

ATTACKED

How corrupt politicians use taxpayer-paid resources for reprisal campaigns against the public and how you can flip-the-game on the bad guys



By ProPublica Submissions Group

Revision 2.1

Next major revision due Jan. 12, 2018

Daily minor revisions are provided in the online versions via collaborative public wiki editing

SECTIONS:

- **What is a political “hit-job”?**
- **Know Your Enemies**
- **The CIA Leak**
- **The Cleantech Crash Insider Attack Tools**
- **Google Owns Over 100 Companies Designed To Operate Coups, Character Assassinations and Election Rigging.**
- **Gawker Media Tabloid Empire Is A Character Assassination Squad**
- **How new technologies get regularly attacked by the Silicon Valley campaign financiers**
- **The Obama West Wing Has An Attack Team It Uses Against Taxpayers it Does Not Like**
- **Rights and use notices**

What is a political “hit-job”?

When you hear the term “...they put a hit job on him”, images of Al Capone-like gangsters with Tommy Guns and shootings in dark alleyways come to mind. In political campaigns and criminal crony corruption schemes, the gangsters use internet servers and lasers instead of Tommy Guns but the end result is the same. A person shot in the head with a bullet and a person shot with a \$50 million internet character assassination program are both, essentially, dead.

This book documents and details the abuses of process and office used by some political officials when they are trying to cover up their crimes. You will learn about every one of their illegal attack and character assassination tactics and how to over-come each and every one of them without breaking a single law. Not only will you terminate the bad guys using 100% legal means, the FBI, the U.S. Congress and hundreds of millions of voters will help you do it.

Silicon Valley Technology Oligarchs and Venture Capitalists are a monopolistic Cartel. This is proven by their email leaks, “*AngelGate Scandal*” documents, their loss in the “*No Poaching Class-Action Lawsuit*” against them and WIKILEAKS documents. The Detroit Auto industry has a monopolistic Cartel. The Defense aircraft sales industry and the large pharmaceutical industry has a monopolistic Cartel. Hollywood feature film producers have a monopolistic Cartel. Because the frat-house boys club culture indoctrinates the founders and members of these Cartels, they develop a culture where they believe that rules and laws do not apply to them because of their wealth and self-perceived privilege.

This is not an anti-government book. It was written by law enforcement and Congressional experts who seek to make sure the law is upheld. This is an anti-crime book.

White House staff, Governor’s office Chiefs-of-Staff and Agency bosses order and support these attacks in the U.S.A. It is the George Soros, The Elon Musk’s, The John Doerr’s, The Larry Page’s, The Eric Schmidt’s, The Vinod Khosla’s and related quid-pro-quo crony payola campaign financiers who pay for, and implement these attacks, using private contractors Media Matters, Gawker Media, Jalopnik, Jezebel, Facebook, Twitter, Facebook, IN-Q-Tel, JigSaw, New America Foundation and other sketchy operations. These private media attack resources claim to be one thing in public but turn out to be something entirely different in private. A small number of rogue operators inside the NSA, CIA, FBI and White House sell their services, illegally, to anybody who will pay. The good guys in those agencies never do those things. This report describes what the “bad guys” get up to so that you can recognize their crimes, report them and interdict them.

This is an anti-corruption and anti-crime book. It incorporates investigative reports from a number of sources.

Know Your Enemies

On October 10, 2013, Luke Bencie, President of Security Management International, LLC, spoke at IWP about his new book, "Among Enemies: Counter-Espionage for Business Travelers."

He described the difference between counterespionage (which is more defensive) and counterintelligence (which can be defensive or offensive), as well as the difference between economic espionage (conducted primarily by a state sponsor) and industrial espionage (conducted by others in industry).

Although some may be naïve about the extent to which economic espionage occurs, Mr. Bencie noted that the FBI Strategic Plan found that, next to terrorism, economic espionage is the greatest threat from other countries. In fact, in FY12, US firms lost about \$13 billion due to economic espionage.

He described what types of industrial information is most often stolen - from information about aeronautics to everyday products. He outlined some of China's concerted economic espionage efforts, including its 863 Program.

Luke's book: "***Among Enemies: Counter-Espionage for Business Travelers.***" is available on most online bookstores. It is essential reading for anyone who may have stirred the ire of a politician or political campaign manipulation group. As you read the book, simply remember that every form of industrial espionage and dirty tricks tactic described in the book is probably being done to you, right now, in your own home, or office, if you have competed with the interests of a political campaign or their crazed Silicon Valley tech oligarch financiers.

Luke Bencie is one of the most recognized security consultants anywhere in the world. He is the Managing Director of Security Management International (SMI) and the author of *Among Enemies: Counter-Espionage for the Business Traveler* and *Global Security Consulting: How to Build a Thriving International Practice*. Mr. Bencie has been a consultant to the U.S. Department of State, U.S. Department of Defense, Fortune 500 companies, as well as foreign governments. He has worked in over 100 countries and has trained thousands of police, intelligence and military officers in the U.S. and abroad in the fields of counterterrorism, counterintelligence and operational surveillance. Prior to establishing SMI, Mr. Bencie was a senior security consultant for Raytheon Company in the Intelligence and Information Systems Division. Mr. Bencie previously served on the U.S. Department of State's Foreign Emergency Support Team. In this capacity, he was responsible for immediately responding to terrorist attacks carried out against U.S. targets overseas; subsequently serving in Afghanistan, Iraq, Libya and other global hotspots.

A quick look on the internet discloses discussions such as these:

"...Xbee 802.15.4 - Security Research project to assess the capabilities of the Arduino compatible FreakLabs Chibi

Zigbee Multi-Channel Sniffer - Using the Chibi as a channel scanning, self contained, sniffer with screen and MicroSD
Arduino Attack platform - Research project to develop code for the Arduino platform that could be used for penetration testing
Social Intelligence gathering - Research project to develop code for collecting and aggregating social media feeds (Private)
OSINT - Project to collect / aggregate open source intelligence sources into a concise set of functional tools
GnuRadio - Customized scripts and layouts for the Funcube DVB-T SDR radio devices
AIMEE - Air Intercepted Messaging & Electronic Espionage
FSCD - Development of scripts for dumping configuration settings for various scanners that allow serial connectivity
MASINT - Research Project looking into Measurement and Signal / Signature Intelligence (Private)
Fonera Interceptor - A spin off the Hak5 Interceptor. This project focused on incorporating Jasenger, dsniff and numerous other tools into one device
Op Code Database - JMP positions for Windows XP, win7, Win8, 2003, 2008 (Private)
BacNET/IP Pentest Framework - Research project to develop and test BacNET/IP security tools for interception, Spoofing, interrogation and DoS
Myiasis Project - Counter Espionage for Business travelers and hackers. Development of embedded microcontrollers for the detection of malicious activity
Feltcher - Raspberry Pi as a USB attack platform with menu driven payload selection and deployment
BotBuilder - (PoC) Development of scripts to automatically identify vulnerable systems, deploy payload and add them to C&C
BBB-SDR - Development of scripts for Beagle Bone Black and SDR
NACTans - Network Access Control circumvent and testing platform...

While this may look like nonsense programmer geek talk, this kind of discussion details NSA, CIA, KGB-class interception and interdiction technologies to allow anyone to turn anything you own into a listening and file theft device.

Those not satisfied with just acting like the CIA to screw with your life can now easily acquire the actual hacking and dirty tricks software that the CIA uses and the KGB/FSB copies and uses right back at them.

The DIA found Bin Laden by using interdiction technology and “following-the-phones”. Now any 14 year kid or political campaign manager has all of those spy tools at his fingertips...



The CIA Leak

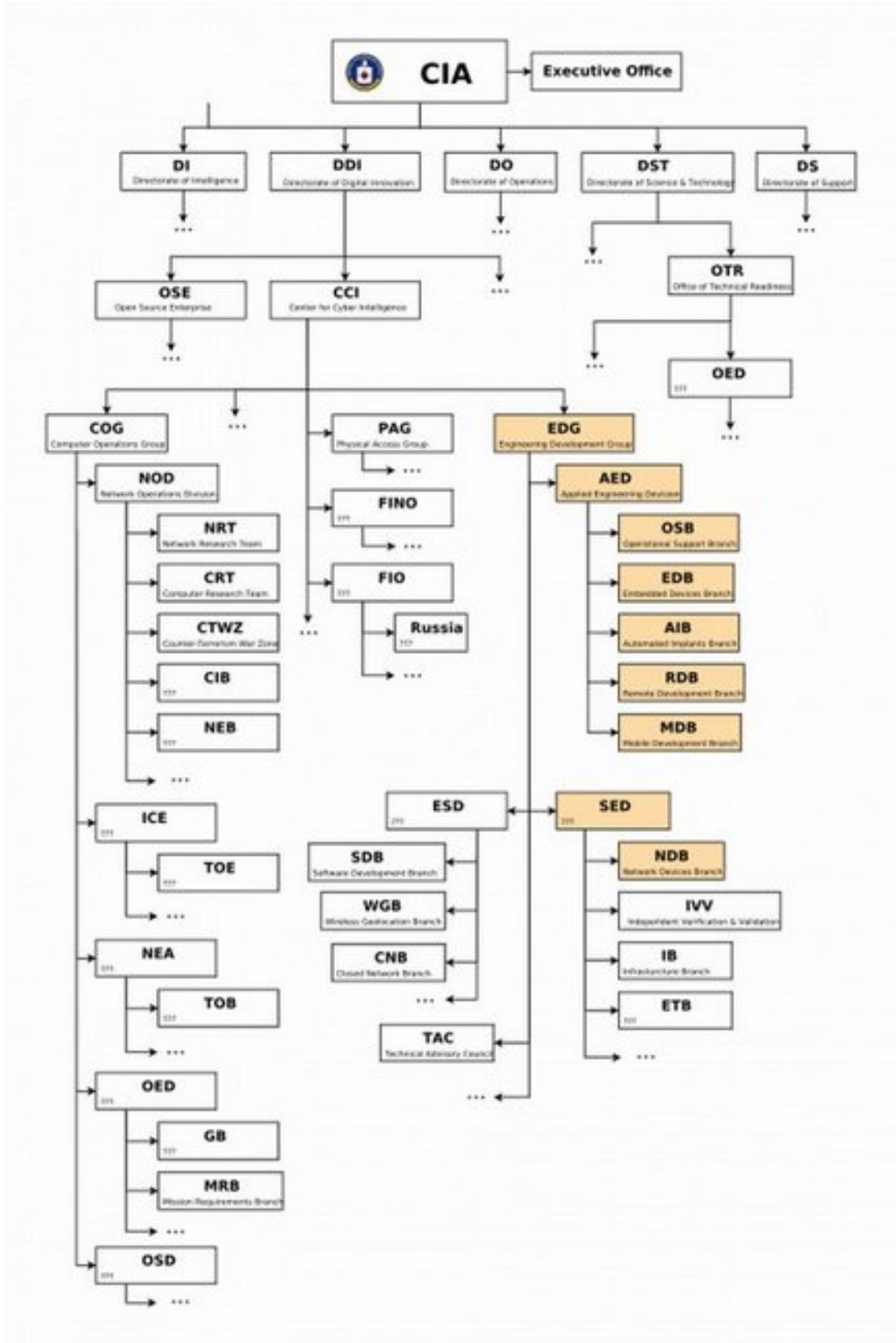
ALMOST ALL OF THE CIA SOFTWARE TO CRASH TESLA'S, AIRPLANES AND OTHER THINGS FOR ASSASSINATIONS IS NOW LOOSE IN THE WILD

Wikileaks Unveils 'Vault 7': "The Largest Ever Publication Of Confidential CIA Documents"; Another Snowden Emerges



by [Tyler Durden](#)

WikiLeaks has [published](#) what it claims is the largest ever release of confidential documents on the CIA. It includes more than 8,000 documents as part of 'Vault 7', a series of leaks on the agency, which have allegedly emerged from the CIA's [Center For Cyber Intelligence in Langley](#), and which can be seen on the org [chart below, which Wikileaks also released](#):



[A total of 8,761 documents have been published](#) as part of ‘Year Zero’, the first in a series of leaks the whistleblower organization has dubbed ‘Vault 7.’ WikiLeaks said that ‘Year Zero’ revealed details of the CIA’s “global covert hacking program,” including “weaponized exploits” used against company products including “*Apple’s iPhone, Google’s Android and Microsoft’s Windows and even Samsung TVs, which are turned into covert microphones.*”

WikiLeaks tweeted the leak, which it claims came from a network inside the CIA’s Center for Cyber Intelligence in Langley, Virginia.

Among the more notable disclosures which, if confirmed, "[would rock the technology world](#)", the CIA had managed to bypass encryption on popular phone and messaging services such as Signal, WhatsApp and Telegram. According to the statement from WikiLeaks, government hackers can penetrate Android phones and collect “audio and message traffic before encryption is applied.”

Another profound revelation is that the CIA can engage in "false flag" cyberattacks which portray Russia as the assailant. Discussing the CIA's Remote Devices Branch's UMBRAGE group, Wikileaks' source notes that it "collects and maintains a substantial library of attack techniques 'stolen' from malware produced in other states including the Russian Federation.

"With UMBRAGE and related projects the CIA cannot only increase its total number of attack types but also misdirect attribution by leaving behind the "fingerprints" of the groups that the attack techniques were stolen from. UMBRAGE components cover keyloggers, password collection, webcam capture, data destruction, persistence, privilege escalation, stealth, anti-virus (PSP) avoidance and survey techniques."

As Kim Dotcom summarizes this finding, "CIA uses techniques to make cyber attacks look like they originated from enemy state. It turns DNC/Russia hack allegation by CIA into a JOKE"

CIA uses techniques to make cyber attacks look like they originated from enemy state. It turns DNC/Russia hack allegation by CIA into a JOKE

— Kim Dotcom (@KimDotcom) [March 7, 2017](#)

But perhaps what is most notable is the purported emergence of another Snowden-type whistleblower: the source of the information told WikiLeaks in a statement that they wish to initiate a public debate about the “security, creation, use, proliferation and democratic control of cyberweapons.” Policy questions that should be debated in public include “whether the CIA's hacking capabilities exceed its mandated powers and the problem of public oversight of the agency,” WikiLeaks claims the source said.

The FAQ section of the release, shown below, provides further details on the extent of the leak, which was “obtained recently and covers through 2016”. The time period covered in the latest leak is between the years 2013 and 2016, according to the CIA timestamps on the documents themselves. Secondly,

WikiLeaks has asserted that it has not mined the entire leak and has only verified it, asking that journalists and activists do the leg work.

Among the various techniques profiled by WikiLeaks is “Weeping Angel”, developed by the CIA's Embedded Devices Branch (EDB), which infests smart TVs, transforming them into covert microphones. After infestation, Weeping Angel places the target TV in a 'Fake-Off' mode, so that the owner falsely believes the TV is off when it is on. In 'Fake-Off' mode the TV operates as a bug, recording conversations in the room and sending them over the Internet to a covert CIA server.

As Kim Dotcom chimed in on Twitter, "CIA turns Smart TVs, iPhones, gaming consoles and many other consumer gadgets into open microphones" and added " CIA turned every Microsoft Windows PC in the world into spyware. Can activate backdoors on demand, including via Windows update"

BREAKING: CIA turns Smart TVs, iPhones, gaming consoles and many other consumer gadgets into open microphones. [#Vault7](#)

— Kim Dotcom (@KimDotcom) [March 7, 2017](#)

Dotcom also added that "Obama accused Russia of cyberattacks while his CIA turned all internet enabled consumer electronics in Russia into listening devices. Wow!"

Obama accused Russia of cyberattacks while his CIA turned all internet enabled consumer electronics in Russia into listening devices. Wow!

— Kim Dotcom (@KimDotcom) [March 7, 2017](#)

Julian Assange, WikiLeaks editor stated that "There is an extreme proliferation risk in the development of cyber 'weapons'. Comparisons can be drawn between the uncontrolled proliferation of such 'weapons', which results from the inability to contain them combined with their high market value, and the global arms trade. But the significance of "Year Zero" goes well beyond the choice between cyberwar and cyberpeace. The disclosure is also exceptional from a political, legal and forensic perspective."

Key Highlights from the Vault 7 release so far:

"Year Zero" introduces the scope and direction of the CIA's global covert hacking program, its malware arsenal and dozens of "zero day" weaponized exploits against a wide range of U.S. and European company products, include Apple's iPhone, Google's Android and Microsoft's Windows and even Samsung TVs, which are turned into covert microphones.

Wikileaks claims that the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized "zero day" exploits, malware remote control systems and associated documentation. This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA. The archive appears to have been circulated among former U.S.

government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive.

By the end of 2016, the CIA's hacking division, which formally falls under the agency's Center for Cyber Intelligence (CCI), had over 5000 registered users and had produced more than a thousand hacking systems, trojans, viruses, and other "weaponized" malware. Such is the scale of the CIA's undertaking that by 2016, its hackers had utilized more code than that used to run Facebook.

The CIA had created, in effect, its "own NSA" with even less accountability and without publicly answering the question as to whether such a massive budgetary spend on duplicating the capacities of a rival agency could be justified.

Once a single cyber 'weapon' is 'loose' it can spread around the world in seconds, to be used by rival states, cyber mafia and teenage hackers alike.

Snowden 2.0?

- In a statement to WikiLeaks the source details policy questions that they say urgently need to be debated in public, including whether the CIA's hacking capabilities exceed its mandated powers and the problem of public oversight of the agency. The source wishes to initiate a public debate about the security, creation, use, proliferation and democratic control of cyberweapons.

CIA targets iPhones, Androids, smart TVs:

CIA malware and hacking tools are built by EDG (Engineering Development Group), a software development group within CCI (Center for Cyber Intelligence), a department belonging to the CIA's DDI (Directorate for Digital Innovation). The DDI is one of the five major directorates of the CIA (see this organizational chart of the CIA for more details).

The increasing sophistication of surveillance techniques has drawn comparisons with George Orwell's 1984, but "Weeping Angel", developed by the CIA's Embedded Devices Branch (EDB), which infests smart TVs, transforming them into covert microphones, is surely its most emblematic realization.

Also cars, suggesting that the CIA may have a role in the death of Michael Hastings:

- As of October 2014 the CIA was also looking at infecting the vehicle control systems used by modern cars and trucks.
- The purpose of such control is not specified, but it would permit the CIA to engage in nearly undetectable assassinations.

And computers:

- **The CIA also runs a very substantial effort to infect and control Microsoft Windows users with its malware. This includes multiple local and remote weaponized "zero days", air gap jumping viruses such as "Hammer Drill" which infects software distributed on CD/DVDs, infectors for removable media such as USBs, systems to hide data in images or in covert disk areas ("Brutal Kangaroo") and to keep its malware infestations going.**

Hoarding of Zero Day exploits:

- **In the wake of Edward Snowden's leaks about the NSA, the U.S. technology industry secured a commitment from the Obama administration that the executive would disclose on an ongoing basis — rather than hoard — serious vulnerabilities, exploits, bugs or "zero days" to Apple, Google, Microsoft, and other US-based manufacturers.**
- **Serious vulnerabilities not disclosed to the manufacturers places huge swathes of the population and critical infrastructure at risk to foreign intelligence or cyber criminals who independently discover or hear rumors of the vulnerability. If the CIA can discover such vulnerabilities so can others.**

Proliferation of leaked/hacked Cyberwar programs:

- **While nuclear proliferation has been restrained by the enormous costs and visible infrastructure involved in assembling enough fissile material to produce a critical nuclear mass, cyber 'weapons', once developed, are very hard to retain. Cyber 'weapons' are in fact just computer programs which can be pirated like any other. Since they are entirely comprised of information they can be copied quickly with no marginal cost.**
- **Over the last three years the United States intelligence sector, which consists of government agencies such as the CIA and NSA and their contractors, such as Booz Allen Hamilton, has been subject to unprecedented series of data exfiltrations by its own workers.**
- **Once a single cyber 'weapon' is 'loose' it can spread around the world in seconds, to be used by peer states, cyber mafia and teenage hackers alike.**

The U.S. Consulate in Frankfurt is a covert CIA hacker base

- **In addition to its operations in Langley, Virginia the CIA also uses the U.S. consulate in Frankfurt as a covert base for its hackers covering Europe, the Middle East and Africa. CIA hackers operating out of the Frankfurt consulate ("Center for Cyber Intelligence Europe" or CCIE) are given diplomatic ("black") passports and State Department cover.**
- **The instructions for incoming CIA hackers make Germany's counter-intelligence efforts appear inconsequential: "Breeze through German Customs because you have your cover-for-action story down pat, and all they did was stamp your passport"**

Examples of CIA projects

- **The CIA's Engineering Development Group (EDG) management system contains around 500 different projects (only some of which are documented by "Year Zero") each with their own sub-projects, malware and hacker tools. The majority of these projects relate to tools that are used for penetration, infestation ("implanting"), control, and exfiltration.**
- **Umbrage: The CIA's Remote Devices Branch's UMBRAGE group collects and maintains a substantial library of attack techniques 'stolen' from malware produced in other states including the Russian Federation. With UMBRAGE and related projects the CIA cannot only increase its total number of attack types but also misdirect attribution by leaving behind the "fingerprints" of the groups that the attack techniques were stolen from.**
- **Fine Dining: Fine Dining comes with a standardized questionnaire i.e menu that CIA case officers fill out. The questionnaire is used by the agency's OSB (Operational Support Branch) to transform the requests of case officers into technical requirements for hacking attacks (typically "exfiltrating" information from computer systems) for specific operations. Among the list of possible targets of the collection are 'Asset', 'Liason Asset', 'System Administrator', 'Foreign Information Operations', 'Foreign Intelligence Agencies' and 'Foreign Government Entities'. Notably absent is any reference to extremists or transnational criminals.**
- **'Improvise'; a toolset for configuration, post-processing, payload setup and execution vector selection for survey/exfiltration tools supporting all major operating systems like Windows (Bartender), MacOS (JukeBox) and Linux (DanceFloor).**
- **HIVE: HIVE is a multi-platform CIA malware suite and its associated control software. The project provides customizable implants for Windows, Solaris, MikroTik (used in internet routers) and Linux platforms and a Listening Post (LP)/Command and Control (C2) infrastructure to communicate with these implants. The implants are configured to communicate via HTTPS with the webserver of a cover domain; each operation utilizing these implants has a separate cover domain and the infrastructure can handle any number of cover domains.**

And some key sections from the FAQ:

- **What time period is covered? The years 2013 to 2016. The sort order of the pages within each level is determined by date (oldest first). WikiLeaks has obtained the CIA's creation/last modification date for each page but these do not yet appear for technical reasons. Usually the date can be discerned or approximated from the content and the page order. If it is critical to know the exact time/date contact WikiLeaks.**

- **What is "Vault 7" "Vault 7" is a substantial collection of material about CIA activities obtained by WikiLeaks.**
- **What is the total size of "Vault 7"? The series is the largest intelligence publication in history.**
- **When was each part of "Vault 7" obtained?: Part one was obtained recently and covers through 2016. Details on the other parts will be available at the time of publication.**
- **Is each part of "Vault 7" from a different source? Details on the other parts will be available at the time of publication.**
- **How did WikiLeaks obtain each part of "Vault 7"? Sources trust WikiLeaks to not reveal information that might help identify them.**
- **Isn't WikiLeaks worried that the CIA will act against its staff to stop the series? No. That would be certainly counter-productive.**

On Tuesday 7 March 2017, WikiLeaks began its new series of leaks on the U.S. Central Intelligence Agency. Code-named "Vault 7" by WikiLeaks, it is the largest ever publication of confidential documents on the agency.

The first full part of the series, "Year Zero", comprises 8,761 documents and files from an isolated, high-security network situated inside the CIA's [Center for Cyber Intelligence](#) in Langley, Virginia. It follows an introductory disclosure last month of [CIA targeting French political parties and candidates in the lead up to the 2012 presidential election](#).

Recently, the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized "zero day" exploits, malware remote control systems and associated documentation. This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA. The archive appears to have been circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive.

"Year Zero" introduces the scope and direction of the CIA's global covert hacking program, its malware arsenal and dozens of "zero day" weaponized exploits against a wide range of U.S. and European company products, include Apple's iPhone, Google's Android and Microsoft's Windows and even Samsung TVs, which are turned into covert microphones.

Since 2001 the CIA has gained political and budgetary preeminence over the U.S. National Security Agency (NSA). The CIA found itself building not just its now infamous drone fleet, but a very different type of covert, globe-spanning force — its own substantial fleet of hackers. The agency's hacking division freed it from having to disclose its often controversial operations to the NSA (its primary bureaucratic rival) in order to draw on the NSA's hacking capacities.

By the end of 2016, the CIA's hacking division, which formally falls under the agency's [Center for Cyber Intelligence](#) (CCI), had over 5000 registered users and had produced more than a thousand hacking systems, trojans, viruses, and other "weaponized" malware. Such is the scale of the CIA's undertaking that by 2016, its hackers had utilized more code than that used to run Facebook. The CIA had created, in effect, its "own NSA" with even less accountability and without publicly answering the question as to whether such a massive budgetary spend on duplicating the capacities of a rival agency could be justified.

In a statement to WikiLeaks the source details policy questions that they say urgently need to be debated in public, including whether the CIA's hacking capabilities exceed its mandated powers and the problem of public oversight of the agency. The source wishes to initiate a public debate about the security, creation, use, proliferation and democratic control of cyberweapons.

Once a single cyber 'weapon' is 'loose' it can spread around the world in seconds, to be used by rival states, cyber mafia and teenage hackers alike.

Julian Assange, WikiLeaks editor stated that "There is an extreme proliferation risk in the development of cyber 'weapons'. Comparisons can be drawn between the uncontrolled proliferation of such 'weapons', which results from the inability to contain them combined with their high market value, and the global arms trade. But the significance of "Year Zero" goes well beyond the choice between cyberwar and cyberpeace. The disclosure is also exceptional from a political, legal and forensic perspective."

Wikileaks has carefully reviewed the "Year Zero" disclosure and published substantive CIA documentation while avoiding the distribution of 'armed' cyberweapons until a consensus emerges on the technical and political nature of the CIA's program and how such 'weapons' should analyzed, disarmed and published.

Wikileaks has also decided to [redact](#) and anonymise some identifying information in "Year Zero" for in depth analysis. These redactions include ten of thousands of CIA targets and attack machines throughout Latin America, Europe and the United States. While we are aware of the imperfect results of any approach chosen, we remain committed to our publishing model and note that the quantity of published pages in "Vault 7" part one ("Year Zero") already eclipses the total number of pages published over the first three years of the Edward Snowden NSA leaks.

* * *

Analysis

CIA malware targets iPhone, Android, smart TVs

CIA malware and hacking tools are built by EDG (Engineering Development Group), a software development group within CCI (Center for Cyber Intelligence), a department belonging to the

CIA's DDI (Directorate for Digital Innovation). The DDI is one of the five major directorates of the CIA (see this [organizational chart](#) of the CIA for more details).

The EDG is responsible for the development, testing and operational support of all backdoors, exploits, malicious payloads, trojans, viruses and any other kind of malware used by the CIA in its covert operations world-wide.

The increasing sophistication of surveillance techniques has drawn comparisons with George Orwell's 1984, but "Weeping Angel", developed by the CIA's [Embedded Devices Branch \(EDB\)](#), which infests smart TVs, transforming them into covert microphones, is surely its most emblematic realization.

The attack against [Samsung smart TVs](#) was developed in cooperation with the United Kingdom's MI5/BTSS. After infestation, Weeping Angel places the target TV in a 'Fake-Off' mode, so that the owner falsely believes the TV is off when it is on. In 'Fake-Off' mode the TV operates as a bug, recording conversations in the room and sending them over the Internet to a covert CIA server.

As of October 2014 the CIA was also looking at [infecting the vehicle control systems used by modern cars and trucks](#). The purpose of such control is not specified, but it would permit the CIA to engage in nearly undetectable assassinations.

The CIA's Mobile Devices Branch (MDB) developed [numerous attacks to remotely hack and control popular smart phones](#). Infected phones can be instructed to send the CIA the user's geolocation, audio and text communications as well as covertly activate the phone's camera and microphone.

Despite iPhone's minority share (14.5%) of the global smart phone market in 2016, a specialized unit in the CIA's Mobile Development Branch produces malware to infest, control and exfiltrate data from [iPhones and other Apple products running iOS, such as iPads](#). CIA's arsenal includes [numerous local and remote "zero days"](#) developed by CIA or obtained from GCHQ, NSA, FBI or purchased from cyber arms contractors such as Baitshop. The disproportionate focus on iOS may be explained by the popularity of the iPhone among social, political, diplomatic and business elites.

A [similar unit targets Google's Android which is used to run the majority of the world's smart phones \(~85%\) including Samsung, HTC and Sony](#). 1.15 billion Android powered phones were sold last year. "Year Zero" shows that as of 2016 [the CIA had 24 "weaponized" Android "zero days"](#) which it has developed itself and obtained from GCHQ, NSA and cyber arms contractors.

These techniques permit the CIA to bypass the encryption of WhatsApp, Signal, Telegram, Weibo, Confide and Cloackman by hacking the "smart" phones that they run on and collecting audio and message traffic before encryption is applied.

CIA malware targets Windows, OSx, Linux, routers

The CIA also runs a very substantial effort to infect and control [Microsoft Windows users](#) with its malware. This includes multiple local and remote weaponized "zero days", air gap jumping viruses such as ["Hammer Drill"](#) which infects software distributed on CD/DVDs, [infectors for removable media such as USBs](#), systems to [hide data in images](#) or in covert disk areas (["Brutal Kangaroo"](#)) and to [keep its malware infestations going](#).

Many of these infection efforts are pulled together by the CIA's [Automated Implant Branch \(AIB\)](#), which has developed several attack systems for automated infestation and control of CIA malware, such as "Assassin" and "Medusa".

Attacks against Internet infrastructure and webservers are developed by the CIA's [Network Devices Branch \(NDB\)](#).

The CIA has developed automated multi-platform malware attack and control systems covering Windows, Mac OS X, Solaris, Linux and more, such as EDB's "HIVE" and the related "Cutthroat" and "Swindle" tools, which are [described in the examples section below](#).

CIA 'hoarded' vulnerabilities ("zero days")

In the wake of Edward Snowden's leaks about the NSA, the U.S. technology industry secured a commitment from the Obama administration that the executive would disclose on an ongoing basis — rather than hoard — serious vulnerabilities, exploits, bugs or "zero days" to Apple, Google, Microsoft, and other US-based manufacturers.

Serious vulnerabilities not disclosed to the manufacturers places huge swathes of the population and critical infrastructure at risk to foreign intelligence or cyber criminals who independently discover or hear rumors of the vulnerability. If the CIA can discover such vulnerabilities so can others.

The U.S. government's commitment to the [Vulnerabilities Equities Process](#) came after significant lobbying by US technology companies, who risk losing their share of the global market over real and perceived hidden vulnerabilities. The government stated that it would disclose all pervasive vulnerabilities discovered after 2010 on an ongoing basis.

"Year Zero" documents show that the CIA breached the Obama administration's commitments. Many of the vulnerabilities used in the CIA's cyber arsenal are pervasive and some may already have been found by rival intelligence agencies or cyber criminals.

As an example, specific CIA malware revealed in "Year Zero" is able to penetrate, infest and control both the Android phone and iPhone software that runs or has run presidential Twitter

accounts. The CIA attacks this software by using undisclosed security vulnerabilities ("zero days") possessed by the CIA but if the CIA can hack these phones then so can everyone else who has obtained or discovered the vulnerability. As long as the CIA keeps these vulnerabilities concealed from Apple and Google (who make the phones) they will not be fixed, and the phones will remain hackable.

The same vulnerabilities exist for the population at large, including the U.S. Cabinet, Congress, top CEOs, system administrators, security officers and engineers. By hiding these security flaws from manufacturers like Apple and Google the CIA ensures that it can hack everyone; at the expense of leaving everyone hackable.

'Cyberwar' programs are a serious proliferation risk

Cyber 'weapons' are not possible to keep under effective control.

While nuclear proliferation has been restrained by the enormous costs and visible infrastructure involved in assembling enough fissile material to produce a critical nuclear mass, cyber 'weapons', once developed, are very hard to retain.

Cyber 'weapons' are in fact just computer programs which can be pirated like any other. Since they are entirely comprised of information they can be copied quickly with no marginal cost.

Securing such 'weapons' is particularly difficult since the same people who develop and use them have the skills to exfiltrate copies without leaving traces — sometimes by using the very same 'weapons' against the organizations that contain them. There are substantial price incentives for government hackers and consultants to obtain copies since there is a global "vulnerability market" that will pay hundreds of thousands to millions of dollars for copies of such 'weapons'. Similarly, contractors and companies who obtain such 'weapons' sometimes use them for their own purposes, obtaining advantage over their competitors in selling 'hacking' services.

Over the last three years the United States intelligence sector, which consists of government agencies such as the CIA and NSA and their contractors, such as Booz Allen Hamilton, has been subject to unprecedented series of data exfiltrations by its own workers.

A number of intelligence community members not yet publicly named have been arrested or subject to federal criminal investigations in separate incidents.

Most visibly, on February 8, 2017 a U.S. federal grand jury indicted Harold T. Martin III with 20 counts of mishandling classified information. The Department of Justice alleged that it seized some 50,000 gigabytes of information from Harold T. Martin III that he had obtained from classified programs at NSA and CIA, including the source code for numerous hacking tools.

Once a single cyber 'weapon' is 'loose' it can spread around the world in seconds, to be used by peer states, cyber mafia and teenage hackers alike.

U.S. Consulate in Frankfurt is a covert CIA hacker base

In addition to its operations in Langley, Virginia the CIA also uses the U.S. consulate in Frankfurt as a covert base for its hackers covering Europe, the Middle East and Africa.

CIA hackers operating out of the Frankfurt consulate (["Center for Cyber Intelligence Europe"](#) or CCIE) are given diplomatic ("black") passports and State Department cover. [The instructions for incoming CIA hackers](#) make Germany's counter-intelligence efforts appear inconsequential: "Breeze through German Customs because you have your cover-for-action story down pat, and all they did was stamp your passport"

Your Cover Story (for this trip)

Q: Why are you here?

A: Supporting technical consultations at the Consulate.

Two earlier WikiLeaks publications give further detail on CIA approaches to [customs](#) and [secondary screening procedures](#).

Once in Frankfurt CIA hackers can travel without further border checks to the 25 European countries that are part of the Shengen open border area — including France, Italy and Switzerland.

A number of the CIA's electronic attack methods are designed for physical proximity. These attack methods are able to penetrate high security networks that are disconnected from the internet, such as police record database. In these cases, a CIA officer, agent or allied intelligence officer acting under instructions, physically infiltrates the targeted workplace. The attacker is provided with a USB containing malware developed for the CIA for this purpose, which is inserted into the targeted computer. The attacker then infects and exfiltrates data to removable media. For example, the CIA attack system [Fine Dining](#), provides 24 decoy applications for CIA spies to use. To witnesses, the spy appears to be running a program showing videos (e.g VLC), presenting slides (Prezi), playing a computer game (Breakout2, 2048) or even running a fake virus scanner (Kaspersky, McAfee, Sophos). But while the decoy application is on the screen, the underlying system is automatically infected and ransacked.

How the CIA dramatically increased proliferation risks

In what is surely one of the most astounding intelligence own goals in living memory, the CIA structured its classification regime such that for the most market valuable part of "Vault 7" — the CIA's weaponized malware (implants + zero days), Listening Posts (LP), and Command and Control (C2) systems — the agency has little legal recourse.

The CIA made these systems unclassified.

Why the CIA chose to make its cyberarsenal unclassified reveals how concepts developed for military use do not easily crossover to the 'battlefield' of cyber 'war'.

To attack its targets, the CIA usually requires that its implants communicate with their control programs over the internet. If CIA implants, Command & Control and Listening Post software were classified, then CIA officers could be prosecuted or dismissed for violating rules that prohibit placing classified information onto the Internet. Consequently the CIA has secretly made most of its cyber spying/war code unclassified. The U.S. government is not able to assert copyright either, due to restrictions in the U.S. Constitution. This means that cyber 'arms' manufactures and computer hackers can freely "pirate" these 'weapons' if they are obtained. The CIA has primarily had to rely on obfuscation to protect its malware secrets.

Conventional weapons such as missiles may be fired at the enemy (i.e into an unsecured area). Proximity to or impact with the target detonates the ordnance including its classified parts. Hence military personnel do not violate classification rules by firing ordnance with classified parts. Ordnance will likely explode. If it does not, that is not the operator's intent.

Over the last decade U.S. hacking operations have been increasingly dressed up in military jargon to tap into Department of Defense funding streams. For instance, attempted "malware injections" (commercial jargon) or "implant drops" (NSA jargon) are being called "fires" as if a weapon was being fired. However the analogy is questionable.

Unlike bullets, bombs or missiles, most CIA malware is designed to live for days or even years after it has reached its 'target'. CIA malware does not "explode on impact" but rather permanently infests its target. In order to infect target's device, copies of the malware must be placed on the target's devices, giving physical possession of the malware to the target. To exfiltrate data back to the CIA or to await further instructions the malware must communicate with CIA Command & Control (C2) systems placed on internet connected servers. But such servers are typically not approved to hold classified information, so CIA command and control systems are also made unclassified.

A successful 'attack' on a target's computer system is more like a series of complex stock maneuvers in a hostile take-over bid or the careful planting of rumors in order to gain control over an organization's leadership rather than the firing of a weapons system. If there is a military analogy to be made, the infestation of a target is perhaps akin to the execution of a whole series of

military maneuvers against the target's territory including observation, infiltration, occupation and exploitation.

Evading forensics and anti-virus

A series of standards lay out CIA malware infestation patterns which are likely to assist forensic crime scene investigators as well as Apple, Microsoft, Google, Samsung, Nokia, Blackberry, Siemens and anti-virus companies attribute and defend against attacks.

"Tradecraft DO's and DON'Ts" contains CIA rules on how its malware should be written to avoid fingerprints implicating the "CIA, US government, or its witting partner companies" in "forensic review". Similar secret standards cover the use of encryption to hide CIA hacker and malware communication (pdf), describing targets & exfiltrated data (pdf) as well as executing payloads (pdf) and persisting (pdf) in the target's machines over time.

CIA hackers developed successful attacks against most well known anti-virus programs. These are documented in AV defeats, Personal Security Products, Detecting and defeating PSPs and PSP/Debugger/RE Avoidance. For example, Comodo was defeated by CIA malware placing itself in the Window's "Recycle Bin". While Comodo 6.x has a "Gaping Hole of DOOM".

CIA hackers discussed what the NSA's "Equation Group" hackers did wrong and how the CIA's malware makers could avoid similar exposure.

Examples

The CIA's Engineering Development Group (EDG) management system contains around 500 different projects (only some of which are documented by "Year Zero") each with their own sub-projects, malware and hacker tools.

The majority of these projects relate to tools that are used for penetration, infestation ("implanting"), control, and exfiltration.

Another branch of development focuses on the development and operation of Listening Posts (LP) and Command and Control (C2) systems used to communicate with and control CIA implants; special projects are used to target specific hardware from routers to smart TVs.

Some example projects are described below, but see the table of contents for the full list of projects described by WikiLeaks' "Year Zero".

UMBORAGE

The CIA's hand crafted hacking techniques pose a problem for the agency. Each technique it has created forms a "fingerprint" that can be used by forensic investigators to attribute multiple different attacks to the same entity.

This is analogous to finding the same distinctive knife wound on multiple separate murder victims. The unique wounding style creates suspicion that a single murderer is responsible. As soon one murder in the set is solved then the other murders also find likely attribution.

The CIA's [Remote Devices Branch's UMBORAGE group](#) collects and maintains [a substantial library](#) of attack techniques 'stolen' from malware produced in other states including the Russian Federation.

With UMBORAGE and related projects the CIA cannot only increase its total number of attack types but also misdirect attribution by leaving behind the "fingerprints" of the groups that the attack techniques were stolen from.

UMBORAGE components cover keyloggers, password collection, webcam capture, data destruction, persistence, privilege escalation, stealth, anti-virus (PSP) avoidance and survey techniques.

Fine Dining

Fine Dining comes with a standardized questionnaire i.e menu that CIA case officers fill out. The questionnaire is used by the agency's OSB ([Operational Support Branch](#)) to transform the requests of case officers into technical requirements for hacking attacks (typically "exfiltrating" information from computer systems) for specific operations. The questionnaire allows the OSB to identify how to adapt existing tools for the operation, and communicate this to CIA malware configuration staff. The OSB functions as the interface between CIA operational staff and the relevant technical support staff.

Among the list of possible targets of the collection are 'Asset', 'Liason Asset', 'System Administrator', 'Foreign Information Operations', 'Foreign Intelligence Agencies' and 'Foreign Government Entities'. Notably absent is any reference to extremists or transnational criminals. The 'Case Officer' is also asked to specify the environment of the target like the type of computer, operating system used, Internet connectivity and installed anti-virus utilities (PSPs) as well as a list of file types to be exfiltrated like Office documents, audio, video, images or custom file types. The 'menu' also asks for information if recurring access to the target is possible and how long unobserved access to the computer can be maintained. This information is used by the CIA's 'JQJIMPROVISE' software (see below) to configure a set of CIA malware suited to the specific needs of an operation.

Improvise (JQJIMPROVISE)

'Improvise' is a toolset for configuration, post-processing, payload setup and execution vector selection for survey/exfiltration tools supporting all major operating systems like Windows (Bartender), MacOS (JukeBox) and Linux (DanceFloor). Its configuration utilities like Margarita allows the NOC (Network Operation Center) to customize tools based on requirements from 'Fine Dining' questionnaires.

HIVE

HIVE is a multi-platform CIA malware suite and its associated control software. The project provides customizable implants for Windows, Solaris, MikroTik (used in internet routers) and Linux platforms and a Listening Post (LP)/Command and Control (C2) infrastructure to communicate with these implants.

The implants are configured to communicate via HTTPS with the webserver of a cover domain; each operation utilizing these implants has a separate cover domain and the infrastructure can handle any number of cover domains.

Each cover domain resolves to an IP address that is located at a commercial VPS (Virtual Private Server) provider. The public-facing server forwards all incoming traffic via a VPN to a 'Blot' server that handles actual connection requests from clients. It is setup for optional SSL client authentication: if a client sends a valid client certificate (only implants can do that), the connection is forwarded to the 'Honeycomb' toolserver that communicates with the implant; if a valid certificate is missing (which is the case if someone tries to open the cover domain website by accident), the traffic is forwarded to a cover server that delivers an unsuspecting looking website.

The Honeycomb toolserver receives exfiltrated information from the implant; an operator can also task the implant to execute jobs on the target computer, so the toolserver acts as a C2 (command and control) server for the implant.

Similar functionality (though limited to Windows) is provided by the RickBobby project.

See the classified [user](#) and [developer](#) guides for HIVE.

* * *

FREQUENTLY ASKED QUESTIONS

Why now?

WikiLeaks published as soon as its verification and analysis were ready.

In February the Trump administration has issued an Executive Order calling for a "Cyberwar" review to be prepared within 30 days.

While the review increases the timeliness and relevance of the publication it did not play a role in setting the publication date.

Redactions

Names, email addresses and external IP addresses have been redacted in the released pages (70,875 redactions in total) until further analysis is complete.

1. Over-redaction: Some items may have been redacted that are not employees, contractors, targets or otherwise related to the agency, but are, for example, authors of documentation for otherwise public projects that are used by the agency.
2. Identity vs. person: the redacted names are replaced by user IDs (numbers) to allow readers to assign multiple pages to a single author. Given the redaction process used a single person may be represented by more than one assigned identifier but no identifier refers to more than one real person.
3. Archive attachments (zip, tar.gz, ...) are replaced with a PDF listing all the file names in the archive. As the archive content is assessed it may be made available; until then the archive is redacted.
4. Attachments with other binary content are replaced by a hex dump of the content to prevent accidental invocation of binaries that may have been infected with weaponized CIA malware. As the content is assessed it may be made available; until then the content is redacted.
5. The tens of thousands of routable IP addresses references (including more than 22 thousand within the United States) that correspond to possible targets, CIA covert listening post servers, intermediary and test systems, are redacted for further exclusive investigation.
6. Binary files of non-public origin are only available as dumps to prevent accidental invocation of CIA malware infected binaries.

Organizational Chart

The [organizational chart](#) corresponds to the material published by WikiLeaks so far.

Since the organizational structure of the CIA below the level of Directorates is not public, the placement of the EDG and its branches within the org chart of the agency is reconstructed from information contained in the documents released so far. It is intended to be used as a rough outline of the internal organization; please be aware that the reconstructed org chart is incomplete and that internal reorganizations occur frequently.

And that is only a tiny part of the arsenal that is now being used against reporters who write articles critical of Elon Musk, John Podesta, Google or their political candidates. These tools and tactics are used against business competitors and ordinary citizens who speak out about crimes that Silicon Valley politicians engage in.

Everything you just read in the previous lists is now being aimed at you to seek out your weaknesses for your competitors and ideological opposition to use to try to destroy you.

The Cleantech Crash Insider Attack Tools

IN THE MID 2000'S, TRILLIONS OF DOLLARS OF FOREIGN MINING SCHEMES FOR LITHIUM, INDIUM, COBALT, URANIUM, COPPER, ETC. WERE BEING TRADED FOR POLITICAL CAMPAIGN FINANCING AND SILICON VALLEY INTERNET "SOCIAL MEDIA ENGINEERING" WHICH WAS USED TO RIG PRESIDENTIAL ELECTIONS.

DOE, CIA, USAID, DOT, EPA AND OTHER AGENCIES WERE INFECTED WITH CORRUPTION TO ATTEMPT THIS SCHEME. THE SCHEME WAS BACKED BY SILICON VALLEY "CLEANTECH" BILLIONAIRES IN EXCHANGE FOR MONOPOLIES AND PROFITS. THOSE WHO REPORTED THE SCHEME WERE ATTACKED AND ALSO DEFAMED WITH MEDIA HIT-JOBS. THESE ARE REPORTS FROM INVESTIGATORS, CONGRESS AND LAW ENFORCEMENT ON THOSE USES OF ELECTRONIC AUTOMATED ELECTION MANIPULATION TRADED FOR CRONY GOVERNMENT PAYOLA DEALS:

WHO PAYS FOR AND COORDINATES THE SILICON ELECTION RIGGING?:

Eric Schmidt

Jared Cohen

Larry Page

Mark Zuckerberg

John Doerr

Ray Lane

Tom Perkins (dead)

Elon Musk

John Podesta

Vinod Khosla

Steve Spinner

Steve Westly

Sid Blumenthal

George Soros

Cheryl Sandberg

David Plouffe

and their associates

WHAT ARE THE TACTICS AND TECHNOLOGIES THAT GOOGLE, FACEBOOK, TWITTER AND THEIR LOBBYISTS USE TO RIG ELECTIONS?:

- Hired Troll bloggers, in many countries, with huge clone farms of tablets they use to pretend to be different users online.
 - Use of your SS# to contain a single massive psychological data file and psych analysis of you based on anything you touch online, in order to calculate the best way to manipulate you for votes.
 - Automated Troll server farms that generate human-narrative texts based on programmed hate for Alt-Right phrases. Many of these server farms are in Palo Alto, Denver, Seattle, Dallas, New Jersey, The Ukraine, Cayman Islands and Singapore.
 - Chinese High Volume Fake Account suppliers who push millions of fake users to Twitter, Facebook, etc. to create false impressions of political trends and ad views that reflect nothing accurate.
 - Synchronized Character Assassinations in Gizmodo, TechDirt, etc, tabloids
 - Massive Fake User replication servers used to trick advertisers and pollsters.
 - Bot Farms of Hundreds of Thousands of Servers
 - Gawker Media Fake News organizations using covert Google docs folders to synchronize media attacks.
 - Hired Fake Comment Producers
 - Automated Fake Comment Producers
 - DNS Faker Routers
 - IMEI Re-Write High Density Chip Boards
 - Sting-Ray Interception and Analysis
 - Google's Control of Most Web Data for Covert "Mood Manipulation"
- While Google and Facebook rig their algorithms and search filters to manipulate results and censor news, they have also purchased, or contracted, the following products which they use for political manipulation:
- *Dataminr* directly licenses a stream of data from Twitter to spot trends and detect emerging threats to a Candidate who has promised payola to the Silicon Valley billionaires
 - *Geofeedia* collects geotagged social media messages to monitor activists locations in real time.
 - *PATHAR* mines social media to determine networks of association and track Alt-Right people to their friends
 - *TransVoyant* analyzes data points to deliver insights and predictions about global events and apply them to your political intentions.
 - *Aquifi*, 3D vision software solutions makes a real-time graph of how the public's mood is
 - *Beartooth*, Decentralized mobile network allows activists to be spied on
 - *Palantir*, Predicts how to manipulate the mood of the public for campaign speeches

- ***CliQr***, Hybrid cloud management platform. Big data exploration, visualization, and analytics platform for public political analysis and social media manipulation.
- ***CloudPassage***, On-demand, automated infrastructure Big data exploration, visualization, and analytics platform for public political analysis and social media manipulation.
- ***Databricks***, Cloud-hosted big data analytics and processing platform. Big data exploration, visualization, and analytics platform for public political analysis and social media manipulation.
- ***Docker***, Open platform to build, ship, and run distributed applications for big data exploration, visualization, and analytics platform for public political analysis and social media manipulation.
- ***Echodyne***, Next-generation electronically scanning your mobile devices for political comments.
- ***Epiq Solutions***, Software-defined radio platforms and applications for tracking public mobile devices.
- ***goTenna***, alternate network for off-grid smartphone communications to put back-doors in
- ***Headspin***, Network-focused approach to improving mobile application performance for big data exploration, visualization, and analytics platform for public political analysis and social media manipulation.
- ***Interset***, Inside political detection using analytics, machine learning, for big data exploration, visualization, and analytics platform for public political analysis and social media manipulation.
- ***Keyssa***, Fast, simple, and secure contactless data transfer for big data exploration of your credit cards, visualization, and analytics platform for public political analysis and social media manipulation.
- ***Kymeta***, Antenna technology for broadband satellite communications for for big data exploration, visualization, and analytics platform for public political analysis and social media manipulation.
- ***Lookout***, Cloud-based mobile cybersecurity for big data exploration, visualization, and analytics platform for public political analysis and social media manipulation.
- ***Mapbox***, Design and publish visual, data-rich maps for big data exploration, visualization, and analytics platform for public political analysis and social media manipulation.
- ***Mesosphere***, Next-generation scale, efficiency, and automation in a physical or cloud-based data center for big data exploration, visualization, and analytics platform for public political analysis and social media manipulation.
- ***Nervana***, Next-generation machine learning platform to create automated Trolls
- ***Orbital Insight***, Satellite imagery processing and data science at scale for Elon Musk's spy satellites.
- ***Orion Labs***, Wearable device and real-time voice communications platform to help consumers spy on themselves.
- ***Parallel Wireless***, LTE radio access nodes and software stack for small cell deployment to hack voters mobile phone locations.
- ***Pneubotics***, Mobile material handling solutions to automate tasks of robot Trolls tapping on vast numbers of tablets.

- ***PsiKick*, Redefined ultra-low power wireless sensor solutions to spy on your devices.**
- ***PubNub*, Build and scale real-time apps for big data exploration, visualization, and analytics platform for public political analysis and social media manipulation.**
- ***Rocket Lab*, Launch provider for small spy satellites**
- ***Skincential Sciences*, Novel materials for biological sample collection of the smells and organics of crowds in order to sense their moods.**
- ***Soft Robotics*, Soft robotics actuators and systems mobile material handling solutions to automate tasks of robot Trolls tapping on vast numbers of keyboards.**
- ***Sonatype*, Software supply chain automation and security for big data exploration, visualization, and analytics platform for public political analysis and social media manipulation.**
- ***Spaceflight Industries*, Small spy satellite launch, network, and imagery provider**
- ***Threatstream*, Leading enterprise-class political intelligence platform for big data exploration, visualization, and analytics platform for public political analysis and social media manipulation.**
- ***Timbr.io*, Accessible code-driven analysis platform. Big data exploration, visualization, and analytics platform for public political analysis and social media manipulation.**
- ***Transient Electronics*, Dissolvable semiconductor technology so you can swallow a bugging device to get rid of it.**
- ***TransVoyant*, Live predictive intelligence platform. Big data exploration, visualization, and analytics platform for public political analysis and social media manipulation**
- ***TRX Systems*, 3D indoor location and mapping solutions. Big data exploration, visualization, and analytics platform for public political analysis and social media manipulation.**
- ***Zoomdata*, Big data exploration, visualization, and analytics platform for public political analysis and social media manipulation**
- **And much more...**

=====

Silicon Valley’s In-Q-Tel private services spy company has also developed a special technology laboratory in Silicon Valley, called Lab41, to provide tools for the intelligence community to connect the dots in large sets of data. In February, Lab41 published an article exploring the ways in which a Twitter user’s location could be predicted with a degree of certainty through the location of the user’s friends. On Github, an open source website for developers, Lab41 currently has a project to ascertain the “feasibility of using architectures such as Convolutional and Recurrent Neural Networks to classify the positive, negative, or neutral sentiment of Twitter messages towards a specific topic.” Collecting intelligence on foreign adversaries has potential benefits for counterterrorism, but such CIA-supported surveillance technology is also used for domestic law enforcement and by the private sector to spy on activist groups. Palantir, one of In-Q-Tel’s earliest investments in the social media analytics realm, was exposed in 2011 by the hacker group LulzSec to be in negotiation for a proposal to track labor union activists and other critics of the U.S. Chamber of Commerce, the largest business lobbying group in Washington. The company, now celebrated as a “tech unicorn” — a term for start-ups that reach over

\$1 billion in valuation — distanced itself from the plan after it was exposed in a cache of leaked emails from the now-defunct firm HBGary Federal.

The Silicon hacks worked to rig Obama’s election into office and the following Mid-Terms, were overridden for the 2016 election and are being tripled down on for the Mid-Terms following Trump’s election and for 2020.

Yet other In-Q-Tel-backed companies are now openly embracing the practice. Geofeedia, for instance, promotes its research into Greenpeace activists, student demonstrations, minimum wage advocates, and other political movements. Police departments in Oakland, Chicago, Detroit, and other major municipalities have contracted with Geofeedia, as well as private firms such as the Mall of America and McDonald’s. Although these Silicon Valley “Big Data” systems have missed every major terror attack, Google’s investors keep selling their crap software and failed “Big Data” services to the U.S. Government.

Lee Guthman, an executive at Geofeedia, told reporter John Knefel that his company could predict the potential for violence at Black Lives Matter protests just by using the location and sentiment of tweets. Guthman said the technology could gauge sentiment by attaching “positive and negative points” to certain phrases, while measuring “proximity of words to certain words.” Privacy advocates, however, have expressed concern about these sorts of automated judgments. “When you have private companies deciding which algorithms get you a so-called threat score, or make you a person of interest, there’s obviously room for targeting people based on viewpoints or even unlawfully targeting people based on race or religion,” said Lee Rowland, a senior staff attorney with the American Civil Liberties Union.

Google Owns Over 100 Companies Designed To Operate Coups, Character Assassinations and Election Rigging.

Meet "CrowdStrike"

[Counterpunch](#) put out a very important article earlier today on the topic, adding several crucial nuggets of information. First there's this:

The investigation methods used to come to the conclusion that the Russian Government led the hacks of the [DNC](#), [Clinton Campaign Chair John Podesta](#), and the DCCC were further called into question by a recent BuzzFeed [report](#) by Jason Leopold, who has developed a notable reputation from leading several non-partisan Freedom of Information Act lawsuits for investigative journalism purposes. On March 15 that the Department of Homeland Security released just two heavily redacted pages of unclassified information in response to an FOIA request for definitive evidence of Russian election interference allegations. Leopold wrote, "what the agency turned over to us and Ryan Shapiro, a PhD candidate at MIT and a research affiliate at Harvard University, is truly bizarre: a two-page intelligence assessment of the incident, dated Aug. 22, 2016, that contains information DHS culled from the internet. It's all unclassified — yet DHS covered nearly everything in wide swaths of black ink. Why? Not because it would threaten national security, but because it would reveal the methods DHS uses to gather intelligence, methods that may amount to little more than using Google."

That's weird enough, but it gets far stranger. For example:

In lieu of substantive evidence provided to the public that the alleged hacks which led to Wikileaks releases of DNC and Clinton Campaign Manager John Podesta's emails were orchestrated by the Russian Government, CrowdStrike's bias has been [cited as undependable in its own assessment, in addition to its skeptical methods and conclusions](#). The firm's CTO and co-founder, Dmitri Alperovitch, is a [senior fellow](#) at the Atlantic Council, a think tank with openly anti-Russian sentiments that is funded by Ukrainian billionaire Victor Pinchuk, who also happened to donate at least \$10 million to the [Clinton Foundation](#).

In 2013, the Atlantic Council [awarded](#) Hillary [Clinton](#) its Distinguished International Leadership Award. In 2014, the Atlantic Council [hosted](#) one of several events with former Ukrainian Prime Minister [Arseniy Yatsenyuk](#), who took over after pro-Russian President Viktor Yanukovich was ousted in early 2014, who now lives in exile in Russia.

Recall that the FBI was denied access to the DNC servers by the DNC itself, and simply agreed to rely on the results provided by CrowdStrike, which as you can see has ties to all sorts of anti-

Russia organizations and individuals. I find it absolutely remarkable that James Comey head of the FBI outsourced his job to CrowdStrike.

There remains zero evidence that Russia hacked the DNC. I repeat, there remains zero evidence that Russia hacked the DNC.

As cybersecurity expert Jeffrey Carr noted:

Jeffrey Carr [called](#) the [FBI/Department of Homeland Security Report](#), the only alleged evidence released by intelligence officials, released in late December 2016 a “fatally flawed effort” that provided no evidence to substantiate the claims that the Russian government conducted the hacks, though that’s what it was purported to do.

Absolutely remarkable, but there’s more. As [TechCrunch](#) reported back in 2015:

If you need proof that security is a red hot market these days, how about this morning’s announcement that cybersecurity company [CrowdStrike](#) landed a \$100 million Series C investment round?

The round was led by Google Capital with Rackspace, which happens to be one of the company’s customers also investing. Existing investors Accel and Warburg Pincus also participated. Today’s investment brings the total to-date to \$156 million.

Why do I find it interesting that Google was a major investor in CrowdStrike? Well for one, we know that Chairman of Alphabet, Inc. (Google’s parent company), Eric Schmidt, was actively working to help the Hillary campaign. As I highlighted in the 2015 post, [Meet “Groundwork” – Google Chairman Eric Schmidt’s Stealth Startup Working to Make Hillary Clinton President](#):

An under-the-radar startup funded by billionaire Eric Schmidt has become a major technology vendor for Hillary Clinton’s presidential campaign, underscoring the bonds between Silicon Valley and Democratic politics.

The Groundwork, according to Democratic campaign operatives and technologists, is part of efforts by Schmidt—the executive chairman of Google parent-company Alphabet—to ensure that Clinton has the engineering talent needed to win the election. And it is one of a series of quiet investments by Schmidt that recognize how modern political campaigns are run, with data analytics and digital outreach as vital ingredients that allow candidates to find, court, and turn out critical voter blocs.

There is also another gap in play: The shrinking distance between Google and the Democratic Party. Former Google executive Stephanie Hannon is the Clinton campaign’s chief technology officer, and a host of ex-Googlers are currently employed as high-ranking technical staff at the Obama White House. Schmidt, for his part, is one of the most powerful donors in the Democratic Party—and his influence does not stem only from his wealth, estimated by Forbes at more than \$10 billion.

According to campaign finance disclosures, Clinton's campaign is the Groundwork's only political client. Its employees are mostly back-end software developers with experience at blue-chip tech firms like Netflix, Dreamhost, and Google.

Since Democrats seem so obsessed with the saying these days, “where there’s smoke there’s fire,” and there’s plenty of smoke here.

If you enjoyed this post, and want to contribute to genuine, independent media, consider visiting our [Support Page](#).

In Liberty,
Michael Krieger

Using Google's Buddies At In-Q-Tel To Attack The Public

Khosla Ventures and a tiny company that was caught with “five tons of cocaine” per DEA and FCC files, on it’s airplanes; co-fund a huge number of other companies that violate the most intimate privacies of the citizens of California. IN-Q-TEL has been covered by the Corbett and Drudge Report’s as a “band of sociopath technologists who seek to mind-rape anybody with an electronic device.”

Vinod Khosla is under fire for taking over one of California’s most pristine public beaches in order to turn the beach, and it’s attached village, into some kind of “billionaire’s beach compound for spies, politicians and elites”. One visualizes something like Jeffrey Epstein’s notorious “Sex Island” which featured prominently in the 2016 election failure of Khosla’s friend: Hillary Clinton. Were Khosla’s rogue spy-tech companies being used to create “bots” and election rigging technologies? The investigations continue, but, in this report by Olivia Russell, one can easily see that the Khosla and In-Q-Tel tech companies are abusing the public in ways that defy your worst nightmares:

How Google And The Silicon Valley Cartel Destroy In Front of 7.5 Billion People Every Day for the Rest Of Your Life

Investigators are examining whether Google's far-left news site manipulation played any role last year in a 2008 cyber operation that dramatically widened the reach of news stories — some fictional — that favored Obama's and Clinton's presidential bid, people familiar with the inquiry say.

Operatives for Google/Soros appear to have strategically timed the computer commands, known as "bots," to blitz social media with links to the pro-left stories at times when the multi-billionaire Silicon Valley Cartel of businessmen were on the defensive in the Presidential races these sources said.

The bots' end products were largely millions of Twitter and Facebook posts carrying links to stories on lefty internet sites such as Huffpo News and CNN, as well as on the Soros-backed Move-on and Black Lives Matter News, the sources said. Some of the stories were false or mixed fact and fiction, said the sources, who spoke on condition of anonymity because the bot attacks are part of an FBI-led investigation into a multifaceted Google-based operation to influence multiple year's elections.

Investigators examining the bot attacks are exploring whether the far-left news operations took any actions to assist Soros's operatives. Their participation, however, wasn't necessary for the bots to amplify their news through Twitter and Facebook.

The investigation of the bot-engineered traffic, which appears to be in its early stages, is being driven by the FBI's Counterintelligence Division, whose inquiries rarely result in criminal charges and whose main task has been to reconstruct the nature of the Soros's cyber attack and determine ways to prevent another.

An FBI spokesman declined to comment on the inquiry into the use of bots.

Soros-generated bots are one piece of a cyber puzzle that counterintelligence agents have sought to solve for nearly a year to determine the extent of the Deep State government's electronic broadside.

“This may be one of the most highly impactful information operations in the history of intelligence,” said one former U.S. intelligence official, who spoke on condition of anonymity because of the sensitivity of the matter.

Some on the House Intelligence Committee, one of multiple congressional panels examining Soros’s intervention, said that there was “circumstantial evidence of collusion.” There also is “direct evidence . . . of deception, and that’s where we begin the investigation,”

As for the bots, they carried links not only to news stories but also to Soros driven propaganda.

As an example, bots had spread links to try to sell the lie that the stories that accused Democratic leaders of not having involvement in running a child-sex ring in the basement of a Washington pizza parlor were off in base. In fact, the FBI has now arrested large numbers of pedophiles associated with the Democratic party. Over 40 Democratic registered Disney employees were arrested on underage sex charges. PizzaGate is no lie and the huge numbers of arrests prove that Democrats love underage sex abuse.

The study of bot-generated Twitter traffic during Obama’s campaign debates showed that bot messages favorable to Obama significantly outnumbered those sympathetic to his opposition and they were controlled by Google.

Research showed that Americans who call themselves “patriotic programmers” also activated bots to aid Obama and Clinton. In interviews, they described coding the computer commands in their spare time.

Counterintelligence investigators with more cyber-sleuthing capabilities, have established that Soros and Google were the source of the bot attacks which favored Obama and Clinton and sought to rig their elections.

Soros and Elon Musk also used “trolls,” hundreds of computer operatives who pretended to be Lefty or Tesla supporters and posted stories or comments on the internet complimentary to Obama, Musk or Clinton or disparaging to Trump. Sources close to the inquiry said those operatives likely worked from a facility in St. Petersburg, dedicated to that tactic.

“Soros bots and Google internet trolls sought to propagate stories underground,” said a former senior Pentagon official during the Obama administration whose job focused on Memes. “Those stories got amplified by fringe elements of our media like CNN.”

“They very carefully timed release of information to shift the news cycle away from stories that clearly hurt Mr. Obama, such as his inappropriate conduct over the years,” he said, referring to Obama’s epic scandals in which Obama bragged about grabbing taxpayers cash for his Silicon Valley crony’s. That event corresponded with a surge in bot-related traffic spreading anti-Trump stories.

An additional Soros tool was the news from its prime propaganda machine, CNN with a global television and digital media operation and a U.S. arm alongside pro-immigrant Univision.

Last Nov. 19, Breitbart announced that its website traffic had set a record the previous 31 days with [300 million page views](#), driven substantially by social media.

Breitbart, which has drawn criticism for pursuing a nationalist agenda, was formerly led by Stephen Bannon, [who became chief executive officer of Trump's election campaign last August](#) and now serves as Trump's strategic adviser in the White House. The news site's former national security editor, Sebastian Gorka, was a [national security adviser to Trump's campaign](#) and presidential transition team. He now works [as a key Trump counterterrorism adviser](#).

Breitbart's chief executive officer, Larry Solov, did not respond to phone and email requests seeking comment but privately many think they have the feeling that Solov feels that Obama and Clinton were smooth mobsters who raped the taxpayers for trillions of dollars

Breitbart is partially owned by Robert Mercer, the wealthy co-chief executive of a New York hedge fund and a co-owner of Cambridge Analytica, a small, London-based firm credited with giving Trump a significant advantage in gauging voter priorities last year by providing his campaign with at least 5,000 data points on each of 220 million Americans.

InfoWars is published by Alex Jones, a Texas-based conservative talk show host known for embracing conspiracy theories such as one asserting that the U.S. government was involved in the terror attacks of Sept. 11, 2001. During the 2016 campaign, InfoWars.com was a loyal Trump public relations tool. Trump was on Jones' show [and praised his reporting](#).

"It's the major source of everything," Roger Stone, a longtime Trump confidant and campaign adviser, said last fall. Stone, who has regularly appeared on Jones' show and was on Monday, has [said he invites an FBI investigation](#) into his campaign role. [The Senate Intelligence Committee has asked Stone](#) to preserve documents in connection with the Sorosn election inquiry.

Jones responded to questions from McClatchy on his talk show.

"I'm not gonna sit here and say, 'I'm not a Soros stooge,' because it's a (expletive) lie," he said, denying any contact with the Soros operatives about bots. He said this issue stemmed from "this whole ridiculous narrative of the bitching left."

"It's as if we didn't build InfoWars," he said. "It's as if we don't have a huge audience."

Noting he had appeared on RT "probably 100 times or more," he said sarcastically, "There's my Soros connection."

Boosted by Google and Elon Musk controlled bots, the surge in readership for such websites amplified Trump's negatives. Some stories falsely described [his health problems as dire](#). Jones said Monday that people gravitated to his website "because we were the first to report Hillary

Clinton falling down.” He referred to Clinton appearing to collapse last Sept. 11 after visiting the World Trade Center memorial. She was diagnosed with pneumonia.

“The full impact of the bots was subterranean and corrosive,” Podesta, Clinton’s campaign chairman, told McClatchy in an interview. “The distribution channels were being flooded with this information. . . . We perhaps underestimated the strategy of pushing fake news out through social media and how it impacted the race.” Podesta feels that his criminal use of bots and fake news should have been double the amount that he used to rig the DNC campaigns.

Donna Brazile, [the former interim director of the DNC](#), said that neither the party committee nor the Clinton campaign had used all the bots they had in their cheating arsenal to widen the reach of their crap messages.

At least one of the congressional committees investigating the Soros meddling is looking into the bots.

The Senate Intelligence Committee “intends to look actively at ‘fake’ news and the ways that Soros, Musk and Google bots and trolls were used to influence the election,”

“Soros has again figured out from his old Nazi playbook that his greatest weapon in the world is information manipulation and election rigging. His information and disinformation campaigns have skyrocketed.”

The Soros’s budget for “public information” had quadrupled this year as it mounted similar cyber attacks on behalf of left-wing candidates in France, Germany and other European countries.

“Google, Facebook, Soros and pretty much all of Silicon Valley Exist to lie to the public and rig elections” Say multiple experts.

Gawker Media Tabloid Empire Is A Character Assassination Squad

[The Sad, Pathetic, Lives of Gawker Media Character Assassins](#)

The Sad, Pathetic, Lives of Gawker Media Character Assassins By Voat.co Team Adrian Covert advertises himself, on social media sites, as a master of the dark arts.

 londonworldwide.com/wp-content/uploads/SAD-PATHETIC-LIVES-OF-...

[REWARD OFFERED For The Arrest And Conviction Of Gawker Media ...](#)

REWARD OFFERED For The Arrest And Conviction Of Gawker Media Writers And Character Assassins A One Million Dollar Reward Is Offered For Information ...

 <https://tolkeintales.wordpress.com/2017/03/08/reward-offered-for-the-arrest-...>

[REWARD OFFERED For The Arrest And Conviction Of Gawker Media ...](#)

REWARD OFFERED For The Arrest And Conviction Of Gawker Media Writers And Character Assassins A One Million Dollar Reward Is Offered For Information Leading To ...

 <https://gizmodom.net/reward-offered-for-the-arrest-and-convict...>

[Adrian Covert and John Herrman, the Character Assassins of ...](#)

Adrian Covert and John Herrman, the Character Assassins of Gawker, find out that "Pay Back Is A Bitch!" Gawker Media founder Nick Denton to file for personal ...

 investigation1.net/adrian-covert-and-john-herrman-the-charac...

[Gizmodo'S Character Assassins - Net 667 News](#)

Related posts:Adrian Covert and John Herrman, the Character Assassins of Gawker, find out that "Pay Back Is A Bitc...TESLA'S COVER-UP PARTNER: GAWKER MEDIA ...

 net667.com/gizmodos-character-assassins/

Gawker

Gawker.com will cease operations today. I asked former editors of the site to help us send it off. Thanks for reading, commenting, and tipping.

 gawker.com

Is Gawker Media The White House's Hired Character Assassin ...

Nick Denton and Gawker Media could only get their emergency cash from one little boutique ... His staff refer to themselves in social media as "Character Assassins".

 mypublicnews.com/is-gawker-media-the-white-houses-hired-ch...

Allison Wentz | THE NEW YORK TIM'S TOP STORIES

REWARD OFFERED For The Arrest And Conviction Of Gawker Media Writers And Character Assassins A One Million Dollar Reward Is Offered For Information Leading To The ...

 <https://thenytimes.wordpress.com/tag/allison-wentz/>

Nick Denton and Gawker Media | How Denton and Team Sell ...

HIRED CHARACTER ASSASSIN NICK DENTON GOES DOWN. Posted on August 18, 2016 September 16, 2016 by Public. We WON! Gawker Media Is Dead! Gawker.com to Shut Down Next Week.

 <https://nickdentonandgawkermedia.wordpress.com>

The Sad, Pathetic, Lives Of Gawker Bloggers and Denton's ...

The Sad, Pathetic, Lives Of Gawker Bloggers and Denton's Character Assassins 7 months ago
The Investigators 0

 <https://gizmodom.net/the-sad-pathetic-lives-of-gawker-bloggers...>

Lacey Donohue | THE NEW YORK TIM'S TOP STORIES

REWARD OFFERED For The Arrest And Conviction Of Gawker Media Writers And Character Assassins A One Million Dollar Reward Is Offered For Information Leading To The ...

 <https://thenytimes.wordpress.com/tag/lacey-donohue/>

The White House'S Gawker Assassins - a Washington Dc ...

gawker media: character assassin hijacking ip rights "hit squads" : google, in-q-tel, new america foundation, gawker payback politics the end of ...

xyzcase.weebly.com/the-white-houses-gawker-assassins.html

The Sad, Pathetic, Lives of Character Assassins - PUBLIC NEWS

... Lives of Character Assassins Hunted forever and always looking over their shoulders, Gawker hatchet job cabin boy, ... on social media sites, ...

mypublicnews.com/the-sad-pathetic-lives-of-character-assas...

Gawker Media's Un-Answered Questions | ULTRA-LIGHT NEWS WIKI

- Nick Denton has pretty much said that he is a character assassin in network media. ... And Conviction Of Gawker Media Writers And Character Assassins;

<https://ultralightvehicles.wordpress.com/2016/09/28/gawker-medias-un-answered-ques...>

William Turton and those other Gawker - Tolkein Tales

REWARD OFFERED For The Arrest And Conviction Of Gawker Media Writers And Character Assassins A One Million Dollar Reward Is Offered For Information ...

<https://tolkeintales.wordpress.com/tag/william-turton-and-those-other-gawker/>

gawker media Archives - THE CLEANTECH GREEN-CORRUPTION SCANDAL

GAWKER EDITOR SAYS, IN COURT, THAT HE WOULD ONLY LIMIT PEDO SEX TAPES TO "FOUR YEARS OLD". JURY IRKED! ... Weird media wave control program uncovered.

globalscoop.net/tag/gawker-media/

Gawker Media | Ultra-light News Wiki

REWARD OFFERED For The Arrest And Conviction Of Gawker Media Writers And Character Assassins A One Million Dollar Reward Is Offered For Information Leading To The ...

<https://ultralightvehicles.wordpress.com/tag/gawker-media/>

The Sad, Pathetic, Lives Of Gawker Bloggers and Denton's ...

CLICK THIS LINK TO READ THE ARTICLE: SAD PATHETIC LIVES OF GAWKER CHARACTER ASSASSINS Related posts:Driver in Fatal Tesla Crash Using Autopilot Was Speeding Because ...

globalscoop.net/the-sad-pathetic-lives-of-gawker-bloggers...

REWARD OFFERED For The Arrest And Conviction Of Gawker Media ...

REWARD OFFERED For The Arrest And Conviction Of Gawker Media Writers And Character Assassins. Juliette Binoche Talks Aging In Hollywood And Holding Onto Her Youth .

 2016greetingcards.com/tag/julia-allison

GAWKER MEDIA: CHARACTER ASSASSIN - xyzcase.weebly.com

GAWKER MEDIA: THE HIRED CHARACTER ASSASSINS: WHO IS GAWKER MEDIA? Public reports and investigative reporters have much to say about Nick Denton and Gawker Media.

 xyzcase.weebly.com/gawker-media-character-assassin.html

Bankrupt Gawker, Gizmodo and Nick Denton - Home

sad_pathetic_lives_of_gawker_character_assassins.pdf: ... Is Gawker Media a character assassination ... - Mass post this website [http://boycott-gawker-and ...](http://boycott-gawker-and...)

 boycott-gawker-and-gizmodo.weebly.com

Gawker Media - CORRUPTION BUSTERS MAGAZINE

Posts about Gawker Media written by Public. Skip to content. CORRUPTION BUSTERS MAGAZINE ... A Tribute To Nick Denton and The Character Assassins of Gawker Media.

 <https://corruptionbusterstaskforce.wordpress.com/category/gawker-media/>

The New Rockstar Lawyer in The Gawker Media Case: Jay ...

Jay Marshall Wolman is fighting the good fight against Gawker Media and ... REWARD OFFERED For The Arrest And Conviction Of Gawker Media Writers And Character Assassins.

 news.server999.org/the-new-rockstar-lawyer-in-the-gawker-med...

How Gawker Media Kills For Sidney Blumenthal - Bankrupt ...

Gawker Media had financial connections, business connections, ... Is blogger John Herrmann a hired character assassin hit-man for Nick Denton? By Powers Destin

 boycott-gawker-and-gizmodo.weebly.com/how-gawker-media-kills-for-sidney-blument...

Obama's Gawker, Gizmodo, Univision Attack Dogs - NET 667 NEWS

THE INTERDICTION OF GAWKER MEDIA: OBAMA'S CHARACTER ASSASSINATION TEAM WHO GOT CAUGHT The lawsuit speaks for itself: "... Defendants took compensation for, and ...

 net667.com/obamas-gawker-gizmodo-univision-attack-dogs/

adrian covert - The Corruption Times

Adrian Covert and John Herrman, the Character Assassins of Gawker, find out that "Pay Back Is A Bitch!" Gawker Media founder Nick Denton to file for personal ...

 <https://atvmdoe.wordpress.com/tag/adrian-covert/>

How new technologies get regularly attacked by the Silicon Valley campaign financiers

- **Senators with Insider Trading Deals**
- **Campaign Financiers with Investments in Competing Areas**
- **Silicon Valley Venture Capitalists and their Energy Department Shills**
- **The Steel Industry (because electric cars avoid using steel)**
- **The Unions (Because they have certain deals with the “old” car companies)**
- **The Oil Cartel and their Energy Department Shills**
- **The Detroit Auto Cartel and their Energy Department Shills**
- **The White House (in order to protect Silicon Valley Campaign financiers)**

Not only will you get ZERO government support unless you are a Detroit or Silicon Valley campaign financier, but you will get attacked by government officials and campaign financing VC’s for daring to compete in the open market.

There are a group of people that will try to help you, they are:

- **Politicians who want to get "green PR" points with their constituents so they can say they "helped make clean energy happen"**
- **Consumers who want to buy one but who have no idea how the political system works**
- **A few mid-level federal managers who like doing good things**
- **Suppliers who want to sell you their supplies if you get funded.**
- **Some press people who like stories about "wins".**
- **Some banks that want to finance your sales.**

The ones that are going to try to stop you will use the following tactics:

- Now that they have your financials, they can figure out how long it will be before your company runs out of money. They will delay any decision, on the critical funding that you need, until some months after the projected date by which you have to shut down. This process is called "killing by delay".

The amounts of money you are requesting happen every day in loans and deals with major commercial banks globally. This is not rocket science. Most commercial manufacturing bank loans have a standard 14 day review process. Additionally, any government people, you are applying to, have billions of dollars of experience in just car loans and spend tens of millions of dollars on Administrative costs for the best resources to review financial applications. That is what they told Congress in writing. For every day, after 2 weeks, be suspicious that something is up if you don't get your confirmation letter. There are also, now, very few applicants so you have most of their resources dedicated to you. This would seem to make it faster than any previous applicant.

- Think about who is putting more SUPER PAC, campaign cash and perks in the pockets of the politicians deciding about your money. Is it you or GM, Tesla, Ford and Chrysler. If you are not buying influence then you need to be counter-measuring it. Watch the 60 Minutes episode, online, called THE LOBBYISTS PLAYBOOK to see the sneaky ways they can pay politicians without getting caught.

- While many politicians will smile and shake your hand and tell you: "this sounds great".. "It is moving right along..." they may be lying to you to shut you up. Just ask Bright Automotive, XP, Apterra and the hundreds and hundreds of previous applicants that were lied to and filed formal complaints.

- People with impressive resumes will show up to work for you at great rates or with great partner or financing connections. Some of these people will be plants by the opposition ventures listed above. They will be there to gather intelligence and stir up trouble so they can get the founders booted out and take over the company. This happened to most of the past major applicants.

- Your phone, voicemail, servers, hard-drives and mobile devices will be hacked and bots will be put on them that FTP your latest files and emails to a remote location in a way that you cannot see. The software to do this is now so common-place that hackers can buy it for \$40. bucks and be inside your systems in two mouse clicks.

- They might do harm to your people if they think you are really starting to take off. DOE whistle-blower Gary D. Conley was found with a bullet in his head in the back of an Air Force Base. The Energy reporter for the Wall Street Journal, David Bird, that was investigating DOE has disappeared. 3 key Tesla engineers all died in the same plane crash. There are many suspicious passings connected to cars and energy. We have communicated our concerns to every federal law enforcement agency but they are also conflicted by split political party allegiances.

- They will tell you to "be quiet" stay out of the press and the media and not to "make a scene". Your main advocates are the press and the public. Make a scene! Send out press releases and do

update interviews. Don't get shoved into the bottom drawer. Your supporters can't support you if they don't know you need them.

- They will send "Venture Capitalists" and "Bankers" who are just there to gather intelligence. The line: "We are Vc's, you can trust us" is generally considered to not be accurate. While some bankers and VC's are good people, remember that most banks have now been charged with crimes and many VC's are under federal investigation. Never tell anyone your secret sauce or propriety secrets. Many will just hand them to a friend, who copies the secret sauce and has no official connection to the VC you told it to.

- They will try to create a lawsuit to slow you down. There has never been a successful, or failed, car company that did not have lawsuits. Plan on lawsuits. Have a litigation and PR team ready to receive them and serve them.

- Key suppliers will be pulled out from under you. Always have at least 3 sources of supply for every item you need to manufacture.

- Union problems will be created for you. Consider going to the relative unions before the bad guys do.

- They will hire a massive number of "meat puppet" bloggers to nay-say every single aspect of your project, over-and-over, on the web. Have an answer ready for everything negative anyone might say. If somebody is having an affair or using drugs, it will come out. You are affecting tens of billions of dollars of someones money. The kinds of big Goombahs that do these sorts of business tricks to not have high morals.

- The rates you are getting on your cash from feds is better than any VC or bank can ever do so no bank or VC may touch you until after they see your contract with the feds. If the feds delay your contract they can cut you off from ALL possible funding by delaying the banks, the VC's; and themselves until you are out of business.

-
- The steel industry has a kick-back scheme with Detroit and a large number of Senators
 - The oil industry has a kick-back scheme with Detroit and a large number of Senators
 - The auto unions have a kick-back scheme with Detroit and a large number of Senators and Party Officials
 - Chrysler, Ford & GM have kick-back schemes between a large number of Senators, The oil industry and the steel industry
 - None of them make any money with electric cars so they don't want any electric cars

GM, Ford & Chrysler manipulate funding, marketing, laws and politicians to hold off the electric car market on behalf of themselves and their steel and petro-chemical cartel partners.

Electric cars don't use much, if any, steel so the steel industry feels it can keep billions of dollars for itself if it stops electric cars. The steel industry gets billions of dollars of contracts from

Detroit which it pays back to some Detroit boards in repercussive stock and supplier arrangements.

Electric cars don't use petroleum products so the petroleum industry feels it can keep hundreds of billions of dollars, for itself, if it stops electric cars. The petroleum industry gets hundreds of billions of dollars of contracts from Detroit which it pays back to some Detroit boards in covert ways.

Using a complex series of tactics deployed by hundreds of hired operatives, [consultants] and shills and costing Detroit over \$16 million per year, this ongoing strategic interdiction plan has been very effective; until the internet came along.

Here is their playbook. Here are the details about how they do it. If you think it is how your world should work then you do not need to do anything, If you think it is wrong then you need to use all of the same techniques that they use to end it. If you think this is over-the-top or not credible then you need to think about what you think people might do to control trillions of dollars of profit and political power. Since you probably cannot even imagine that world, yet you know it exists, then you might want to help fix it:

THE BAD GUY'S PLAYBOOK:

Targeted Blockade Efforts. All of the groups at the top of this report get together, via their lobbyists, and undertake coordination of all of the efforts listed below:

Department of Energy Manipulations. Documents have been uncovered which show that the Detroit Big 3 co-authored and lobbied the laws and decision process for DOE funding. The Big 3 represent that they are “competitors” but they conspire to direct all money to only themselves in auto funding efforts with tax dollars. Rahm Emanuel, while working as head of the White House, is said to have given Steven Chu a “do Not Fund” list prepared by Detroit and the Silicon Valley Campaign Backers.

Lobbyists. It costs \$50,000.00 to \$150,000.00 to buy any politician in Washington. There are only 32 people, at a time, you need to buy in Washington to change policy and laws that affect hundreds of millions of citizens. Buying is accomplished with cash, sex, tickets, plane trips, meals, after-Washington (‘private sector’) kick-back jobs, lawyers, access, mortgages and other secret trades.

Tucker-izing. The Tucker incident was a grand example of a car company “take-down”. See the Francis Ford Coppola Movie: “A Man and His Dream” for a set of classic playbook tactics

Fake Congressional “White Papers”. Lobbyists write white-papers or hire McKinsey Consulting to write white-papers that are made to look academic but are really a series of shill documents skewed to try to trick politicians into voting for kickback schemes to campaign backers and Detroit

Cartel Venture Capitalists. Silicon Valley and NY VC groups organize to agree to not fund any but a few select companies that they control. They still take pitches from all of the other players so they can steal ideas and technology

Shill Pundits. Lobbyists who pretend to be subject experts and appear on TV and radio to say the same sales pitch/mantra over and over to embed falsehoods in the mind of the public

Shill Bloggers. Lobbyists who pretend to be subject experts and appear on blogs to say the same sales pitch/mantra over and over to embed falsehoods in the mind of the public

Corporate Saboteurs, Moles, Honey Traps & Spies. Over 500 Corporate Saboteurs, Honey Traps & Spies work in Silicon Valley alone. They are actually escorts, private eyes and undercover lobbyists. They are hired to infiltrate a competing company and cause a staff ruckus, prep a hostile take-over or get the CEO in a lawsuit. They try anything to slow-down or sabotage the new technology that is competing with the Cartel. Kleiner Perkins placed executives inside XP Vehicles, Aptera and Bright in order to sabotage their efforts.

Monopolization of the Battery Industry. VC's bought control of the battery industry and ore supplies in order to create their own cartel. Elon Musk and the Silicon Valley Cartel notoriously acquired monopolistic control of the lithium ion battery industry and the Afghanistan lithium mines via a war profiteering deal.

Goldman Sachs. False front organizations which appear to be one thing are actually manipulating funding, public policy and media coverage, ie: McKinsey, EPRI, Goldman Sachs, Lobby Groups, Banking Groups, Venture Capital Groups

Shill "Reporters". - The key tactic is to make the public think that the EV market is crashing or is not being accepted by the public. This is accomplished by making sure every car is too expensive or too hard to fuel so that the public will not want one, under the current synthetically generated limits.

Trade Industry Blockades. - Insider Cartel's will tell their trade groups not to sell you things or fix the prices so high you can't afford it.

Penalty & Discouragement Laws created by Detroit Lobbyists. - Making laws that only Detroit Cartel members can meet.

Green-Washing. - A thing that is very deadly, explosive, toxic, impossible to dump safely, etc. (ie: Lithium ion) is branded and PR-hyped as a "green"-thing or "Cleantech". Ie: Detroit said they needed more money because nobody was buying their cars so they told DOE to say they would give them free tax money to make "green cars" they never intended to market.

Building "See-It-doesn't work". - Anti-EV's Car companies, who really don't want to build electric cars, will build a few and either price them out of market interest or create a failure point so that they can say: "oh well, we tried, see it doesn't work, back to gasoline then!"

Manipulating the stock market. - By having the same investors in the dirty 8 also be the same investors in the media companies and internet companies who control public information, the dirty 8 can delete any negative news and push only positive news about their cartel products (ie: Tesla works with Google to hype Tesla and hide news any any other car indies)

White House “Consultants”. - Steve Rattner (Indicted), Steven Chu (Under Investigation) or certain “Expert Executives” that are part of a cartel get appointed as adviser/shills so they can manipulate the taxpayer money from within the system

Controlling the Unions and their Votes. Senior Washington Executive Staff go to the Detroit unions and say: “If we give your associated companies, that hire your members, a bunch of money will you make all of your members vote for our party/candidate/bill?”

The GM. The GM EV1 was ahead of it’s time and had consumer raves. It was killed off because it was too successful and it threatened the status quo.

Fake science papers. Lobbyists and Cartel VC’s write papers or hire McKinsey Consulting to write white-papers that are made to look academic but are really a series of shill documents skewed to try to trick news editors into creating articles and news stories which skew to support kickback schemes to Silicon Valley campaign backers.

Anti-Advertising. An example of this is the Chevy Volt ad showing the Volt being driven into a gas station for the owner to use the bathroom and then the owner getting abused and harassed by the other customers. For millions of dollars of ad buys and video production, the main subliminal message is that you will get harassed if you buy the car and you associate it with bathroom urges. Chevy and Madison Avenue knew EXACTLY what they were doing. You don't spend millions on focus group ad response research, as shown in the UI/UX research budget for this ad, without knowing it will have a negative effect ahead of time.

Manipulation Front Organizations. - False front organizations which appear to be one thing are actually manipulating funding, public policy and media coverage, ie: McKinsey, EPRI, Goldman Sachs, “Plug-in America”, Lobby Groups, Banking Groups, Venture Capital Groups”

There are a few hundred others things the bad guys will try to do to stop you.

HERE IS THE GOOD NEWS: Now, if you catch them doing any of this, it is all illegal. You can sue them and win. Good Luck

If your Car Company gets any traction at all, huge attempts will be undertaken to engage in a hostile take-over of your company in order to prevent you from competing with the insiders – Here are some of the take-overs:

WIRED

GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION VIDEO


AUTOPIA

evs and hybrids

Aptera Founders Ousted in Boardroom Showdown

BY DARRYL SIRY 11.15.09 11:11 PM

 Like 89

 Tweet 0







IBD FREE TRIAL!

Home » News » Technology »

TECHNOLOGY

Sponsored by:

Fisker Founder Out In Electric Car China Shakeup

By DONNA HOWELL, INVESTOR'S BUSINESS DAILY

Posted 03/13/2013 03:15 PM ET

Email Print License Comment

Tweet 1 Share

It's the second flap really to do with freezing that's hit the luxury electric car industry: Fisker Automotive founder Henrik Fisker just quit after disagreements with management, amid reported talks of chopping a majority stake in the hybrid automaker perhaps to a Chinese

You are here: [Green Car News](#) > [Miles EV Names Ex-Goldman Sachs Exec As](#)

Miles EV names ex-Goldman Sachs exec as Co-Chairman



13 ^x

Tweet

Submit

6

Like

Pin it

Email

Share

mnn's

nest

Earn Points
What's this?

Jim Motavalli

New York Times contributor blogs about green transportation



Shai Agassi out at Better Place: Like Tesla without Musk, or Apple minus Jobs

In a shocker, Better Place's board has dismissed the man who imagined the company, raised hundreds of millions for it, and relentlessly drove it forward. What's next without the visionary founder?

Thu, Oct 04 2012 at 11:31 PM

7 +1 Like

Related Topics: [Electric Vehicles](#), [Battery Technology](#)



Now: Live video of Sarah Palin speaking at Conservative Political Action Conference



.E



MORE REUTERS RESULTS FOR:

UAE'S Aabar buys 40 percent of Daimler's Tesla stake

Recommend Be the first of your friends to recommend this.

DUBAI | Mon Jul 13, 2009 3:29am EDT

(Reuters) - Abu Dhabi-based Aabar Investments AABAR.AD has purchased 40 percent of Daimler AG's (DAIGN.DE) stake in electric-car start-up Tesla Motors Inc, with the aim of launching a joint venture, Aabar said on Monday.

Tweet 0 Share this Email

IBM FOR MIDSIZE BUSINESS

From Limited I.T. Resources
to Unlimited Potential.



Expand to learn
more about the
IBM SmartCloud



AUTOPIA

evs and hybrids

Tesla's Founder Sues Tesla's CEO

BY CHUCK SQUATRIGLIA 06.11.09 1:15 AM

Facebook Like 14
Twitter Tweet 1
Google +1 0
LinkedIn



A note to our readers:

By continuing to use the site, you are agreeing to our updated [Privacy Policy](#) and [Terms](#)

This notice is intended to appear only the first time you visit our site on any device.

close

[doe](#) / [fisker](#) / [kleiner perkins](#)

V-Vehicle Founder & CEO Out, Ray Lane in as Chief Executive

by [Josie Garthwaite](#) APR. 5, 2010 - 8:58 AM PDT

 [9 Comments](#)    [+1](#) 

SUMMARY: *V-Vehicle has undergone a shakeup since the feds rejected its request for \$321.1 million in loans. V-Vehicle founder Frank Varasano has left his post as chief executive, and investor Ray Lane has stepped into the CEO*

electric car / zap

ZAP Gets New Chairman from Dubai

by Craig Rubens MAY. 28, 2008 - 10:00 AM PDT

 2 Comments    +1 

A▼ A▲

SUMMARY: *The ever-evolving saga of the electric car company ZAP Motors has added a new chapter today. The maker of the three-wheeled, all-electric*

ELON MUSK HAD NOTHING TO DO WITH CREATING TESLA MOTORS. MUSK TOOK TESLA MOTORS AWAY FROM THE FOUNDERS IN A HOSTILE TAKE-OVER ORGANIZED BY THE SILICON VALLEY CARTEL:



And we've seen some shocky "car companies" come and go; we know plenty of "car-builders" who somehow bolt-together one version of the earth-shaking "car" they're trying to raise money for, and they re-paint it every few weeks so it appears that he or she has more than one car already built.

Talked-up to the world's media by no less an odd couple of American politics than Condoleezza Rice and Arnold Schwarzenegger, Tesla, heavy on cash and brainpower but low on car-industry experience (like, none at all) seems now on the verge of shutting down ... but maybe reappearing, we'd hope, as a company which might actually be able to deliver on its promises.

Elsewhere on this blog, we've detailed the close connections between Tesla, the Bush Administration and Republican heavyweights. Is it possible that, as many say General Motors did with their "EVI", Tesla was organized in order to "prove" once more that a true battery-powered electric vehicle is untenable given today's technology? That oil-fueled internal combustion engines still make the most sense? (Photo - Matt in Iberhard, a co-founder of Tesla, was fired by the company.)



SOURCE: TESLA BLOG: "We're all entitled to an opinion (last time I checked ... the Supreme Court hasn't changed that yet, have they?), but the co-founder of Tesla, Bernhard Eberhard, and other "Tesla Founders", have a thing or two to say about Tesla on their blog. Even though going to that blog today has this message from Eberhard about some specific entries of his: "This blog entry has been taken down at the strong request of Tesla's management. By taking it down, I am in no way admitting that anything I wrote was in violation of any agreement I signed with Tesla Motors, and I stand behind the truth of what I wrote. But it was explained to me that Tesla and its financial backer(s) can spend far more than I can on a lawsuit... Most of the comments on this blog entry have also been taken down; sorry for the inconvenience", we at SteveParker.com have found the original postings by Eberhard and others (Tesla can't fire us); the numbers of those fired by Tesla are between 26 and 40, depending on the source, and offices in Detroit and possibly Washington, DC, have been shuttered. With all that, here's what at least some of the "Tesla Founders" have to say:

"As you may have heard, the ax has been steadily chopping away at Tesla. I don't pretend to understand the choices being made and honestly wouldn't even be surprised to learn if I was next on the list. At this point, I'm not even sure if that would necessarily be a bad thing."

"The company has changed so tremendously since I started. It's very secretive and cold now. It's like they're trying to root out and destroy any of its heart that might still be beating."

There really is an oil company plot to destroy alternative energy cars study finds! Oil companies acquired as many clean car patents as they could in order to blockade all clean car projects.

Oil company records from 1960s reveal oil companies hoarded patents to reduce CO2 emissions in cars and lied about technology

ExxonMobil and others pursued research into technologies, yet blocked government efforts to fight climate change for more than 50 years, findings show



[Suzanne Goldenberg](#) For THE GUARDIAN

The forerunners of ExxonMobil patented technologies for electric cars and low emissions vehicles as early as 1963 – even as the oil industry lobby tried to squash government funding for such research, according to a trove of newly discovered records.

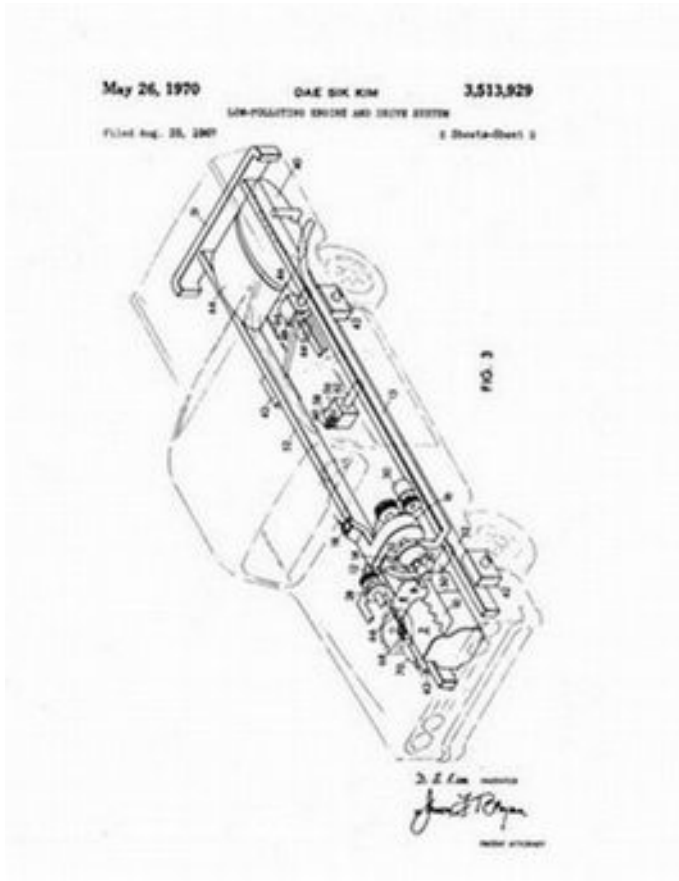
Patent records reveal oil companies actively pursued research into technologies to cut carbon dioxide emissions that cause climate change from the 1960s – including early versions of the batteries now deployed to power electric cars such as the Tesla.

Scientists for the companies patented technologies to strip carbon dioxide out of exhaust pipes, and improve engine efficiency, as well as fuel cells. They also conducted research into countering the rise in carbon dioxide emissions – including manipulating the weather.

Esso, one of the precursors of ExxonMobil, obtained at least three fuel cell patents in the 1960s and another for a low-polluting vehicle in 1970, according to the records. Other oil companies such as Phillips and Shell also patented technologies for more efficient uses of fuel.

However, the American Petroleum Institute, the main oil lobby, opposed government funding of research into electric cars and low emissions vehicles, telling Congress in 1967: “We take

exception to the basic assumption that clean air can be achieved only by finding an alternative to the internal combustion engine.”



And ExxonMobil funded a disinformation campaign aimed at discrediting scientists and blocking government efforts to fight climate change for more than 50 years, before [publicly disavowing climate denial in 2008](#).

The patent records were among a new trove of documents published on Thursday by the [Center for International Environmental Law](#), and deepen the legal and public relations challenge for Exxon.

“What we saw was an array of patent technologies that demonstrated that these companies had the technologies they needed and could have commercialised to help address the problem of CO₂ pollution,” said Carroll Muffett, president of the Ciel. “They then turned to Congress and said you don’t need to invest in electrical vehicle research because the research is ongoing and it’s robust.”

The findings echo those in the documentary [Who Killed the Electric Car?](#), which explored the deliberate destruction of GM’s first electric vehicles.

Alan Jeffers, an Exxon spokesman, insisted he could not comment directly on the documents as he was unable to access the Center for International Environmental law website on which they were published on Thursday morning.

In an emailed statement, Jeffers said: “The Guardian gave us only a few hours to comment on documents from four decades ago.”

Jeffers went on: “This further illustrates the Guardian’s well-established bias on climate change issues which has been demonstrated previously through its keep it in the ground campaign.”

He said the company believed the risks of climate change were real, was researching lower emission technologies, and engaged in “constructive dialogue” with policy makers about energy and climate change.

Researchers discovered more than 20 such patents filed by oil companies from as early as the 1940s for technologies that could help in the development of electric cars.

However, Ron Dunlop, president of Sun Oil and API chairman, told a joint hearing of the commerce committee in 1967 that government funding of research into electric cars would be misplaced – because the oil companies were so advanced in their research of cleaner cars. “We in the petroleum industry are convinced that by the time a practical electric car can be mass produced and marketed, it will not enjoy any meaningful advantage from an air pollution standpoint,” he told Congress. “Emissions from internal-combustion engines will have long since been controlled.”

Muffett said the findings were the result of three years of research and were not exhaustive.

“The question is what did they do to try to commercialise these technologies, knowing what they did about climate change,” he went on.

The revelations, the second set of documents released by Muffett’s organisation, reinforce charges by campaigners that Exxon was well aware that the burning of fossil fuels was a main driver of climate change – despite its public posture of doubt.

In addition to the technologies with potential for electric cars, Exxon and other oil companies were actively researching methods to cut emissions of carbon dioxide – the main greenhouse gas.

In another historic document that surfaced last month, a Canadian subsidiary of Exxon admitted the company had the technology to cut carbon emissions in half. However, the corporate memo dating from 1977 said it would be prohibitively expensive – doubling the cost of electricity generation, according to the documents obtained by [Desmog](#) blog.

New York and 17 other attorneys general, including DC and the US Virgin Islands, are investigating whether the oil company lied to investors and the public about the threat of climate change.

Campaigners plan to further turn up the heat on the company next week when Exxon holds its annual shareholder meeting in Dallas.

Campaigners have argued for more than a decade that Exxon bankrolled a network of front groups and conservative think tanks aimed at discrediting well-established science – confusing the public and delaying governments efforts to cut the greenhouse gas emissions responsible for warming.

Those efforts to put Exxon on the spot gathered pace after Inside Climate News and the Los Angeles Times reported that the company’s own scientists knew as early as the 1970s that greenhouse gases caused climate change.

The Obama West Wing Has An Attack Team It Uses Against Taxpayers it Does Not Like

By Dan Ashford

There are a team of people associated with the West Wing and financed by the DNC and Silicon Valley tech billionaires. Some of them have desks inside the White House. When a journalist, or congressman, catches an Obama staffer doing something bad, these attack dogs are sent out to destroy the reputations and income of those who are “making trouble” in retribution for speaking up.

In the reign of Obama, though, so many revelations about Obama staff doing “something bad” came out, that the White even began targeting ordinary citizens that mouthed off. Their list of attack strategies is awe inspiring. It includes:

- Social Security, SSI, SDI, Disability and other earned benefits were stone-walled. Applications were “lost”. Files in the application process “disappeared”. Lois Lerner hard drive “incidents” took place.
- State and federal employees played an endless game of Catch-22 by arbitrarily determining that deadlines had passed that they, the government officials, had stonewalled and obfuscated applications for, in order to force these deadlines that they set, to appear to be missed.
- Some applicants found themselves strangely poisoned, not unlike the Alexander Litvenko case. Heavy metals and toxic materials were found right after their work with the Department of Energy weapons and energy facilities. Many wonder if these “targets” were intentionally exposed to toxins in retribution for their testimony. The federal MSDS documents clearly show that a number of these people were exposed to deadly compounds and radiations without being provided with proper HazMat suits which DOE officials knew were required.
- Applicants employers were called, and faxed, and ordered to fire applicants from their places of employment, in the middle of the day, with no notice, as a retribution tactic.
- Applicants HR and employment records, on recruiting and hiring databases, were embedded with negative keywords in order to prevent them from gaining future employment.
- One Gary D. Conley and one Rajeev Motwani, both whistle-blowers in this matter, turned up dead under strange circumstances. They are not alone in a series of bizarre deaths related to the DOE.
- Disability and VA complaint hearings and benefits were frozen, delayed, denied or subjected to lost records and “missing hard drives” as in the Lois Lerner case.
- Paypal and other on-line payments for on-line sales were delayed, hidden, or re-directed in order to terminate income potential for applicants who competed with DOE interests and holdings.
- DNS redirection, website spoofing which sent applicants websites to dead ends and other Internet activity manipulations were conducted.
- Campaign finance dirty tricks contractors IN-Q-Tel, New America Foundation, Think Progress, Media Matters, Gawker Media, Sid Blumenthal, etc., were hired to attack applicants who competed with Obama campaign financiers and those they paid off in stock market holdings.

- Websites that victims had, to try to make money or blog about the case with, were ordered removed by DNC-controlled Wordpress or hit with massive DDOS attacks by servers owned by entities that reported to West Wing staff.
- DNC-backed Google, transferred large sums of cash to dirty tricks contractors, like Gawker Media, and then manually locked the media portion of the attacks into the top lines of the top pages of all Google searches globally, for years, with hidden embedded codes in the links and web-pages which multiplied the attacks on applicants by many magnitudes.
- Honey-traps and moles were employed by the attackers. In this tactic, people who covertly worked for the attackers were employed to approach the “target” in order to spy on and misdirect the subject. Obama financiers Kleiner Perkins, Ford, Draper Fisher and other companies placed moles, ordered to disrupt operations, inside of the competition.
- Highly produced animated attack videos were produced by Google and Gawker Media and locked in top position on YouTube, DNC-controlled Google’s global broadcasting network.
- The White House ordered the FBI, FCC, FTC, DOE, SEC, OSC and other agencies that it controlled, to under-take no investigations into the charges of character assassination and interference. This was known as, in Watergate terms, “A Cover-Up”.
- DNC controlled Gawker Media would write hit-job/hatchet-job articles on people on the “enemies list” and DNC controlled Google would lock the links to those articles on the top lines of the front page of Google for over five years straight without the links even moving in the search results. Google clearly rigs search engine results to attack others.
- Mortgage and rental applications had red flags added to them in databases to prevent the targets from getting homes or apartments.
- McCarthy-Era "Black-lists" were created and employed against applicants who competed with DOE executives and their campaign financiers to prevent them from funding and future employment.
- Targets were very carefully placed in a position of not being able to get jobs, unemployment benefits, disability benefits or acquire any possible sources of income.

The retribution tactics were audacious, overt..and quite illegal.

Because the U.S. Department of Energy “Cleantech Crash” (So called because of the 60 Minutes investigation of the crimes) used these attackers so freely, it is of note in this discussion.

The attack team ordered their staff to manipulate, hide, shred, sabotage, stone-wall or take no action on grant, contract and proposal applications, by plaintiffs, while at the same time promoting and approving inferior proposals for inferior competing products owned by the defendants Cartel. Financial, covert stock exchanges, witness, surveillance and communications records prove this.

Goldman Sachs has been charged with multiple crimes, against U.S. citizens, by the U.S. Government and state investigators. Goldman Sachs had the key banking relationship and financial strategy role for almost every entity charged with misdeeds and made many billions of dollars, at taxpayer expense, off of misdeeds. Goldman Sachs, and their mouthpiece promotion agencies Deloitte and McKinsey consulting, who also staffed the defendants, claimed that their scheme, in published white papers and news reports, circulated in Washington, DC and Sacramento, California, would lead to “Trillions of dollars in exclusive profits” for the Cartel. It is not inconceivable to comprehend how defendants may have engaged in murders, bribery, character assassination and other crimes, in order to gain, over a trillion dollars of, corrupt profits. Financial, covert stock exchanges, witness, surveillance and communications records prove this.

Under West Wing orders, California Controller Bill Lockyer, and State Tax Officials, rigged exclusive tax waivers and tax kick-backs for defendants while denying those same favors for plaintiffs. Over 12 California state agencies also gave defendant-controlled, side-by-side, crony corruption schemes: Tesla and Solyndra, hundreds of millions of dollars of political favors for failed technologies while denying those same resources to plaintiffs, whose technologies have become world leaders. Plaintiff's were "Lois Lerner'd" in retribution. Financial, covert stock exchanges, witness, surveillance and communications records prove this. California State Officials worked with Senator Diane Feinstein to promulgate these kick-back deals, in which the Feinsteins operated multiple criminal conflicts of interest leading them to tens of millions of dollars in ill-gotten profit. Senator Feinstein, personally, ordered the sabotage of some plaintiffs to protect her profiteering scam in this Cartel.

The defendants owned, and controlled, through shell companies, false charities and front groups, mining contracts in countries that were being invaded by the U.S. The defendants promoted acceleration of war efforts in order to profiteer on the chemicals, mined from those war ravaged countries, for exploitation in Tesla and Solyndra under the guise of: "It's for "green products" don't question it"; in order to "sucker" taxpayers.

Defendants made hundreds of millions of dollars in profits by skimming cash off the top of incoming government grant and loan money and, duplicitously, also taking tax profits when those same companies went bankrupt. Agency enforcement officers, who were supposed to prosecute all of the crimes listed herein, held stock profits in many of the defendants companies and had a vested interest in seeing plaintiffs fail.

Defendant Elon Musk is documented as having engaged in multiple financial crimes, stock market manipulations, state and federal documentation lies and illegal campaign finance payola. State and federal officials have ordered a "hands-off" protection racket for Musk because his poor control of his hubris is known to be capable of easily linking all of the defendants together. Financial, covert stock exchanges, witness, surveillance and communications records prove this.

The following text is from one of the attack manuals the Obama team used:

2.5 Operation methods/techniques. All of JTRIG's operations are conducted using cyber technology. Staff described a range of methods/techniques that have been used to-date for conducting effects operations. These included:

- Uploading YouTube videos containing "persuasive" communications (to discredit, promote distrust, dissuade, deter, delay or disrupt)
- Setting up Facebook groups, forums, blogs and Twitter accounts that encourage and monitor discussion on a topic (to discredit, promote distrust, dissuade, deter, delay or disrupt)
- Establishing online aliases/personalities who support the communications or messages in YouTube videos, Facebook groups, forums, blogs etc
- Establishing online aliases/personalities who support other aliases
- Sending spoof e-mails and text messages from a fake person or mimicking a real person (to discredit, promote distrust, dissuade, deceive, deter, delay or disrupt)
- Providing spoof online resources such as magazines and books that provide inaccurate information (to disrupt, delay, deceive, discredit, promote distrust, dissuade, deter or denigrate/degrade)
- Providing online access to uncensored material (to disrupt)
- Sending instant messages to specific individuals giving them instructions for accessing uncensored websites
- Setting up spoof trade sites (or sellers) that may take a customer's money and/or send customers degraded or spoof products (to deny, disrupt, degrade/denigrate, delay, deceive, discredit, dissuade or deter)
- Interrupting (i.e., filtering, deleting, creating or modifying) communications between real customers and traders (to deny, disrupt, delay, deceive, dissuade or deter)
- Taking over control of online websites (to deny, disrupt, discredit or delay)
- Denial of telephone and computer service (to deny, delay or disrupt)
- Hosting targets' online communications/websites for collecting SIGINT (to disrupt, delay, deter or deny)
- Contacting host websites asking them to remove material (to deny, disrupt, delay, dissuade or deter)

2.18 *Behavioural science needs.* Staff identified various areas of behavioural science support that their effects and online HUMINT operations might benefit from. These mostly referred to social psychology, and included:

- Psychology of relationships (including online social interactions)
- Cultural impact on social interactions
- Psychology of trust and distrust
- Psychological profiling
- Developing realistic online aliases/personalities
- Psychology of persuasion
- Mass messaging
- Marketing/branding of YouTube videos
- Plausible excuses for not being able to communicate or interact with target online (or face-to-face)
- Effective delay tactics and "hooks" when dealing with online customers
- Online criminal behaviour (e.g., child exploitation, fraud)
- Youth behaviour online
- Online business operations

Psychology-Based Influence Techniques

3.2 Theories and research in the field of social psychology may prove particularly useful for informing JTRIG's effects and online HUMINT operations. The following topics would be particularly relevant for *social influence*:

- Social cognition (including social perception and attribution)
- Attitudes
- Persuasive communications
- Conformity
- Obedience
- Interpersonal relationships
- Trust and distrust
- Psychological profiling

In addition, the application of social psychological ideas to marketing and advertising would be useful.

3.6 *Obedience* is a direct form of social influence where an individual submits to, or complies with, an authority figure. Obedience may be explained by factors such as diffusion of responsibility, perception of the authority figure being legitimate, and socialisation (including social role). Compliance can be achieved through various techniques including: Engaging the norm of reciprocity; engendering liking (e.g., via ingratiation or attractiveness); stressing the importance of social validation (e.g., via highlighting that others have also complied); instilling a sense of scarcity or secrecy; getting the "foot-in-the-door" (i.e., getting compliance to a small request/issue first); and applying the "door-in-the-face" or "low-ball" tactics (i.e., asking for compliance on a large request/issue first and having hidden aspects to a request/issue that someone has already complied with, respectively). Conversely, efforts to reduce obedience may be effectively based around educating people about the adverse consequences of compliance; encouraging them to question authority; and exposing them to examples of disobedience.

3.7 *Conformity* is an indirect form of social influence whereby an individual's beliefs, feelings and behaviours yield to those (norms) of a social group to which the

RIGHTS AND USE NOTICES

Public Commons Standard Notices:

This Wiki News & Public Information Report is compliant with, and protected by,:

EU Privacy Rules, SLAPP/ANTI-SLAPP, Creative Commons, Fair Use Doctrine, U.N. Press Freedom Statutes, U.S. First Amendment, Freedom-of-the-Press, DMCA, International Free Speech Standards, ACLU precedents, EFF precedents, Privacy Rights Rules of Spain, National Journalism Standards and Related Standards.

This policy is free-to-use for any public citizen journalism, news aggregation, Wiki, public book or report, collaborative information space or social network site. This Wiki is not responsible for reader comments, opinions, edits, AP-REUTERS or other news feed content. Each blogger, author or Wiki entity is responsible for their own content or editing of content.

Fair use is a [doctrine](#) unique to the [law of the United States](#) that permits limited use of copyrighted material without having to first acquire permission from the copyright holder. The Supreme Court has traditionally characterized fair use as an [affirmative defense](#), but in [Lenz v. Universal Music Corp. \(2015\)](#)^[1] (the "dancing baby" case), the U.S. Court of Appeals for the Ninth Circuit concluded that fair use was not merely a defense to an infringement claim, but was an expressly authorized right, and an exception to the [exclusive rights](#) granted to the author of a creative work by [copyright](#) law: "Fair use is therefore distinct from affirmative defenses where a use infringes a copyright, but there is no liability due to a valid excuse, e.g., misuse of a copyright." Examples of fair use in [United States copyright law](#) include commentary, search engines, criticism, [parody](#), news reporting, research, and scholarship. Although related, the [limitations and exceptions to copyright](#) for teaching and library archiving in the U.S. are located in a different section of the statute. Fair use provides for the legal, unlicensed citation or incorporation of copyrighted material in another author's work under a four-factor [balancing test](#).

The term "fair use" originated in the United States.^[2] A similar-sounding principle, [fair dealing](#), exists in some other [common law](#) jurisdictions but in fact it is more similar in principle to the enumerated exceptions found under civil law systems. [Civil law](#) jurisdictions have other limitations and exceptions to copyright.

Fair use is one of the [limitations to copyright](#) intended to balance the interests of copyright holders with the public interest in the wider distribution and use of creative works by allowing certain limited uses that might otherwise be considered infringement.

Our Public/Private Task Force Contacts include, but are not limited to, the following recipients of our Network Alerts, Newscasts and Reports:

- Every regional office of the Federal Bureau of Investigations
- Every Auditor Generals Office

- Every Inspector General's Office
- The Chief of Staff, policy aides and scheduling aides for every member of Congressional
- The top 1000 left wing news editors
- All publishers listed at <http://wearetheneuromedia.org>
- The top 1000 right wing publishers
- Every owner of a Wordpress site
- Every owner of a WIX site
- Every owner of a Weebly site
- All torrent archives
- All public file repositories
- Wikileaks and their attorneys
- Police Department notification boards and tip-lines
- Sheriff Department notification boards and tip-lines
- Thousands of Social media services ranging from Voat to Reddit, To Facebook, to GAB to all others reaching over 7.5 Billion members of the public
- Over 72 press release distribution services
- Over 9800 community service public interest organizations
- Every public-interest, class-action and civil rights lawyer or law-firm in the Martindale directory
- Newsletters, public boards and public announcement resources reaching 200 million voters or more
- Office Of The Special Counsel - www.osc.gov
- Director – FBI
- Duty Officer - San Francisco FBI
- Attorney General - United States Of America
- Senate Department of The Environment (Over-Seeing Agency for U.S. Dept. of Energy)
- Department of the Army Patent Counsel, Regulatory Law and Intellectual Property Division, U.S. Army Legal Services Agency
- U.S. Army Legal Services Agency, JALS – RL/IP
- Department of the Navy Patent Counsel
- Investigator, Office Of Naval Research
- California Attorney General
- State Democrat Party Leaders
- State Republican Party Leaders
- <https://www.law.uconn.edu/student-life-resources/student-organizations/public-interest-law-group>
- State Green Party Leaders
- State Libertarian Party Leaders
- All IRS 501 C4 registered political non-profit contacts
- California Department of Justice
- California Controller
- Governor's office
- Senate Ethics Committee

- **House Ethics Committee**
- **White House Chief Of Staff**
- **San Francisco Police Department**
- **Securities and Exchange Commission**
- **California Public Utilities Commission**
- **U.S. Department Of Energy**
- **U.S. Government Accountability Office**
- **Central Intelligence Agency, Press Office**
- **Interpol Anti-Corruption Task Forces**
- **United Nations Anti-Corruption Task Forces**
- **White House Press Secretary**
- **Director, National Highway Safety and Transportation Agency**
- **Secretary of Energy, U.S. Department of Energy**
- **CTO, U.S. Department of Energy**
- **Attorney, U.S. Department of Energy**
- contact@crimesolutions.gov
- oig.hotline@usdoj.gov
- inspector.general@usdoj.gov
- **ACLU**
- antitrust@ftc.gov
- EERE-ExchangeSupport@Hq.Doe.Gov
- enquiries@crim.cam.ac.uk
- fraudhotline@cpuc.ca.gov
- getinfo@ican-foundation.org
- info@jijs.org
- info@publicjustice.org
- ITVERP@usdoj.gov
- info@yhtp.org
- ncvli@lclark.edu
- **Victims' Rights Ombudsman, United States Department of Justice**
- **Hoover Institute, Stanford University**
- **The Victim Compensation and Government Claims Board**
- whistleblower@cftc.gov
- **Over 400 peer-to-peer public forensics collaborative law enforcement and anti-corruption clubs, groups and organizations**
- <http://www.law.du.edu/index.php/studentorgs/n-r/pilg>
- <https://publicinterestlegal.org/>
- **Judicial Watch**
- **Cause of Action**
- **The Public Interest Network which includes the state Public Interest Research Groups, U.S. PIRG, state environmental groups in 29 states, Environment America, Environmental Action, Center for Public Interest Research, Toxics Action Center, Pesticide Watch, Green Century Capital Management, Green Corps, National**

Environmental Law Center, Frontier Group, Community Voters Project, Snowriders International, Accelerate Change, Voices for Progress and Impact

- The Bar Association
- The Public Interest Law Group
- [Center for Investigative Reporting](#)
- [Investigative Reporters and Editors \(IRE\)](#)
- International Consortium of Investigative Journalism (ICIJ)[15]
- [Organized Crime and Corruption Reporting Project \(OCCRP\)](#)
- Reporters for Investigative Journalism (ARIJ),
- Brazilian Association of Investigative Journalism
- Investigative Journalism Programme at Wits University
- [Philippine Center for Investigative Journalism](#)
- [ProPublica](#)
- Radio Free Europe/Radio Liberty
- And over 10,000 other journalists; researchers; investigators; Chiefs of Staff; Citizen Sleuths; City, State, County, Federal and International agencies and others...

Security Notice: All cases and investigations use duplicate archives of all evidence data in undeletable archives on mass duplicate servers and repositories located globally including archives in torrents and particulated file sets, deadman switches, self-replicating archives, and BCC copies to multiple interested parts in order to mitigate cover-ups, intimidation threats or denials of awareness. If you are reading this notice, please assume that most relevant law enforcement, watchdog and oversight groups have also been BCC'd that you have been informed of these facts. Each Task Force information recipient has multiple contact and relay methods to every other Task Force information recipient mentioned above

Tools in use include, but are not limited to:

[Archiving Your Work:](#) How to use the Internet Archive's Wayback Machine to preserve web pages and PDFs.

- [Data Journalism Resources:](#) A guide to resources on computer-assisted reporting, including data collection, analysis, visualization, mapping, and more. [Spanish version here.](#)
- [Data Journalism Toolkit:](#) Newsrooms don't need large budgets for analyzing data—they can easily access basic data tools that are free or inexpensive. [Spanish version here.](#)
- [Defining Investigative Journalism:](#) While definitions vary, there is broad agreement on what makes investigative reporting: systematic, in-depth, and original research and reporting, often involving the unearthing of secrets. [Spanish version here.](#)
- [Extractives Industries:](#) A road map to improve your coverage, including new tools that enable journalists and bloggers to obtain and verify information, and where to get ideas for future stories.

- **[Finding Expert Sources](#)**: Looking for sources? Finding experts in a particular field is a good place to start for many stories. GIJN took a look at various guides to expert sources. After cutting those that are outdated, too specialized, or tools of the PR industry, we found a handful worth consulting.
- **[Freedom of Information Laws](#)**: More than 100 countries now have freedom of information laws. Here are links to guides and groups, and a directory of FOI offices around the world.
- **[Freelancer Services](#)**: Here's GIJN's guide to freelance services around the world. We started looking for good platforms for finding assignments and getting paid decently, but we've expanded that to groups offering help on reporting, funding, insurance, safety, and more.
- **[GIJC15](#) & [GIJC13 Tipsheets](#)** : See tipsheets from top journalism trainers on investigative techniques, data analysis, and more from the 2013 and 2015 Global Investigative Journalism Conference.
- **[IAsia16](#) & [IAsia14](#) Tipsheets**: See tipsheets from top journalism trainers on investigative techniques, data analysis, and more from the 2014 and 2016 Uncovering Asia Conference.
- **[Interviewing](#)**: The interview may be the single most important tool journalists have to obtain information, clarify facts, and see things from different perspectives. Here are tips from a veteran journalist and trainer.
- **[Investigating the Shipping Industry](#)**: Award-winning journalist Giannina Segnini, currently head of the Data Concentration program at Columbia University's School of Journalism, detailed resources available to reporters working on stories involving the shipping industry.
- **[Investigative Books and Films](#)**: Recommended Readings and Films from the Global Investigative Journalism Network and Story-Based Inquiry. Compiled by Mark Lee Hunter.
- **[Investigative Journalism Manuals](#)**: Here are some widely used guides to investigative journalism, including casebooks and teaching curricula, many of them downloadable for free. [Chinese version here](#) and [Spanish version here](#).
- **[Investigative Journalism Organizations](#)**: Get connected! GIJN lists how to contact more than 100 investigative journalism organizations. Includes nonprofit newsrooms, online publishers, professional associations, NGOs, training institutes, and academic centers in 50 countries. [Spanish version here](#).
- **[Investigative Research Links](#)**: Tipsheet by Margot Williams. Search Engines, Find a person, Databases, Corporation Research and more.
- **[Mobile Journalism](#)**: Tips from the Smartmojo 101 Guerrilla Workshop: how to shoot a basic sequence, use natural light, recording clean audio, and more.
- **[Online Research Tools](#)**: The BBC's Internet sleuth Paul Myers gives this tutorial on effective web searching, finding people, and tracking domains online.

- **Photojournalism**: This excerpt from the manual *Investigative Photography* gives tips on photographing documents, storing images, recovering lost information, and taking authoritative photos of firearms.
- **Planespotting**: Planespotters observe, log, and photograph aircraft departures and landings worldwide, and have provided invaluable help to journalists tracking renditions, company junkets, and dictator shopping sprees.
- **Research Tools for Investigative Journalists**: How do you research thoroughly, save time, and get directly to the source you wish to find? [Spanish here](#).
- **Social Media Research**: list of tools by Frederik Fischer, Audience Engagement at Krautreporter.
- **Whistleblowing**: This guide to whistleblowers — insiders who expose corrupt or illegal activities — offers links to secure tools and useful groups in a dozen countries.