir software is designed to make it easy to sift through piles of information that would be completely inscrutable to a human alone, but the human driving the computer is still responsible for making judgments, good or bad.

A 2011 document by GCHQ's SIGINT Development Steering Group, a staff committee dedicated to implementing new spy methods, listed some of these worries. In a table listing "risks & challenges," the SDSG expressed a "concern that [Palantir] gives the analyst greater potential for going down too many analytical paths which could distract from the intelligence requirement." What it could mean for analysts to distract themselves by going down extraneous "paths" while browsing the world's most advanced spy machine is left unsaid. But Palantir's data-mining abilities were such that the SDSG wondered if its spies should be blocked from having full access right off the bat and suggested configuring Palantir software so that parts would "unlock … based on analysts skill level, hiding buttons and features until needed and capable of utilising." If Palantir succeeded in fixing the intelligence problem of being overwhelmed with data, it may have created a problem of over-analysis — the company's software offers such a multitude of ways to visualize and explore massive data sets that analysts could get lost in the funhouse of infographics, rather than simply being overwhelmed by the scale of their task.

If Palantir's potential for misuse occurred to the company's spy clients, surely it must have occurred to Palantir itself, especially given the company's aforementioned "commitment" to privacy and civil liberties. Sure enough, in 2012 the company announced the formation of the Palantir Council of Advisors on Privacy and Civil Liberties, a committee of academics and consultants with expertise in those fields. Palantir claimed that convening the PCAP had "provided us with invaluable guidance as we try to responsibly navigate the often ill-defined legal, political, technological, and ethical frameworks that sometimes govern the various activities of our customers," and continued to discuss the privacy and civil liberties "implications of product developments and to suggest potential ways to mitigate any negative effects." Still, Palantir made clear that the "PCAP is advisory only — any decisions that we make after consulting with the PCAP are entirely our own."

What would a privacy-minded conversation about privacy-breaching software look like? How had a privacy and civil liberties council navigated the fact that Palantir's clientele had directly engaged in one of the greatest privacy and civil liberties breaches of all time? It's hard to find an answer.

Palantir wrote that it structured the nondisclosure agreement signed by PCAP members so that they "will be free to discuss anything that they learn in working with us unless we clearly designate information as proprietary or otherwise confidential (something that we have rarely found necessary except on very limited occasions)." But despite this assurance of transparency, all but one of the PCAP's former and current members either did not return a request for comment for this article or declined to comment citing the NDA.

The former PCAP member who did respond, Stanford privacy scholar Omer Tene, told The Intercept that he was unaware of "any specific relationship, agreement, or project that you're referring to," and said he was not permitted to answer whether Palantir's work with the intelligence community was ever a source of tension with the PCAP. He declined to comment on either the NSA or GCHQ specifically. "In general," Tene said, "the role of the PCAP was to hear about client engagement or new products and offerings that the company was about to launch, and to opine as to the way they should be set up or delivered in order to minimize privacy and civil liberties concerns." But without any further detail, it's unclear whether the PCAP was ever briefed on the company's work for spy agencies, or whether such work was a matter of debate.

There's little detail to be found on archived versions of Palantir's privacy and civil liberties-focused blog, which appears to have been deleted sometime after the PCAP was formed. Palantir spokesperson Matt Long told The Intercept to contact the Palantir media team for questions regarding the vanished blog at the same email address used to reach Long in the first place. Palantir did not respond to additional repeated requests for comment and clarification.

A GCHQ spokesperson provided a boilerplate statement reiterating the agency's "longstanding policy" against commenting on intelligence matters and asserted that all its activities are "carried out in accordance with a strict legal and policy framework." The NSA did not provide a response.

Anyone worried that the most powerful spy agencies on Earth might use Palantir software to violate the privacy or civil rights of the vast number of people under constant surveillance may derive some cold comfort in a portion of the user agreement language Palantir provided for the Kite plug-in, which stipulates that the user will not violate "any applicable law" or the privacy or the rights "of any third party." The world will just have to hope Palantir's most powerful customers follow the rules.

Documents published with this article:

- GCHQ VisWeek 2008 Conference Report
- Palantir Executive Summary
- NDIST Cyber Defence
- Mastering the Internet
- The Tale of Two Sources
- TWO FACE on GCHQ Wiki
- XKEYSCORE Helper Notes
- SDSG Integrated Analytics Workshop

Listen to Jeremy Scahill's interview with Sam Biddle on Episode 4 of Intercepted (begins at 32:05).

Intercepted with Jeremy Scahill

The Undisciplined Authoritarian

Journalist James Risen faced imprisonment under Obama's Justice Department and is preparing to do…

01:08:31

RELATED

Peter Thiel's CIA-Backed Data Mining Company Wins Court Battle Against the U.S. Army

Forget Trump: Peter Thiel Is So Dangerous and Fascinating You Have to Watch Him Tonight

Apple, Google and Others at Trump Tech Summit Have Stashed $560 Billion in Profits Overseas

Transition Adviser Peter Thiel Could Directly Profit From Mass Deportations

Trump Homeland Security Adviser Helped Contractors Profit Off Harsh Deportation Policies

Popular Security Software Came Under Relentless NSA and GCHQ Attacks

CONTACT THE AUTHOR:

Sam Biddle

✉ sam.biddle@theintercept.com

@samfbiddle

ADDITIONAL CREDITS:

Research: John Thomason, Talya Cooper and Westley Hennigh-Palermo.

101 Comments

The Intercept_

Newsletter

Don’t miss the best of The Intercept

Enter your email address

Email list managed by MailChimp