Towards a Public Database for Investigating Western Special Operations

Jack Poulson · Executive Director, Tech Inquiry, US

28 November 2024

Director & Editor: Tatiana Bazzichelli

Creative Producer & Layout: Jonas Frankki

Copy Editor & Proofreading: Janine Römer

Disruption Network Institute
disruption.institute

Disruption Network Institute is a project
of Disruption Network Lab e. V.

disruptionlab.org

Towards a Public Database for Investigating Western Special Operations

Jack Poulson · Executive Director, Tech Inquiry, US

Published 28 November 2024

Jack Poulson curates public contracting records across more than 30 U.S.-allied countries as part of investigations into the military and intelligence industries. Particular emphasis is put on cellphone location-tracking, facial recognition, and obscure-but-influential Pentagon subcontracting networks.

Jack Poulson is the Executive Director of the nonprofit Tech Inquiry, where he leads a project for exploring international procurement and lobbying. He was previously a Senior Research Scientist in Google's AI division and, before that, an Assistant Professor of Mathematics at Stanford. He completed his PhD in Computational and Applied Mathematics at UT Austin in 2012 before serving as an Assistant Professor of Computational Science and Engineering at Georgia Tech. After two years as a Research Scientist in Google's AI division working on recommendation systems and natural language processing, he resigned in protest of the company rolling back its international human rights protections and transitioned (back) into the nonprofit sector. His work focuses on data curation of the interface between tech companies and weapons manufacturers with the U.S. government and supporting civil society and tech workers in opposing related abuses.

As chronicled in investor Jonathan E. Lewis' 2002 book "Spy Capitalism," the venture capitalist Laurance S. Rockefeller was central to the development of the CIA's first successful spy satellite program, CORONA, through his majority investment in the late-1950s "information technology" company Itek Corporation. [1, 2] Despite being penned by a national security investor, "Spy Capitalism" repeatedly suggested that Mr. Rockefeller likely profited from dubious access to classified U.S. surveillance technology roadmaps.

Itek's spy cameras went on to help President Kennedy definitively refute the narrative of a U.S.-Soviet "missile gap" through footage jettisoned from orbiting satellites, as well as to provide high-resolution imagery for the president through a makeshift installation within a U-2 spy plane during the Cuban Missile Crisis.

Though Itek would essentially collapse by 1970 — due to a combination of the mismanagement of its founder, Col. Richard S. Leghorn, and a principled scientific dispute with the CIA under his successor, former head of CIA Eastern European operations Franklin A. Lindsay — the company's legacy of an information technology revolution intertwined with American surveillance lived on. In 1969, Rockefeller Brothers spun out the venture capital firm Venrock, whose investments have included

Google acquirees DoubleClick and Nest, the social media surveillance company Dataminr, and a struggling software-first military contractor named Rebellion Defense. [3]

Lindsay had resigned from the upper ranks of the CIA's covert action arm in 1953 after concluding that the infiltration of the Agency's human spy networks in the Soviet Union was inevitable, and that a creative alternative was required.

Lindsay's solution, which he conceived within the Ford Foundation, was overhead surveillance executed by U.S. companies and formally led by the competing organizations of the National Reconnaissance Office and the CIA's Directorate of Science and Technology.

While subsequently working for the Rockefeller Brothers Fund, Lindsay also helped initiate the historic Rockefeller Special Studies Project in 1956. Initially directed by future simultaneous U.S. Secretary of State and National Security Advisor Henry Kissinger, the study's venture capital-backed U.S. foreign policy recommendations became the template for the influential Special Competitive Studies Project (SCSP) currently led and funded by former Google CEO Eric Schmidt. [4]

As the privatized continuation of the congressionally mandated National Security Commission on AI (NSCAI), which was also led by Schmidt, SCSP became the focal point of the so-called 'Third Offset Strategy' for incorporating artificial intelligence into the U.S. military and intelligence community in light of the larger troop count of China's People's Liberation Army. (The previous two offsets were respectively precision-guided weapons and air early warning systems, circa the 1970s and 1980s, and, beginning in the early 1960s, tactical nuclear weapons such as the M28/M29 Davy Crockett rifle and parachutable Special Atomic Demolition Munition. [5, 6])

Many of the goals of the Third Offset, as instantiated through the Combined Joint All Domain Command and Control (CJADC2) program, would be identical to that of President Reagan's failed Strategic Computing Program forty years earlier. As noted in a 1984 article produced by Computer Professionals for Social Responsibility, the principal three focuses of the SCP program were: autonomous vehicles, software pilot assistants, and software-aided "battle management systems." [7]

Then U.S. Senator Biden received widespread press coverage for criticizing Reagan's related Strategic Defense Initiative — aka 'Star Wars' — proposal to take the U.S. president out of the nuclear response loop. [8]

U.S. Senator Paul Tsongas (D-MA) satirically stated : "Perhaps we should run R2-D2 for President in the 1990s. At least he'd be on line all the time." Tsongas then asked if "anyone told the President that he's out of the decision-making process?"

Senator Biden subsequently attempted to inquire into the possibility of an error provoking the Soviets to launch a nuclear attack: "Let's assume the President himself were to make a mistake… ," Biden began, before Cooper interrupted with: "Why? We might have the technology so he couldn't make a mistake."

"OK," stated Biden. "You've convinced me that I don't want you running this program."

Under the Biden administration nearly forty years later, the Pentagon adopted a series of five "ethical principles for artificial intelligence" drafted by its Defense Innovation Board, with a central focus on the rules beyond the incorporation of artificial intelligence into U.S. weapons systems, and the U.S. Intelligence Community soon followed with its own analogue. [9, 10] The Defense Innovation Board was at the time chaired by former Google CEO Eric Schmidt, and its executive director was Joshua Marcuse, who was soon after hired directly into government relations at Google Cloud. [11]

According to an article published by the trade publication Defense One in early 2019, which quoted Marcuse, the Pentagon's development of AI guidelines was inspired by Google's development of internal 'AI Principles' in response to rank-and-file protests about the company's involvement in military drone surveillance. [12] The primary purpose of the Pentagon's ethical commitments would be to help managers at U.S. tech companies assuage concerned staffers, as suggested by both the Defense One article and a Microsoft manager commenting at a public Defense Innovation Board meeting surrounding the principles.

From spy satellites to cloud computing

Google's 2004 acquisition of the satellite imagery company Keyhole Corp. from the U.S. intelligence community's nonprofit venture capital arm In-Q-Tel cemented Eric Schmidt and Google as a successful realization of the legacy of Laurance Rockefeller and Itek. [13, 14] Keyhole's satellite imagery technology became both Google Maps and Google Earth, with the latter's relationship with the U.S. military and intelligence community having been primarily maintained through Thermopylae Sciences & Technology, which has gone dark since its acquisition by the Swedish technology company Hexagon. [15]

WikiLeaks editor Julian Assange's 2014 book 'When Google Met WikiLeaks' was an early warning of Google's transformation into a military contractor, noting that Schmidt's own book from the previous year had argued that: "What Lockheed Martin was to the twentieth century, technology and cyber-security companies will be to the twenty-first." [16, 17] Google helped establish itself as an embodiment of this promise eight years later, through acquiring the cyber-security giant Mandiant. [18]

Google's initial attempt at a federal technology branch lasted only about three years, with its CTO, Rob Painter, having arrived from In-Q-Tel in 2005 following the Keyhole acquisition. [19] As noted by Market Watch in 2008, "While [Google] had $394,760 in [U.S. federal] contracts in 2006, … in 2007 it had only $129,820."

The retail giant Amazon's profitable cloud computing subsidiary, Amazon Web Services (AWS), reinvented the relationship between tech companies and the U.S. intelligence in 2013, with the company receiving a $600 million award directly from the

CIA, known as Commercial Cloud Services (C2S). [20] Officials from the CIA's Directorate of Digital Innovation, which runs both the Agency's cloud computing contracts and the information operations center highlighted by WikiLeaks' Vault 7 disclosures, recently publicly noted that C2S only ended earlier this year. [21] The replacement is the potentially multi-billion dollar Commercial Cloud Enterprise (C2E) contract, which was jointly awarded to five major U.S. tech giants in late 2020: Amazon, Microsoft, Google, Oracle, and IBM. [22]

Google's path to C2E had been rocky. Google employees published an open letter in The New York Times in 2018 which broadly demanded an end to their company's participation in "the business of war." [23] Specifically, the workers were demanding an end to Google's development of custom computer vision software for analyzing city-wide drone surveillance footage collected by Gorgon Stare camera systems flying on General Atomics MQ-9 Reaper drones, a central component of the Pentagon's "Project Maven" experiment, whose unwieldy official name was the Algorithmic Warfare Cross-Functional Team. [24, 25]

The result was Google beginning a shift in late 2018 to providing 'black box' cloud computing support for Maven and handing the lead over to Palantir, resulting in the Maven Smart System, whose deployment in Ukraine was announced in early 2023. [26, 27, 28, 29]

While public subcontracting records revealed that the American AI startup Clarifai had been paid to develop facial recognition for Project Maven, the controversial American facial recognition company Clearview AI separately supported a Ukrainian psychological operation involving contacting the mothers of dead Russian soldiers. [30, 31] And roughly $200 million in Maven-related contracts to ECS Federal were silently deleted from public record after the author's forensic analysis of them in late 2021. [32, 121]

Perhaps as a result of protest fatigue, news of Google's participation in the U.S. Intelligence Community's C2E project was met with little-to-no internal resistance. But worker protests made headlines in late 2021 when Google reversed its previous decision to not participate in the Pentagon's doomed single-vendor Joint Enterprise Defense Initiative (JEDI) cloud contract by announcing an intent to participate in the $9 billion ceiling multi-vendor replacement, Joint Warfighting Cloud Capability (JWCC). [33]

There was also little fanfare surrounding Lockheed Martin's December 2020 announcement that, roughly 38 years after President Kennedy tasked a U-2 to fly over Cuba with an Itek surveillance camera, a U-2 test flight was successfully flown with Google's Kubernetes distributed computing software running onboard. [34] As already understood by Computer Professionals for Social Responsibility in the early 1980s, computer science "has taken over as the critical field underlying modern weapon systems." [7]

A major through line since Itek's role on CORONA has been the Pentagon's [Defense] Advanced Research Project Agency, now universally known as DARPA, which

also aided South Vietnam's counterinsurgency efforts. DARPA's role as the intermediator between the U.S. military and both Silicon Valley and academia has been well-documented, particularly in Sharon Weinberger's 2017 book 'The Imagineers of War' and Yasha Levine's subsequent 'Surveillance Valley'. [35, 36] Beyond DARPA's support for medium-term research and In-Q-Tel's focus on commercialization, the return to so-called 'Great Power' competition with China and Russia in 2014 led to the creation of a new wave of defense commercialization organizations, most notably the Pentagon's Defense Innovation Unit, whose founders recently published the memoir 'Unit X', which is argues a similar 'Third Offset' narrative to that of Anduril chief strategy officer Christian Brose's earlier book, 'The Kill Chain'. [37, 38]

Despite the historical importance of satellite surveillance, the primary financial relationship between U.S. tech giants and the U.S. national security state — so far as public records and reporting have revealed, beyond the exception of Microsoft's $22 billion ceiling Integrated Visual Augmentation System — is through supplying cloud computing and artificial intelligence, especially through the aforementioned C2E contract with the U.S. Intelligence Community, the JWCC contract with the Pentagon, and with the Project Nimbus award from the Israeli government. [39, 40] C2E was initially estimated by the CIA to have a potential ultimate payout of "tens of billions" of dollars, whereas JWCC's public ceiling is $9 billion, and Nimbus — which was split between Amazon and Google — is worth roughly $1.2 billion.

(The author published a detailed study of known government contracts with Google, Microsoft, and Amazon two years ago, concluding that Microsoft was the largest recipient of government funds of the three, with Google in a distant third. [41])

Despite Oracle having been born out of a 1977 project with the CIA under the same name, like the even older company IBM, Oracle's technology is widely viewed by governments as outdated and expensive, leading to Oracle's humiliating loss on Nimbus to Amazon and Google. [42, 43] Arguably, Oracle's core competency of database management has been supplanted by its 9/11-era competitor, data-fusion giant Palantir, which Oracle considered acquiring in 2016. [44]

As revealed by Google training materials for Nimbus uncovered by the author, Nimbus involves the sale of software stacks helping the Israeli military train its own artificial intelligence on top of proprietary datasets. [45] A subsequent investigation by the author uncovered the close relationship between Google and Microsoft and the Lotem Technology Division of the Israeli military's Computer Services Directorate — their rough analogue of the U.S. Defense Information Systems Agency, which runs JWCC. [46] Three months later, the Israeli +972 magazine published similar findings. [47]

After its humble beginnings helping the 18th Airborne Corps find an inflatable tank decoy in a sea of imagery in 2020, Palantir's Maven Smart System was quickly deployed in response to the Hamas attacks of October 7, 2023, providing a shared common operating picture with allies, presumably including the Israel Defense Forces (IDF). [48, 29]

“We were fortunate prior to October 7, that all of our [CENTCOM] components were already actively using MSS and the tools that we had built on it,” stated CENTCOM’s lead for the Maven Smart System, Liam M. Hulin, during a half-day conference hosted by the Center for Security and Emerging Technology (CSET) in late August, where he was introduced as a former commander of SEAL Team Six.

The underlying CSET report for the conference, “Building the Tech Coalition,” stated that the Maven Smart System had enabled an 18th Airborne artillery targeting cell containing “roughly 20 people” to “match the performance of the time-critical targeting cell in Operation Iraqi Freedom” which “benefitted from more than two thousand staff members.” [49, 29]

An anonymous member of the IDF’s Lotem technology unit put the impacts of faster targeting more bluntly in an interview with The Jerusalem Post in February, stating: “the new speed of digital targeting has crossed a threshold where the military can now add new targets in real time faster than it disposes of old ones.” [50] The following month, Columbia epidemiologist Les Roberts noted in TIME Magazine that Israel’s ongoing invasion of Gaza had already killed more than 30,000 people, most of whom were women and children. [51]

Hulin further explained during a half-day CSET conference in late August that the Maven Smart System is “a platform where we fuse and filter data from 179 different live data feeds,” likening the operational team to a “Star Wars bar” based in Tampa. [29] In a clear usage of Palantir’s parlance for its proprietary data management system, Hulin continued that: “MSS is powered by what we call the ‘ontology layer.’ It pulls that data in. It standardizes it so that data can be fused and used together, and then exchanged with cloud and edge systems that we use to work different processes for us.”

“We estimate about 2500 [CENTCOM] people a day, or at least a few times a week, are logging into their [Maven Smart System] accounts and using it,” Hulin added.

Maven has also quietly been integrated into U.S. border surveillance activities through the U.S. Navy and U.S. Coast Guard’s Minotaur Mission System, a sort of data fusion system, or “common operating picture,” for maritime surveillance aircraft such as Lockheed’s P-3 Orion and HC-130J Super Hercules. [122] Developed by the Johns Hopkins University Applied Physics Laboratory, with contracts continuing into at least 2025, the Minotaur software has been promoted in trade publications as “the underlying software backbone for the Pentagon’s Artificial Intelligence (AI)-based Project Maven initiative.” The bold claim is bolstered by a $137,713 subaward to Prescient Edge Corporation from ECS Federal as part of its ongoing “Avalanche” Project Maven award on March 18, 2021, with a subaward description including: “attempt Minotaur and Maven integration efforts on the following hardware solutions: a) Minotaur laptop (to be procured); b) aircraft mission processor; and c) aircraft work station.” [123]

A recently completed $1.5 million contract for Prescient Edge to support the Air and Marine Contracting Division of U.S. Customs and Border Protection's (CBP) usage of the Minotaur Mission System noted in its second modification summary that it involves "test[ing] the Starlink low orbit system on multi-role enforcement aircraft (BLK I)." [124] That is to say, Project Maven is integrated into a system (Minotaur) actively used by CBP for maritime interdiction, with recent tests to use Space X's Starlink communications system for connectivity. [125]

***

Precisely one year before the CSET conference for the "Building the Tech Coalition" Maven report, Microsoft executive Jason Zander reconstructed for a U.S. Air Force audience how the image search technology of Synthetaic, now RAIC Labs, had been used to track China's infamous High Altitude Balloon up until it was shot down by a U.S. Air Force F-22 fighter jet over South Carolina. [52] The task was analogous to the 18th Airborne's 'broad area search' for the inflatable tank decoy, and Zander subsequently demonstrated how RAIC's software could build on top of OpenAI's DALL-E 2 image generation tool to easily find numerous playgrounds in Milwaukee containing chalk drawings of the contiguous U.S.

During a live webinar thirty days later, the head of the CIA's Open Source Enterprise, Randy Nixon, argued that generative artificial intelligence analogues of OpenAI's ChatGPT had revolutionized U.S. surveillance. [53] Nixon stated that, as a consequence of the CIA's adoption of Large Language Models (LLMs) for automatic summarization: "The only thing that holds [us] back on collection is really … having the amount of money to go out and buy everything that's out there."

Thanks to an obscure nonprofit defense contractor named Alethia Lab accidentally publishing myriad training materials and corporate slide decks, much is now publicly known about how the Pentagon and U.S. intelligence agencies plan to incorporate private sector generative artificial intelligence. A slide deck from the natural language processing-focused defense contractor Primer Technologies pitched an "All-Source Workflow" for producing intelligence products, including for targeting, by feeding HUMINT, SIGINT, OSINT, etc. into its proprietary LLM-based platform, Delta. [52]

One of several leaked slide decks from Scale AI described curated and labeled datasets as "'ammo' for 'AI wars'" in a slide whose title asked "Do you have an AI ammo factory?" It was a pitch for Scale's own AI ammo factory, officially known as its Public Sector AI Center in St. Louis, Missouri, which the company advertised as holding 300 data labeling specialists. According to a leaked slide deck, the St. Louis center can produce, on a weekly basis, 35,000 Electro-Optical (EO) imagery annotations, 20,000 for Synthetic Aperture Radar (SAR), and "thousands" for Full Motion Video (FMV).

The power of databases

Nearly thirty minutes into a speech at The University of California, Santa Cruz in March 2006 entitled "The CIA's Secret War," veteran U.S. national security journalist Dana Priest emphasized the power of public records in exposing covert operations, especially corporate records and flight tail-number records. [54] "The amount of information you can get off of a database now is really pretty phenomenal," she stated. Priest then retraced her discovery of CIA rendition flights to a "small story" published in late October of 2001 by News of Islamabad which discussed the Yemeni microbiologist Jamil Mohammed "being whisked away" in a Gulfstream V aircraft with tail number N379P. [55]

The "conservative news forum" FreeRepublic.com posted that the tail number belonged to Premier Executive Transport Services of Dedham, Massachusetts, alongside a soon-to-be-confirmed suspicion that it was a front company in the vein of the CIA's infamous previous front company, Air America. The confirmation that Premier Executive Transport Services was a front came from public corporate records providing its nominal list of officers, who were found to be fictitious.

Eighteen years later, flight logs of even classified flights are widely scrutinized through Automatic Dependent Surveillance-Broadcast (ADS-B) databases, and corporate records are largely centralized and made freely available through the website OpenCorporates.com. (Strange bedfellows in the human rights community have resulted from one of the most prominent free ADS-B websites, ADS-B Exchange, being closely partnered with the de facto think-tank arm of Palantir, The Center for Advanced Defense Studies, better known as C4ADS, whose former director Jerrold M. Post was the founder of the CIA's Center for the Analysis of Personality and Political Behavior. [56, 57])

The combination of such datasets with daily streams of public contracting summaries from governments around the world, along with an ever-growing body of public interest leaks, has produced an information goldmine containing revelations often exceeding those possible from conversations with high-level inside sources. This year alone, hundreds of gigabytes of apparent Israeli Ministry of Justice and Ministry of Defense emails were published in response to Israel's ongoing invasion of Gaza, following a similarly historic leak of top secret Pentagon assessments of not only the ongoing Russian invasion of Ukraine, but also global signals intelligence on even allied governments collected through the Foreign Intelligence Surveillance Act (FISA).

The baseline for low-budget research has become keyword lookups and alerts through search engines, particularly Google's namesake product and walled garden analogues, such as on X (formerly Twitter), LinkedIn, Telegram, or Facebook. While reporters and researchers may manually set up accounts on each platform through their own email addresses, intelligence agencies tend to use an intermediary company to provide both anonymity and a unified, multi-lingual interface across tens to

hundreds of data sources. At the moment, the most popular companies in this space are Babel Street, Flashpoint, and the Venrock-investee Dataminr.

A typical reporter might also have alerts set up — for example, through Google Alerts — to email them any time one of tens of keywords relating to the companies and people in their beat appears in a news article or press release. Whereas the U.S. State and Defense departments often do the same through tools such as Babel and Dataminr, across a broader range of data sources.

Classified U.S. activities provide useful test cases for the application of data fusion in investigations: with the exceptions of leaks and investigative journalism, no single data source tends to provide a complete picture. Answering even simple questions, such as who has been publicly reported to be a CIA station chief — along with where and over what rough time period — requires scouring thousands of sources. And second-order questions, such as which companies in private industry said station chiefs subsequently worked for, and roughly what those companies have done for various government agencies, generally transition research out of social media and into studying public procurement records, corporate websites, and LinkedIn. For historic information, there is no substitute for reading books authored by investigative journalists.

(Tech Inquiry currently contains 490 reputable citations for specific reported CIA station chief positions, including the Lebanese newspaper Al Akhbar recently naming Sherry Baker as the Agency's Beirut station chief. [58])

Network maps

For decades, nearly every police and intelligence agency in the world has made use of investigatory software to conduct what might be referred to as network mapping — essentially keeping track of the citations as to how various individuals, companies, and government agencies relate. The rough idea is to computerize the police investigation board trope of red strings connecting various photos pinned to a wall. (Despite the centrality of network analysis to governmental investigations, grassroots analogues are culturally relegated to the realm of conspiracy, as epitomized by the 'Pepe Silvia' meme from the television series *It's Always Sunny in Philadelphia*.)

The British company i2 was the first major player in this space, though the American data fusion company Palantir became the largest, reportedly partly through its current chief technology officer Shyam Sankar reverse-engineering i2's technology. According to a keynote speech by i2 founder Michael Hunter attended by the author in mid-2022, the ability to reverse-engineer i2 was aided by the software's modular design, which existed to allow the company's largest power user — the CIA — to enact its own customizations without the help of i2's staff. "We had two really big customers: the CIA and the FBI."

Hunter further claimed that the U.S. origin of the pre-computerized police network maps was the Los Angeles Police Department's adaptation of the graph-based Program Evaluation and Review Technique (PERT) used for the development of Polaris missiles to the high-profile investigation of the assassination of Robert F. Kennedy. [59] The company swung its first major customer, the U.S. Department of Defense, through the ongoing Los Angeles trial of former football star O.J. Simpson: "Being a clever devil, I did charts based upon O.J. Simpson … thereupon followed an hour-long argument between different members of the audience upon whether he was guilty or not," stated Hunter.[1]

Beyond its initial post-9/11 mass adoption for counter-terrorism, network mapping further boomed in the last decade as a result of geopolitical tensions between the U.S. and China, with entire companies now existing to shed light on how the U.S. economy intersects with that of China and its Xinjiang Uyghur Autonomous Region. Many such companies, including Sayari and Accrete, are also covertly or overtly used for U.S. information operations. [52] In the case of Sayari, which received a public investment from In-Q-Tel, the networks of sanctioned entities are generated as targets for offensive U.S. computer network operations.

But the U.S. Government does not fund equivalent research exposing itself or its allies, such as the obvious parallel to Xinjiang of Israel's occupation of Palestine. Only a few scrappy organizations attempt to fill in these gaps, such as the Israeli NGO Who Profits from the Occupation and the U.S.-based 'LittleSis' project run by the Public Accountability Initiative. The author's work with Tech Inquiry broadly exists within this vein.

The basic idea behind Tech Inquiry is to perform open source network mapping on top of myriad public datasets and media — with citations for each connection, along with annotations of their weight — as a low-budget form of data fusion. After more than five years of work, the hand-coded annotations comprise more than a million lines of JavaScript Object Notation (JSON).

For example, our current list of associations with U.S. Embassy Berlin includes a partial list of former CIA station chiefs drawing from an article authored by the late military historian Matthew Aid, books authored directly by former station chiefs Floyd L. Paseman and Milton A. Bearden, declassified documents, and requisite New York Times and Washington Post reporting. [60-65] But ambassadorship tenures can be

1 Hunter also explained in his keynote that the name "i2" was an evolution of the name "information-to-image," which would have produced the name I2I, which he felt was too close to the saying "eye for an eye." But, after dropping the second 'I' from the name, the name kept being confused with the number 12, and so the company stylized the first letter in its name as a lowercase 'i'.

drawn directly from a (now-defunded) public U.S. State Department database and then used to annotate the cache of embassy cables released by WikiLeaks as part of Cablegate. [66] Similarly, daily feeds of U.S. federal contracts and grants affiliated with the embassy can be drawn from fpds.gov and USASpending.gov.

The CIA's Center for Cyber Intelligence, which was previously known as the Information Operations Center and was led circa 2014 by In-Q-Tel co-founder Susan M. Gordon, was indicated by the WikiLeaks 'Vault 7' disclosures on CIA hacking to have operated out of the U.S. Consulate General in Frankfurt.[2] [67] Reporting from The New York Times in 2009 earlier revealed that the Frankfurt consulate served as the CIA's main European supply base and that its chief circa 2003, Kyle "Dusty" Foggo, had led the construction of three secretive European detention centers: a jail in a renovated building on a busy street in Bucharest, a steel-beam structure in Morocco codenamed 'Bombay' which was reportedly never used, and a third outside of Warsaw codenamed 'Quartz'. [68, 69]

One can also reconstruct a procurement feed for U.S. Army Garrison Wiesbaden, which not only serves as the headquarters for U.S. Army Europe, but was the launch site of the first CIA U-2 surveillance flight over the Soviet Union in 1956. The U.S. Army's 66th Military Intelligence Brigade moved its headquarters to Wiesbaden Army Airfield in September 2008 and has been affiliated with the operation of the base's significant signals intelligence capabilities, which were based roughly thirty minutes' drive southeast at the infamous 'Dagger Complex' until moving to the Gray Information Processing Center in 2016. [70, 71, 72]

Former commanders of the 66th MIB have included John G. Lackey III, who later led Joint Special Operations Command circa 1989, and Devon Blake, who became a senior director at the covert human and signals intelligence collection firm Premise Data in 2019, with the company receiving a more than $1 million subaward from JSOC in mid-2022 under General Dynamics Information Technology. [73] The next year, Ms. Blake transitioned to chief growth officer of NexTech Solutions, a reseller of surveillance software such as Clearview AI which is closely partnered with U.S. Special Operations Command.

But the interaction between two entities might be significantly easier to investigate in one direction than in the other. When U.S. 501(c)(3) nonprofits disclose their five-largest independent contractors each year in their public Form 990 filings, the

2 The CIA had reportedly ridiculed the State Department over WikiLeaks revealing much of its cable traffic beginning in 2010, and Yahoo News reported three years ago that, in the months following the 'Vault 7' disclosures, then-CIA director Michael Pompeo considered kidnapping and assassinating WikiLeaks editor-in-chief Julian Assange from his then sanctuary in Ecuador's London embassy.

names can be obscured in a manner which prevents keyword searches. This was the case for In-Q-Tel's 2019 filing, which cryptically listed its $1.6 million check to encrypted messaging application Wickr as going to "W I", with the only determinative information being the listed address. [74] Co-chaired by the former CEO of In-Q-Tel, Gilman Louie, Wickr was acquired by online retail giant Amazon a few months before the author made In-Q-Tel's funding public.[3] [75, 76]

Such investments into secure messaging platforms, as well as the nearly $3 million granted to the encrypted messaging application Signal through the Open Technology Fund, which was then controlled by the CIA spin-out U.S. Agency for Global Media, help underscore the centrality of information operations to modern conflict. [77] Just as national security journalists have gravitated towards Signal for sensitive conversations, so have many U.S. soldiers and spies. While understandably taboo to mention, it is an open secret — in fact, documented by leaked diplomatic cables — that human rights activists and moonlighting journalists are major information sources for U.S. embassies around the world. [78-81]

Brief example: the Airman Teixeira leaks

Before being outed by the former director of research and training of Bellingcat through an article in The New York Times and then arrested by the FBI, the 21-year-old Airman Jack Teixeira leaked dozens of secret and top secret intelligence reports relating to the ongoing Russian invasion of Ukraine. Sixty-four pages of the leaks have been published by the transparency nonprofit Distribute Denial of Secrets (DDoSecrets), twenty of which were previously published by Newsweek journalist William M. Arkin in mid-April 2023. [82, 83]

(Mr. Arkin was also the editor of a recent article from journalist Ken Klippenstein which published two leaked U.S. intelligence assessments similar to those from the Teixeira leaks, in which the National Geospatial-Intelligence Agency correctly assessed that Israel was likely about to strike Iran. [84])

3 Maintaining such a database of citations for entity relationships not only helps overcome one-way information barriers, but also allows for relationships with subsidiaries to be automatically inferred for the parent. As an added benefit to constructing such hierarchy-aware graphs, related entity lists can be automatically generated by querying the nearest neighbors of representations generated through appropriate low-rank approximations of the association matrix. Rather than assuming a fixed variance for all interactions, as implied by the uniform cost function of a Singular Value Decomposition, using a significantly higher variance for unobserved entries is widely understood to produce a higher quality low-rank embedding.

One of the more interesting images from the Teixeira leak, numbered 27 of 64 by DDoSecrets, was produced on March 1, 2023 by the operational arm of the U.S. Joint Chiefs of Staff. Beyond asserting that ninety-seven total special operations forces (SOF) personnel were deployed by NATO countries at the time — primarily from the United Kingdom, Latvia, and France — the document also asserts that, within the next 24 hours, twenty-one units of the secretive "Phoenix Ghost" drones produced by AEVEX Aerospace would be transferred to Ramstein Air Base in Germany, the headquarters of U.S. Air Forces in Europe and Africa. [85] The German, French, and Dutch governments were also described as providing training and advising to Ukrainian Armed Forces through an operation referred to as "Phoenix Strike," whose name suggests the involvement of Phoenix Ghost drones.

The same document from the Joint Chiefs of Staff also described NATO "Airborne Sensitive Reconnaissance Ops" out of Romania and Poland using MQ-9 Reapers, a U-2 Dragon Lady, Northrop Grumman RQ-4 Global Hawks, Bombardier Challenge 650s, and British-owned "Rivet Joint" RC-135 V/W aircraft. Related NATO surveillance flights in the Black Sea near Crimea were the subject of document 13 of 64, which was reported by The Washington Post in early April of 2023 due to the mention of a "near-shoot down" of a British Rivet Joint. [86]

After creating a full-text search interface to manual transcriptions of the text from each of the 64 leaked Teixeira documents, we manually tag the document identifiers in which each relevant entity appears (e.g., document 27 for the Phoenix Ghost, U.S. Embassies Berlin and Riga, Latvian Special Operations Command, and Ramstein Air Base).

The second-order task is then to cite associations between entities that are revealed in the documents, such as the planned transfer of twenty-one Phoenix Ghost kamikaze drones to Ramstein Air Base.

The German-manufactured Leopard 2 main battle tanks provide a more detailed example of revealed associations. Across documents 29, 30, and 53, contributions of Leopard 2 tanks to Ukraine are detailed as originating from the governments of Germany (DEU), Poland (POL), Norway (NOR), Canada (CAN), Finland (FIN), Greece (GRE), Portugal (POR), and Spain (ESP). The bottom-right corner of document 29 also describes its source as U.S. Army Garrison Wiesbaden, the headquarters of U.S. Army Europe.

We use a slightly higher weight for the stated German contribution of fourteen Leopard 2A6 tanks than the six Leopard 2A4 tanks claimed to be contributed by Spain. This not only signals that the former relationship should appear first in the association list for the Leopard 2 profile page, it also yields a higher interaction score between the Leopard 2 and the German Army than with the Spanish Army and helps inform Tech Inquiry's nearest neighbor lists.

While there is an intrinsic value to the clerical work of building out Tech Inquiry's profile pages and searchable document databases, the primary motivation is to serve

as a foundation for investigations into Western governments and the associated weapons and surveillance industries.

Artificial Intelligence and information warfare with China

As revealed by the author earlier this year, U.S. Army Special Operations Command's Capabilities Exercise (CAPEX) for 2023 involved 4th Psychological Operations Group (Airborne) — also known as 'Dark Horse' — simulating the exploitation of the psychological vulnerabilities of numerous mock anti-communist Taipei-based personas, including a Buddhist monk, an emergency surgeon, and the publisher of the Taipei Times. [87] The primary tool for the information warfare exercise was the Pulse platform of the Virginia-based contractor Two Six Technologies, which in May 2022 hired the first female head of the CIA's Directorate of Operations, Elizabeth Kimber, as its Vice President for Intelligence Community Strategy. [88]

And as reported by Reuters in March, a small team of CIA operatives began creating fake online accounts under President Trump's direction in 2019 in order to "spread negative narratives about Xi Jinping's government while leaking disparaging intelligence to overseas news outlets." The narrative attacks, which at least historically would have come from the Political Action Group within the Special Activities Center, were said to focus on discrediting China's 'Belt and Road' infrastructure initiative and promoting allegations that Chinese Communist Party members were hiding their wealth overseas. [89, 90] Echoing motifs from Dark Horse's 'Ghosts in the Machine' recruitment video, a former CIA official told Reuters that "We wanted [Chinese leaders] chasing ghosts." [91]

Through a series of ongoing 'counter-disinformation' contracts beginning in mid-2020 which involve both Joint Special Operations Command and various geographically focused components of 1st Special Forces Command, including Dark Horse itself and the bulk of the numbered Special Forces groups, Two Six's Pulse platform has become perhaps the preeminent modern information warfare tool for U.S. Special Operations Forces. [92] Born out of a classified DARPA crowdsourcing program in Afghanistan known as 'More Eyes' which was operational circa 2011, former DARPA program manager Ryan Paterson commercialized modernized analogues of Cold War-style information operations, such as radio programs and leaflets, in the form of text message blasts and social media campaigns. [93, 35]

The 'Pulse platform' became the flagship product of Paterson's company Information Science Technology Research — which was abbreviated as IST Research — and evolved into the "tactical information warfare" toolkit sold to U.S. Special Operations Forces beginning in mid-2020.

Within a year of IST's relationship with U.S. Special Forces kicking off, the company was acquired by private equity firm The Carlyle Group and merged with cybersecurity firm Two Six Labs to form Two Six Technologies. [94] By mid-2022, Paterson left Two Six to become president of Unplugged Systems, which claims to provide a state-of-the-art secure phone but is best known for its backing from Erik Prince, the founder of infamous private military contractor Blackwater.

Also recently revealed by the author, the Defense Intelligence Agency's Human Intelligence Training Joint Center of Excellence (HT-JCOE), which is co-located with the U.S. Army's Intelligence Center of Excellence (USAIoC) in Fort Huachuca, has been quietly setting up contracts to train members of the U.S. military on how to evade "the capability a modern law enforcement or adversary counterintelligence service would have at their disposal." [95]

One HT-JCOE solicitation, for a "Camera Laboratory", sought to enable "training and exercise against security cameras and associated Artificial Intelligence capabilities of Facial Recognition and Person Tracking." [96] One component of the solicitation implied the usage of Chinese facial recognition cameras as part of the training by stating: "The Gov't [Government] cannot stress enough that the purchase of adversary technology must be done in a manner that is not attributable to the USG [U.S. Government] and where USG end user is not known." When reached for comment, Fort Huachuca public affairs claimed that the Camera Laboratory contract was cancelled and that the statement regarding the covert purchase of "adversary technology" was a mistake.

A separate, $1.9 million HT-JCOE contract was awarded to Quiet Professionals, a contractor led by two former JSOC operators, former Delta Force sergeant major Andy Wilson and former Task Force Orange first sergeant Leo Kryszewski. [97-99] In addition to noting that Quiet Professionals' Cerebra Gray platform supports remotely wiping the hard drives and manipulating the sensors of operatives' cellphones, the contract solicitation also discussed the usage of cellphone "hidden volume[s]". Made infamous by the kingpin-turned-government-asset Paul Le Roux through his E4M encryption software and the derivative TrueCrypt package, hidden volumes encrypt data such that a cover password can be provided which decrypts into a staged environment which plausibly conceals sensitive data requiring a separate password. [100, 101]

As reported by the author last year, Quiet Professionals subsidiary Echo Analytics Group hosted the first 'hunt' of the counter-sex work nonprofit Skull Games in its Tampa office, just 13 miles away from the headquarters of SOCOM. [102] And Skull Games was itself founded to leverage the open-source intelligence capabilities of former Delta Force operator Jeff Tiegs.

The Israeli government's U.S. propaganda campaign

An August 2007 cable attributed to George W. Bush's then Ambassador to Israel, Richard H. Jones, noted that the director of the Shurat HaDin Israel Law Center, Nitsana Darshan-Leitner, had admitted to her organization originally being a lawfare tool of Israel's foreign intelligence service, generally known as the Mossad. The revelation undercut Shurat HaDin's self-branding as an Israeli analogue of the U.S. Southern Poverty Law Center, which used legal action to take down the Ku Klux Klan in the 1980s.[4] [103]

Leitner publicly copped to Shurat HaDin's close collaboration with Israeli intelligence a decade after the cable through her book 'Harpoon', which took its name from the covert financial warfare unit founded by former Mossad director and honorary Black Cube president Meir Dagan.[5] [104] Leitner's book also attributed the rise of current CIA deputy director David S. Cohen from his previous role as Under Secretary of Terrorism and Financial Intelligence to techniques gleaned from the Harpoon program.

Further details on the relationship between Shurat HaDin and the Israeli government emerged from a high-profile leak of roughly 245 gigabytes of emails from the Israeli Ministry of Justice following the country's invasion of Gaza as part of Operation Swords of Iron. [105] Amidst the lawfare organization's public campaigns against the International Committee of the Red Cross, human rights lawyer Amal Clooney, and the U.S. organization Students for Justice in Palestine, the emails appear to show high-level Ministry of Justice officials mocking Shurat HaDin and its unofficial spin-out organization International Legal Forum for overzealous legal arguments. [106-108]

In late June, the author revealed the rebirth of Israel's 'Voices of Israel' propaganda program, with a new focus on winning the narrative war surrounding Opera-

4 The Southern Poverty Law Center has itself engaged in controversial activities in the last decade. Beyond paying the defense contractor Culmen International roughly $1.5 million for a "Big Data Platform" between 2015 and 2017 that included commercial cellphone location-tracking data, SPLC laid off more than 60 employees this year who were attempting to unionize despite sitting on more than $700 million in assets.

5 The legendary Nazi-hunter Simon Wiesenthal was posthumously revealed to have been paid by the Mossad in 2010. In the language of veteran Israeli intelligence journalist Yossi Melman in his 2012 book 'Spies Against Armageddon', Wiesenthal was somewhere between an agent and a *sayan*, the term-of-art for a member of the Jewish diaspora who aids Mossad operations, often through a don't-ask-don't-tell policy.

tions Swords of Iron, using the combination of a searchable mirror of Israeli government contracting records and by transcribing numerous public Knesset hearings in partnership with fellow journalist Lee Fang. [109] Roughly two months later, Tech Inquiry's newly created searchable mirror of the leaked Ministry of Justice emails was used to expose Israeli government strategy documents for avoiding the U.S. Foreign Agents Registration Act, with former Democratic National Committee chair Joseph E. Sandler and his partner Joshua I. Rosenstein as the legal sherpas.[6] [110]

From roughly 2014 to 2015, Israel's Ministry of Strategic Affairs (MSA) was beginning to take on the Israeli government's mandate to oppose the Boycott, Divestment and Sanctions (BDS) movement and was temporarily combined with the Ministry of Intelligence under the direction of former Mossad deputy director Ram Ben-Barak. A freedom of information request published by The Times of Israel in 2019 further showed that then-Mossad chief Yossi Cohen had met the previous year with the MSA head Gilad Erdan, and recent reporting from The Guardian and +972 Magazine revealed that, the same year, Cohen was secretly pressuring International Criminal Court prosecutor Fatou Bensouda to drop her investigation into potential Israeli war crimes. [111, 112]

Despite their well-documented, at least historical, control by the Mossad, Shurat HaDin remains a significant partner of numerous tightly-knit anti-BDS advocacy and lawfare organizations generally clustered around influential right-wing donor Adam Milstein, a convicted felon who previously chaired the Israeli-American Council, an influential pro-Israeli lobbying organization set up under the direction of Israel's Los Angeles consul general Ehud Danoch in 2007. [113]

The marketing firm STOIC, despite its relatively secondary role, received widespread attention earlier this year for attempting to covertly influence the U.S. Congress and to drive a wedge between Black Americans and Palestinians. As noted by Haaretz, STOIC was a competitor to the Voices of Israel joint venture, which was originally set up by the MSA but is now run by the Ministry of Diaspora Affairs.[7] An earlier competitor to Voices of Israel, Psy-Group, received even more attention due to its partnership with the infamous data analytics firm Cambridge Analytica and has recently been reborn as Percepto International.

6 Both articles were published in collaboration with The Guardian as headline news, though only our independently published copy linked to the leaked documents.

7 Voices of Israel was previously known as Concert, and, before that, as Kela Shlomo. Its research and information subsidiary, Keshet David, has also been known as Israel Cyber Shield and Innovative Collaboration Strategies.

The fundamental mechanism of Voices of Israel is to serve as an intermediary between the Israeli government and nonprofits in the U.S. and other strategic countries, such as South Africa and the United Kingdom. Much of the functioning of Voices was exposed through an undercover video investigation by Qatar's Al Jazeera circa 2017, though the U.S. footage was only published in 2018 due to intense lobbying pressure from the far-right, Trump-aligned Zionist Organization of America, which threatened to force Al Jazeera to register as a foreign agent unless it censored the investigation. The footage only appeared online through a leak in late 2018, and the previously mentioned recent investigation by the author ironically revealed Israel's own scheme for avoiding Voices' foreign agent registration. [114]

Perhaps the most incendiary segments of the hours of published footage are from the Israel on Campus Coalition (ICC), a sort of fusion cell for opposition research and smear campaigns against U.S. campus BDS movements. As exposed in a recent investigation from the author based upon a lead from Al Jazeera's undercover investigation, ICC's self-proclaimed "psychological warfare" against U.S. students has been secretly fueled by surveillance software created by the Israeli branch of the Australian advertising technology firm Blend AI. [115] A combination of ICC's tax filings and Israeli corporate registries reveal that ICC has paid Blend AI at least $1.9 million, which is more than the company's last fundraising round. [116]

Corporate records and tax filings similarly demonstrate that ICC paid the Rutgers-affiliated Network Contagion Research Institute (NCRI) $335,000 in 2021 and that NCRI founder Joel Finkelstein is a director of a secretive Israeli anti-BDS organization named Hetz alongside the founder of Voices of Israel, Brig. Gen. (res.) Sima Vaknin-Gill, who was also previously the Israeli military's chief censor. Another previously unreported board member of Hetz is prominent U.S. venture capitalist David M. Magerman, and a public talk given by Hetz CEO Eran Teboul on May 13, 2022 to the Norwegian nonprofit Med Israel for fred (MIFF) noted that his organization has privately fundraised for NCRI.[117]

The 'north star' for Tech Inquiry

When building a knowledge base of entities and their relationships, perhaps the central question is of scope. A common trap for activists is to focus on a list of 'bad' organizations, such as spyware companies, and to avoid documenting relationships with 'good' organizations, such as the billionaires and nonprofits friendly to their political project.

But intelligence operations often purposefully use nonprofits, humanitarian organizations, and journalism as cover. Beyond SEAL Team Six posing as the Red Cross to snatch the war criminal Milan Kovačević in Bosnia on July 10, 1997, the longstanding intelligence partnership between the CIA and the Mossad was born from the Shin Bet recruiting the Polish journalist Victor Grayevsky to steal a copy of Nikita

Khrushchev's speech denouncing former Soviet leader Joseph Stalin. [118, 119] Despite the taboo surrounding their discussion, journalistic, humanitarian, and religious cover are staples of intelligence agencies and special operations forces around the globe, including the U.S. and its allies.

Not to mention that the Ford Foundation and Rockefeller Brothers Fund, both of which played central roles in U.S. surveillance and covert influence during the Cold War, continue to be major funders of progressive movements in the United States.

The unreachable — but still worth pursuing — goal of Tech Inquiry is to manually document all significant financial relationships involving influential and newsworthy organizations, particularly as they relate to weapons and information operations (of which surveillance forms a subset). This includes: every billionaire, every significant governmental organization, every U.S. military base, every U.S. embassy, every CIA chief of station, every U.S. Ambassador, and every influential company and nonprofit.

We would also like to expose a single searchable interface to every government's public procurement and lobbying feeds, as well as every national security-oriented public interest leaked dataset.

The basic methodology with respect to governments is to begin with entities for each country and to gradually refine down to the significant departments or ministries and, where data is available, down to obscure units such as Task Force Orange. In the case of European procurement data, the resolution essentially ends at the sub-ministerial level, such as with the Hungarian Police, which are a component of the Hungarian Ministry of Interior. (Due to a complete rewrite of European Union procurement records being slowly phased in over the last year, support for the format was only recently added into Tech Inquiry, significantly stunting European analysis.)

Months of effort were expended throughout this project to extend Tech Inquiry's existing contracting feeds for U.S. embassies to all (overt) U.S. military bases. [126] While useful as a research tool, said feeds have yet to lead the author to a significant story, as even the Fort Huachuca findings for covert U.S. activities in China were found through keyword searches over a mirror of the U.S. contracting opportunities published on SAM.gov. However, significant stories have resulted from mirroring Israeli procurement and the massive leak of Israeli Ministry of Justice emails and, indeed, the author recently integrated a slightly smaller leak of IDF emails and has manually transcribed the Airman Teixeira leaks.

A significant number of stories are also broken from the major international arms sales announcements of the U.S. Defense Security Cooperation Agency, though they are more interesting to the author as long-term documentation of significant weapons sales. For example, the approval of a contract to sell the Government of Taiwan $300 million of Anduril's ALTIUS 600M-V loitering munitions ("suicide drones") was announced on June 18. [120]

As might be obvious, simply keeping Tech Inquiry's datasets up-to-date is a full-time job in itself. As is entity curation and reverse-engineering government agency feeds. And manually annotating the ever-expanding interactions between these tens

of thousands of entities. And, at least semi-regularly, producing quality journalism on top of these data sources.

Tech Inquiry began with a singular focus on fusing proactively published government datasets with analysis of journalism but has come to appreciate the impact possible from incorporating historic leaks, ranging from Cablegate to Israeli government emails and Airman Teixeira's so-called 'Discord leaks'. In the case of documents with sufficiently sensitive personally identifiable information, we allow all users to discover the documents through a textual index, but access to the underlying documents is restricted to vetted journalists.

Such an approach is both journalistically the preferred course of action when dealing with large, possibly as-yet-unauthenticated datasets containing sensitive info on individuals and, as a U.S. citizen, likely significantly legally safer with little downside.

After adding an authentication guard for sensitive documents, the author began extending Tech Inquiry such that users can easily attach their own tags to entities and mirrored documents, such as *#project-maven or #mq-9-reaper*, and then retrieve all entities and documents with particular tags.

Because all of Tech Inquiry's data and software is public / open-source, ideally another organization could simply spin up its own recreation of the project with a week or two of work and about a $100 budget. This is especially relevant given recent legal aggression from surveillance industry CEOs against both Tech Inquiry and the author personally.

There are few journalists doing serious national security investigations; even fewer have the capacity to analyze massive leaked datasets relating to Western governments. Providing a simple searchable interface can at least remove one of the hurdles.

Loudly declaring strong opinions on geopolitically sensitive topics is certainly much easier and cheaper than conducting investigations. But the U.S. Government didn't consider assassinating Julian Assange because of his opinions. WikiLeaks became an enemy because it exposed damning information about the U.S. Government using primary sources in an often clinical manner.

Even without counting Tech Inquiry's curation of Western public records and leaked datasets, it has likely already become the largest public repository of citations for CIA station chief tenures. That an underfunded project developed by a single person can compete at such a level demonstrates how low the bar is for open source intelligence analysis of Western governments; far more funding is dedicated to monitoring U.S. adversaries. The author hopes to make a humble contribution towards correcting that imbalance.

References

[1] Lewis, Jonathan E. *Spy Capitalism*. Cumberland: Yale University Press, 2002. https://yalebooks.yale.edu/book/9780300209754/spy-capitalism/

[2] “Jonathan E. Lewis,” *Fiera Capital*. Accessed October 17, 2024, https://uk.fieracapital.com/en/team/jonathan-e-lewis/

[3] Guyer, Jonathan. “Inside the chaos at Washington’s most connected military tech startup.” *Vox*. December 14, 2022. https://www.vox.com/recode/23507236/inside-disruption-rebellion-defense-washington-connected-military-tech-startup

[4] Poulson, Jack. "U.S. tech industry gathers to organize against China, while defending its obscured role in ongoing slaughter of Gazans.” *All-Source Intelligence*. May 10, 2024. https://open.substack.com/pub/jackpoulson/p/scsp-ai-expo-2024

[5] Seelinger, Matthew. "The M28/M29 Davy Crockett Nuclear Weapon System.” *The Army Historical Foundation*. Accessed October 17, 2024. https://armyhistory.org/the-m28m29-davy-crockett-nuclear-weapon-system/

[6] Srubas, Paul. "The horrifying purpose of Special Atomic Demolition Munition units: ‘We all knew it was a one-way mission, a suicide mission’.” *Green Bay (Wis.) Press-Gazette*. January 14, 2019. https://www.armytimes.com/news/your-army/2019/01/14/the-horrifying-purpose-of-special-atomic-demolition-munition-units-we-all-knew-it-was-a-one-way-mission-a-suicide-mission/

[7] Ornstein, Severo M., Smith, Brian C., and Lucy A. Suchman. “Strategic Computing.” *Bulletin of the Atomic Scientists* 40, no. 10 (1984): 11-15, https://www.tandfonline.com/doi/abs/10.1080/00963402.1984.11459292

[8] Boffey, Philip M. “‘Star Wars' and Mankind: Unforeseeable Directions.” *The New York Times*. March 8, 1985. https://www.nytimes.com/1985/03/08/us/star-wars-and-mankind-unforeseeable-directions.html

[9] "DOD Adopts Ethical Principles for Artificial Intelligence,” *U.S. Department of Defense*. February 24, 2020. https://www.defense.gov/News/Releases/release/article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/

[10] "Intelligence Community Releases Artificial Intelligence Principles and Framework,” *Office of the Director of National Intelligence*. July 23, 2020. https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2020/3468-intelligence-community-releases-artificial-intelligence-principles-and-framework

[11] Tucker, Patrick. "Defense Innovation Board Director Moves to Google.” *Defense One*. May 1, 2020. https://www.defenseone.com/technology/2020/05/defense-innovation-board-director-moves-google/165086/

[12] Tucker, Patrick. "Pentagon Seeks a List of Ethical Principles for Using AI in War.” *Defense One*. January 4, 2019. https://www.defenseone.com/technology/2019/01/pentagon-seeks-list-ethical-principles-using-ai-war/153940/

[13] "Google Acquires Keyhole,” *The Wall Street Journal*. October 27, 2004. https://www.wsj.com/articles/SB109888284313557107

[14] "In Q Tel Inc,” *ProPublica*. Accessed October 17, 2024. https://projects.propublica.org/nonprofits/organizations/522149962

[15] “Hexagon advances its 5D visualisation portfolio with the acquisition of Thermopylae Sciences and Technology,” Thermopylae Sciences & Technology. February 25, 2019. http://web.archive.org/web/20231001155703/https://www.t-sciences.com/news/hexagon-advances-its-5d-visualisation-portfolio-with-the-acquisition-of-thermopylae-sciences-and-technology

[16] Assange, Julian. *When Google Met WikiLeaks*. New York: OR Books, 2014. https://www.orbooks.com/catalog/when-google-met-wikileaks/

[17] Schmidt, Eric and Jared Cohen. *The New Digital Age*. New York: Penguin Random House, 2013. https://www.penguinrandomhouse.com/books/214925/the-new-digital-age-by-eric-schmidt-and-jared-cohen/

[18] Kurian, Thomas. "Google + Mandiant: Transforming Security Operations and Incident Response." *Google Cloud*. September 12, 2022. https://cloud.google.com/blog/products/identity-security/google-completes-acquisition-of-mandiant

[19] Letzing, John. "Google, seeking to diversify, looks to Uncle Sam." *Market Watch*. March 13, 2008. https://web.archive.org/web/20210227005758/https://www.marketwatch.com/story/google-seeking-to-diversify-looks-to-government-contracts

[20] Konkel, Frank. "The Details About the CIA's Deal With Amazon." *The Atlantic*. July 17, 2014. https://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/

[21] "Coffee & Conversation Insights from CIA on Cloud and Data," *Intelligence & National Security Alliance*. September 4, 2024. https://www.youtube.com/watch?v=J2sZKGOH028

[22] Mitchell, Billy. "CIA quietly awards C2E cloud contract possibly worth billions." *FedScoop*. https://fedscoop.com/cia-quietly-awards-billion-dollar-c2e-cloud-contract/

[23] Shane, Scott and Daisuke Wakabayashi. "'The Business of War': Google Employees Protest Work for the Pentagon." *The New York Times*. April 4, 2018. https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html

[24] Crichton, Danny. "Lt. Gen. Jack Shanahan on Building Trust Between Silicon Valley and the Pentagon." *Lux Capital*. August 30, 2023. https://www.luxcapital.com/content/lt-gen-jack-shanahan-on-rebuilding-trust-between-silicon-valley-and-the-pentagon

[25] Michel, Arthur Holland. *Eyes in the Sky*. New York: Harper Academic. 2019. https://www.harperacademic.com/book/9780544972001/eyes-in-the-sky/

[26] Fang, Lee. "Google Hedges on Promise to End Controversial Involvement in Military Drone Contract." *The Intercept*. March 1, 2019. https://theintercept.com/2019/03/01/google-project-maven-contract/

[27] Poulson, Jack. "Pentagon certified Palantir as only supplier for artificial intelligence targeting tool known as 'Maven Smart System'." *All-Source Intelligence*. May 13, 2023. https://open.substack.com/pub/jackpoulson/p/pentagon-certified-palantir-as-only

[28] Poulson, Jack. "Where Drone Warfare Intersects with Ukraine and U.S. Information Operations." *Tech Inquiry*. March 13, 2023. https://techinquiry.org/?article=insa-maven-ukraine

[29] Probasco, Emelia et al. "Building the Tech Coalition." *Center for Security and Emerging Technology*. August 30, 2024. https://youtube.com/watch?v=bQ1Vxtm4tPA&t=212s

[30] Poulson, Jack. "Easy as PAI (Publicly Available Information)." *Tech Inquiry*. September 10, 2021. https://techinquiry.org/EasyAsPAI/resources/EasyAsPAI.pdf

[31] Harwell, Drew. "Ukraine is scanning faces of dead Russians, then contacting the mothers." *The Washington Post*. April 15, 2022. https://www.washingtonpost.com/technology/2022/04/15/ukraine-facial-recognition-warfare/

[32] Poulson, Jack. "$142 million AI drone warfare contract from 'Project Maven' was silently erased from public record." All-Source Intelligence. October 26, 2024. https://open.substack.com/pub/jackpoulson/p/142-million-ai-drone-warfare-contract

[33] Elias, Jennifer. "Google's pursuit of military cloud deal was among top issues at last week's all-staff meeting." *CNBC*. November 15, 2021. https://www.cnbc.com/2021/11/15/google-pursuit-of-jwcc-among-issues-of-top-concern-at-tgif-meeting-.html

[34] "Lockheed Martin Flies Real-Time, Mission Enabling Kubernetes Onboard U-2," *Lockheed Martin Corporation*. December 14, 2020. https://news.lockheedmartin.com/lockheed-martin-flies-real-time-mission-enabling-kubernetes-onboard-u-2

[35] Weinberger, Sharon. *The Imagineers of War*. New York: Penguin Random House. 2017. https://www.penguinrandomhouse.com/books/234382/the-imagineers-of-war-by-sharon-weinberger/

[36] Levine, Yasha. *Surveillance Valley*. New York: PublicAffairs. 2018. https://www.hachette-bookgroup.com/titles/yasha-levine/surveillance-valley/9781610398039/?lens=publicaffairs

[37] Shah, Raj J. and Christopher Kirchhoff. *Unit X*. New York: Simon & Schuster. 2024. https://www.simonandschuster.com/books/Unit-X/Raj-M-Shah/9781668031384

[38] Brose, Christian. *The Kill Chain*. New York: Hachette Books. 2020. https://www.hachette-bookgroup.com/titles/christian-brose/the-kill-chain/9780316533362/?lens=hachette-books

[39] Harper, John. "Army seeks $255M to procure more than 3,000 IVAS augmented reality systems in fiscal 2025." *DefenseScoop*. March 13, 2024. https://defensescoop.com/2024/03/13/army-ivas-procurement-fiscal-2025-microsoft/

[40] Ziv, Amitai. "Israel Picks Google, Amazon for Massive Official Cloud; 'Data Will Remain Here'." *Haaretz*. April 21, 2021. https://www.haaretz.com/israel-news/tech-news/2021-04-21/ty-article/israel-picks-google-amazon-for-official-state-cloud/0000017f-e896-dc91-a17f-fc9fd1ce0000

[41] Poulson, Jack. "Militaries, Intelligence Agencies, and Law Enforcement Dominate U.S. and U.K. Government Purchasing from U.S. Tech Giants." *Tech Inquiry*. September 5, 2022. https://techinquiry.org/docs/InternationalCloud.pdf

[42] Wilson, Mike. *The Difference Between God and Larry Ellison*. New York: Harper Collins. 1997. https://www.harpercollins.com/products/the-difference-between-god-and-larry-ellison-mike-wilson-1?variant=40970867015714

[43] Melman, Yossi. "Ex-generals in Secret Battle Over Israel's Project Nimbus." *Haaretz*. January 27, 2022. https://www.haaretz.com/israel-news/tech-news/2022-01-27/ty-article/.premium/ex-generals-and-big-tech-the-secret-battle-over-israels-cloud-project/0000017f-da72-d432-a77f-df7b551a0000

[44] Feeley, Jef and Lizette Chapman. "Oracle Weighed Buying Palantir in 2016, Investor Tells Court." *Bloomberg*. June 28, 2017. https://www.bloomberg.com/news/articles/2017-06-28/oracle-discussed-buying-palantir-in-2016-investor-tells-court

[45] Biddle, Sam. "Documents Reveal Advanced AI Tools Google Is Selling to Israel." *The Intercept*. July 24, 2022. https://theintercept.com/2022/07/24/google-israel-artificial-intelligence-project-nimbus/

[46] Poulson, Jack. "Microsoft and Google have been working closely with the Israeli military's Computer Services Directorate for years, in shadow of flashier military intelligence units." *All-Source Intelligence*. May 2, 2024. https://jackpoulson.substack.com/p/microsoft-and-google-have-been-working

[47] Abraham, Yuval. "'Order from Amazon': How tech giants are storing mass data for Israel's war." *+972 Magazine*. August 4, 2024. https://www.972mag.com/cloud-israeli-army-gaza-amazon-google-microsoft/

[48] Lucy A. Suchman, email message to the author, October 18, 2024.

[49] Probasco, Emelia. "Building the Tech Coalition." *Center for Security and Emerging Technology*. August 2024. https://cset.georgetown.edu/publication/building-the-tech-coalition/

[50] Bob, Yonah Jeremy. "Senior IDF official: War friction pushed us to new digital highs." The Jerusalem Post. February 5, 2024. https://www.jpost.com/israel-hamas-war/article-785281

[51] Roberts, Les. "The Science Is Clear. Over 30,000 People Have Died in Gaza." *TIME Magazine*. March 15, 2024. https://time.com/6909636/gaza-death-toll/

[52] Poulson, Jack. "'Your AI is Your Rifle': Leak sheds light on ecosystem behind Pentagon's AI adoption." *All-Source Intelligence*. April 10, 2024. https://jackpoulson.substack.com/p/your-ai-is-your-rifle

[53] Poulson, Jack. "Head of CIA OSINT emphasizes centrality of Twitter and Telegram surveillance." *All-Source Intelligence*. September 28, 2023. https://jackpoulson.substack.com/p/head-of-cia-osint-emphasizes-centrality

[54] Priest, Dana. "The CIA's Secret War with Dana Priest." *UC Santa Cruz*. February 8, 2008. https://youtube.com/watch?v=ne4ao6TANiA&t=1582s

[55] Priest, Dana. "CIA's private jet an open secret in terror war." *NBC News*. December 27, 2004. https://www.nbcnews.com/id/wbna6757281

[56] "Jerrold Post, M.D.," *Center for Advanced Defense Studies*. Accessed on April 23, 2010. https://web.archive.org/web/20100423070523/https://c4ads.org/jerrold.post

[57] Tsao, Daniel. "Psychiatrists, Professors, Patriots: Remembering Drs. Jerrold Post (1934–2020) and Laurence Cove (1933–2020)." *Studies in Intelligence* 65, no. 1 (March 2021), https://www.cia.gov/resources/csi/static/InMemoriamJerroldPostLarryCove.pdf

[58] Broder, Jonathan. "CIA Had Role in Israeli Assassination Try in Lebanon—Report." *SpyTalk*. October 15, 2024. https://www.spytalk.co/p/cia-had-role-in-israeli-assasssination

[59] "Program Evaluation and Review Technique," Britannica. Accessed October 17, 2024. https://www.britannica.com/technology/Program-Evaluation-and-Review-Technique

[60] Aid, Matthew. "The CIA in Germany: A Secret History." *The Daily Beast*. July 10, 2014. https://www.thedailybeast.com/the-cia-in-germany-a-secret-history

[61] Paseman, Floyd. *A Spy's Journey*. Minneapolis: Zenith Press. 2004. https://www.amazon.com/Spys-Journey-CIA-Memoir/dp/B006G83FUM

[62] Bearden, Milt and James Risen. *The Main Enemy*. New York: Penguin Random House. 2003. https://www.penguinrandomhouse.com/books/10139/the-main-enemy-by-milt-bearden-and-james-risen/

[63] "CIA Memo, Air Pouch, Chief of Station, Germany-Chief of Base, Berlin – German Press Flap over Fighting Group Against Inhumanity, November 16, 1955," *National Security Archive*. May 11, 2022. https://nsarchive.gwu.edu/document/28073-document-2-cia-memo-air-pouch-chief-station-germany-chief-base-berlin-german-press

[64] Whitney, Craig R. "Doubt Nibbles at C.I.A. Official's Reputation." *The New York Times*. April 14, 1994. https://www.nytimes.com/1994/04/14/us/doubt-nibbles-at-cia-official-s-reputation.html

[65] Vogel, Steve. "Gardner R. Hathaway, CIA chief of counterintelligence, dies at 88." *The Washington Post*. November 26, 2013. https://www.washingtonpost.com/national/gardner-r-hathaway-cia-chief-of-counterintelligence-dies-at-88/2013/11/26/d58f6b0a-561c-11e3-ba82-16ed03681809_story.html

[66] WikiLeaks. *The WikiLeaks Files*. New York: Verso. 2015. https://www.versobooks.com/products/86-the-wikileaks-files

[67] Sontheimer, Michael. "CIA Spies May Also Operate in Frankfurt." *SPIEGEL International*. March 7, 2017. https://www.spiegel.de/international/world/wikileaks-data-dump-on-cia-spying-vault-7-a-1137740.html

[68] Johnston, David and Mark Mazzetti. "CIA Spies May Also Operate in Frankfurt." *The New York Times*. August 13, 2009. https://www.nytimes.com/2009/08/13/world/13foggo.html

[69] Goldman, Adam. "The hidden history of the CIA's prison in Poland." *The Washington Post*. January 23, 2014. www.washingtonpost.com/world/national-security/the-hidden-history-of-the-cias-prison-in-poland/2014/01/23/b77f6ea2-7c6f-11e3-95c6-0a7aa80874bc_story.html

[70] "Welcome to the 66th MI Brigade Public Web Site," *66th Military Intelligence Brigade*. May 16, 2023. https://www.inscom.army.mil/MSC/66MIB/

[71] Von SPIEGEL Staff. "Inside Snowden's Germany File." *SPIEGEL International*. June 18, 2014. https://www.spiegel.de/international/germany/new-snowden-revelations-on-nsa-spying-in-germany-a-975441.html

[72] Corbin, Jacob. "Transformation managed: Directorate closes after 8 years of hard work." *U.S. Army*. August 12, 2015. https://www.army.mil/article/153696/transformation_managed_directorate_closes_after_8_years_of_hard_work

[73] “Delivery Order PIID 47QFCA19F0035.” USASpending.gov. Accessed October 17, 2024. https://www.usaspending.gov/award/CONT_AWD_47QFCA19F0035_4732_GS00Q14OADU116_4732

[74] Strottman, Matthew. ”In-Q-Tel, Inc. Form 990 for period ending March 2020.” *ProPublica*. February 10, 2021. https://projects.propublica.org/nonprofits/display_990/522149962/04_2021_prefixes_52-54/522149962_202003_990_2021041217921882

[75] Palmer, Annie. "Amazon acquires secure chat app used by government agencies.” *CNBC*. June 25, 2021. https://www.cnbc.com/2021/06/25/amazon-acquires-wickr-secure-messaging-app-used-by-government-agencies.html

[76] Cox, Joseph. "CIA Funding Arm Gave Encrypted App Wickr $1.6 Million.” *VICE News*. October 12, 2021. https://www.vice.com/en/article/y3dawk/wickr-cia-funding-inqtel

[77] "Signal (Open Whisper Systems),” *Open Technology Fund*. Accessed March 23, 2023. https://web.archive.org/web/20230323141335/https://www.opentech.fund/results/supported-projects/open-whisper-systems/

[78] John, Eric G. "SOUTHERN VIOLENCE: HARSH TACTICS, LESS VIOLENCE, LESS HOPE.” *U.S. Embassy Bangkok*. March 25, 2008. https://wikileaks.org/plusd/cables/08BANGKOK943_a.html

[79] Boyce, Ralph L. "SOUTHERN VIOLENCE: LABELING THE MILITANTS ‘BRN-C'." *U.S. Embassy Bangkok*. December 9, 2005. https://wikileaks.org/plusd/cables/05BANGKOK7573_a.html

[80] Boyce, Ralph L. "COUP RUMORS HAVE BANGKOK ON EDGE.” *U.S. Embassy Bangkok*. January 5, 2007. https://wikileaks.org/plusd/cables/07BANGKOK83_a.html

[81] Boyce, Ralph L. "SOUTHERN VIOLENCE: UNDERSTANDING THE INSURGENCY.” *U.S. Embassy Bangkok*. August 29, 2007. https://wikileaks.org/plusd/cables/07BANGKOK4653_a.html

[82] Arkin, William M. “Read the Leaked Secret Intelligence Documents on Ukraine and Vladimir Putin.” *Newsweek*. April 16, 2023. https://www.newsweek.com/2023/05/05/read-leaked-secret-intelligence-documents-ukraine-vladimir-putin-1794656.html

[83] “Airman Teixeira Leaks,” *Distributed Denial of Secrets*. January 16, 2024. https://ddosecrets.com/article/airman-teixeira-leaks

[84] Klippenstein, Ken. “Israel Preps for Strike on Iran, Top Secret Leak Reveals.” *Ken Klippenstein*. October 19, 2024. https://www.kenklippenstein.com/p/israel-preps-for-strike-on-iran-top

[85] Zoria, Yuri. “Aver unveils secretive Phoenix Ghost kamikaze drones, supplied to Ukraine.” *Euromaidan Press*. October 18, 2024. https://euromaidanpress.com/2024/10/18/twz-aevex-unveils-secretive-phoenix-ghost-kamikaze-drones-supplied-to-ukraine/

[86] Lamothe, Dan. “Russia nearly shot down British spy plane near Ukraine, leaked document says.” The Washington Post. April 9, 2023. https://www.washingtonpost.com/national-security/2023/04/09/leaked-documents-surveillance-plane-rivet-joint/

[87] Poulson, Jack. "U.S. Army simulated exploiting The Taipei Times, Buddhist monks, and surgeons through online propaganda in context of Chinese invasion of Taiwan.” *All-Source Intelligence*. March 23, 2024. https://jackpoulson.substack.com/p/exclusive-us-army-simulated-exploiting

[88] “PULSE," *Two Six Technologies*. Accessed October 17, 2024. https://twosixtech.com/products/pulse/

[89] Schectman, Joel and Christopher Bing. "Trump launched CIA covert influence operation against China.” *Reuters*. March 14, 2024. https://www.reuters.com/world/us/trump-launched-cia-covert-influence-operation-against-china-2024-03-14/

[90] "CIA propaganda officer Joe Goldberg on disinfo ops, narrative building, and more. Ep. 54,” *The Team House*. August 7, 2020. https://youtube.com/watch?v=Fu4QhAERYVE

[91] Amaro, William. "Ghosts In The Machine.” *4th Psychological Operations Group*. May 1, 2023. https://www.dvidshub.net/video/882019/ghosts-machine

[92] Poulson, Jack. "Pollster for Niger coup support is a surveillance platform for U.S. Special Operations Forces." *All-Source Intelligence*. August 27, 2023. https://jackpoulson.substack.com/p/pollster-for-niger-coup-support-is

[93] Poulson, Jack. "Mai Tais, More Eyes, and Mercenaries." *All-Source Intelligence*. April 12, 2023. https://jackpoulson.substack.com/p/mai-tais-more-eyes-and-mercenaries

[94] "IST Research and Two Six Labs Combine to Form High-Growth Government Technology Platform," *The Carlyle Group*. February 1, 2021. https://www.carlyle.com/media-room/news-release-archive/ist-research-and-two-six-labs-combine-form-government-technology-platform

[95] Poulson, Jack. "Where the U.S. is training soldiers to spy on China in the age of cellphones and facial recognition." *All-Source Intelligence*. March 20, 2024. https://jackpoulson.substack.com/p/where-the-us-is-training-soldiers

[96] "Camera Laboratory," *SAM.gov*. August 17, 2023. https://sam.gov/opp/cf81984dd95845f48ab3a62291b9c213/view

[97] "Purchase Order PIID W91RUS23P0081," *USASpending.gov*. Accessed October 17, 2024. https://www.usaspending.gov/award/CONT_AWD_W91RUS23P0081_9700_-NONE-_-NONE-

[98] "Andrew Wilson," *Quiet Professionals*. Accessed October 17, 2024. https://innovationsoftheworld.com/andrew-wilson-quiet-professionals/

[99] "Leo Kryszewski," *Quiet Professionals*. Accessed October 17, 2024. https://quietprofessionalsllc.com/leo-kryszewski/

[100] Ratliff, Evan. "The Mastermind." *Atavist Magazine*. Accessed October 17, 2024. https://magazine.atavist.com/the-mastermind/

[101] "Hidden Volume," *Truecrypt,* July 30, 2015. https://www.truecrypt71a.com/documentation/plausible-deniability/hidden-volume/

[102] Poulson, Jack and Sam Biddle. "The Online Christian Counterinsurgency Against Sex Workers." *The Intercept*. July 29, 2023. https://theintercept.com/2023/07/29/skull-games-surveillance-sex-workers/

[103] "SPLC History: 1980s," *Southern Poverty Law Center*. Accessed October 17, 2024. https://www.splcenter.org/about-us/our-history/splc-history-1980s

[104] Darshan-Leitner, Nitsana and Samuel M. Katz. *Harpoon*. New York: Hachette Books. 2018. https://www.hachettebookgroup.com/titles/nitsana-darshan-leitner/harpoon/9780316399012/?lens=hachette-books

[105] "Israel Ministry of Justice," *Distributed Denial of Secrets*. July 25, 2024. https://ddosecrets.com/article/israel-ministry-of-justice

[106] Rabin, Roni. "Hamas Hostages and Families of Captives Sue Red Cross in Israeli Court." *The New York Times*. December 22, 2023. https://www.nytimes.com/2023/12/22/world/middleeast/israel-hamas-hostages-red-cross-lawsuit.html

[107] Eichner, Itamar. "Israeli group urges US to probe Amal Clooney's role in ICC warrant for Netanyahu." *Ynet News*. June 28, 2024. https://www.ynetnews.com/article/syeqrz2uc

[108] Eichner, Itamar. "'Terrorist wing in academia': October 7 victims sue Students for Justice in Palestine organization." *Ynet News*. May 4, 2024. https://www.ynetnews.com/article/rj5ymweg0

[109] Fang, Lee and Jack Poulson. "Israeli documents show expansive government effort to shape US discourse around Gaza war." *The Guardian*. June 24, 2024. https://www.theguardian.com/world/article/2024/jun/24/israel-fund-us-university-protest-gaza-antisemitism

[110] Fang, Lee and Jack Poulson. "Israel feared legal trouble over US advocacy efforts, leaked files suggest." *The Guardian*. August 17, 2024. https://www.theguardian.com/world/article/2024/aug/17/israel-foreign-agent-law-leaked-documents

[111] TOI Staff. "Mossad involved in Israel's anti-BDS efforts – report." *The Times of Israel*. June 12, 2019. https://www.timesofisrael.com/mossad-involved-in-israels-anti-bds-efforts-report/

[112] Davies, Harry. "Israeli spy chief 'threatened' ICC prosecutor over war crimes inquiry." *The Guardian*. May 28, 2024. https://www.theguardian.com/world/article/2024/may/28/israeli-spy-chief-icc-prosecutor-war-crimes-inquiry

[113] "The history of the IAC," *Israeli-American Council*. Accessed June 2, 2024. https://web.archive.org/web/20240602225159/https://www.israeliamerican.org/national/history-of-iac

[114] "Watch the film the Israel lobby didn't want you to see." *The Electronic Intifada*. November 2, 2018. https://electronicintifada.net/content/watch-film-israel-lobby-didnt-want-you-see/25876

[115] Poulson, Jack. "The Australian ad-tech firm secretly fueling 'psychological warfare' against U.S. university students." *All-Source Intelligence*. June 10, 2024. https://jackpoulson.substack.com/p/the-australian-ad-tech-firm-secretly

[116] Thomsen, Simon. "Adtech startup BlendAI raises $1.5 million to automate e-commerce online ads." *Startup Daily*. July 13, 2022. https://www.startupdaily.net/topic/funding/adtech-startup-blendai-raises-1-5-million-to-automate-e-commerce-online-ads/

[117] "Eran Teboul: How to build collaboration to fight hate and demonization," *Med Israel for fred*. May 13, 2022. https://youtube.com/watch?v=CkdjfwoEfcg&t=2501s

[118] Naylor, Sean. *Relentless Strike*. New York: Macmillan. 2015. https://us.macmillan.com/books/9781466876224/relentlessstrike

[119] Raviv, Dan and Yossi Melman. *Spies Against Armageddon*. Sea Cliff: Levant Books. 2012. https://www.amazon.com/Spies-Against-Armageddon-Dan-Raviv/dp/0985437812

[120] "Taipei Economic and Cultural Representative Office in the United States – ALTIUS 600M-V Unmanned Aerial Vehicles," *Defense Security Cooperation Agency*. June 18, 2024. https://www.dsca.mil/press-media/major-arms-sales/taipei-economic-and-cultural-representative-office-united-states-34

[121] Poulson, Jack. "Pentagon confirms erasure of Project Maven-related contract records." *All-Source Intelligence*. November 5, 2024. https://open.substack.com/pub/jackpoulson/p/pentagon-confirms-erasure-of-project

[122] "Rugged high-density computing for Minotaur-integrated platforms and programmes," *Shephard Media*. May 6, 2019. https://www.shephardmedia.com/news/naval-warfare/rugged-high-density-computing-minotaur-integrated-/

[123] "Delivery Order (DO) PIID N0002423F8170," *USASpending.gov*. Accessed on November 5, 2024. https://www.usaspending.gov/award/CONT_AWD_N0002423F8170_9700_N0002422D6404_9700

[124] "Delivery Order (DO) PIID 70B02C23F00000438," *USASpending.gov*. Accessed on November 5, 2024. https://www.usaspending.gov/award/CONT_AWD_70B02C23F00000438_7014_70B02C23D00000004_7014

[125] "Multi-role Enforcement Aircraft," *U.S. Customs and Border Protection*. September 28, 2016. https://www.cbp.gov/newsroom/video-gallery/video-library/multi-role-enforcement-aircraft

[126] Campbell, Duncan. *The Unsinkable Aircraft Carrier*. London: Paladin. 1986. https://www.duncan-campbell.org/unsink