Another Mega Group Spy Scandal? Samanage, Sabotage, And The SolarWinds Hack

The devastating hack on SolarWinds was quickly pinned on Russia by US intelligence. A more likely culprit, Samanage, a company whose software was integrated into SolarWinds' software just as the "back door" was inserted, is deeply tied to Israeli intelligence and intelligence-linked families such as the Maxwells.

BY **WHITNEY WEBB** JANUARY 22, 2021 19 MINUTE READ

Originally published at *The Last American Vagabond*

In mid-December of 2020, a massive hack compromised the networks of numerous US federal agencies, major corporations, the top five accounting firms in the country, and the military, among others. Despite most US media attention now focusing on election-related chaos, the fallout from the hack continues to make headlines day after day.

The hack, which affected Texas-based software provider SolarWinds, was blamed on Russia on January 5 by the US government's Cyber Unified Coordination Group. Their statement asserted that the attackers were "likely Russian in origin," but they failed to provide evidence to back up that claim.

Since then, numerous developments in the official investigation have been reported, but no actual evidence pointing to Russia has yet to be released. Rather, mainstream media outlets began reporting the intelligence community's "likely" conclusion as fact right away, with the *New York Times* subsequently reporting that US investigators were examining a product used by SolarWinds that was sold by a Czech

Republic–based company, as the possible entry point for the "Russian hackers." Interest in that company, however, comes from the fact that the attackers most likely had access to the systems of a contractor or subsidiary of SolarWinds. This, combined with the evidence-free report from US intelligence on "likely" Russian involvement, is said to be the reason investigators are focusing on the Czech company, though any of SolarWinds' contractors/subsidiaries could have been the entry point.

Such narratives clearly echo those that became prominent in the wake of the 2016 election, when now-debunked claims were made that Russian hackers were responsible for leaked emails published by WikiLeaks. Parallels are obvious when one considers that SolarWinds quickly brought on the discredited firm CrowdStrike to aid them in securing their networks and investigating the hack. CrowdStrike had also been brought on by the DNC after the 2016 WikiLeaks publication, and subsequently it was central in developing the false declarations regarding the involvement of "Russian hackers" in that event.

There are also other parallels. As Russiagate played out, it became apparent that there was collusion between the Trump campaign and a foreign power, but the nation was Israel, not Russia. Indeed, many of the reports that came out of Russiagate revealed collusion with Israel, yet those instances received little coverage and generated little media outrage. This has led some to suggest that Russiagate may have been a cover for what was in fact Israelgate.

Similarly, in the case of the SolarWinds hack, there is the odd case and timing of SolarWinds' acquisition of a company called Samanage in 2019. As this report will explore, Samanage's deep ties to Israeli intelligence, venture-capital firms connected to both intelligence and Isabel Maxwell, as well as Samange's integration with the Orion software at the time of the back door's insertion warrant investigation every bit as much as SolarWinds' Czech-based contractor.

Orion's Fall

In the month since the hack, evidence has emerged detailing the extent of the damage, with the Justice Department quietly announcing, the same day as the Capitol riots (January 6), that their email system had been breached in the hack—a "major incident" according to the department. This terminology means that the attack "is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people," per NextGov.

The Justice Department was the fourth US government agency to publicly acknowledge a breach in connection to the hack, with the others being the Departments of Commerce and Energy and the Treasury. Yet, while only four agencies have publicly acknowledged fallout from the hack, SolarWinds software is also used by the Department of Defense, the State Department, NASA, the NSA, and the Executive Office. Given that the Cyber Unified Coordination Group stated that "fewer than ten" US government agencies had been affected, it's likely that some of these agencies were compromised, and some press reports have asserted that the State Department and Pentagon were affected.

In addition to government agencies, SolarWinds Orion software was in use by the top ten US telecommunications corporations, the top five US accounting firms, the New York Power Authority, and numerous US government contractors such as Booz Allen Hamilton, General Dynamics, and the Federal

Reserve. Other notable SolarWinds clients include the Bill & Melinda Gates Foundation, Microsoft, Credit Suisse, and several mainstream news outlets including the *Economist* and the *New York Times*.

Based on what is officially known so far, the hackers appeared to have been highly sophisticated, with FireEye, the cybersecurity company that first discovered the implanted code used to conduct the hack, stating that the hackers "routinely removed their tools, including the backdoors, once legitimate remote access was achieved—implying a high degree of technical sophistication and attention to operational security." In addition, top security experts have noted that the hack was "very very carefully orchestrated," leading to a consensus that the hack was state sponsored.

FireEye stated that they first identified the compromise of SolarWinds after the version of the Orion software they were using contained a back door that was used to gain access to its "red team" suite of hacking tools. Not long after the disclosure of the SolarWinds hack, on December 31, the hackers were able to partially access Microsoft's source code, raising concerns that the act was preparation for future and equally devastating attacks.

FireEye's account can be taken with a grain of salt, however, as the CIA is one of FireEye's clients, and FireEye was launched with funding from the CIA's venture capital arm In-Q-tel. It is also worth being skeptical of the "free tool" FireEye has made available in the hack's aftermath for "spotting and keeping suspected Russians out of systems."

In addition, Microsoft, another key source in the SolarWinds story, is a military contractor with close ties to Israel's intelligence apparatus, especially Unit 8200, and their reports of events also deserve scrutiny. Notably, it was Unit 8200 alumnus and executive at Israeli cybersecurity firm Cycode, Ronen Slavin, who told *Reuters* in a widely quoted article that he "was worried by the possibility that the SolarWinds hackers were poring over Microsoft's source code as prelude to a much more ambitious offensive." "To me the biggest question is, 'Was this recon for the next big operation?'" Slavin stated.

Also odd about the actors involved in the response to the hack is the decision to bring on not only the discredited firm CrowdStrike but also the new consultancy firm of Chris Krebs and Alex Stamos, former chief information security officer of Facebook and Yahoo, to investigate the hack. Chris Krebs is the former head of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and was previously a top Microsoft executive. Krebs was fired by Donald Trump after repeatedly and publicly challenging Trump on the issue of election fraud in the 2020 election.

As head of CISA, Krebs gave access to networks of critical infrastructure throughout the US, with a focus on the health-care industry, to the CTI League, a suspicious outfit of anonymous volunteers working "for free" and led by a former Unit 8200 officer. "We have brought in the expertise of Chris Krebs and Alex Stamos to assist in this review and provide best-in-class guidance on our journey to evolve into an industry leading secure software development company," a SolarWinds spokesperson said in an email cited by *Reuters*.

It is also worth noting that the SolarWinds hack did benefit a few actors aside from the attackers themselves. For instance, Israeli cybersecurity firms CheckPoint and CyberArk, which have close ties to Israeli intelligence Unit 8200, have seen their stocks soar in the weeks since the SolarWinds compromise was announced. Notably, in 2017, CyberArk was the company that "discovered" one of the main tactics used in an attack, a form of SAML token manipulation called GoldenSAML. CyberArk does not specify how they discovered this method of attack and, at the time they announced the tactic's existence, released a free tool to identify systems vulnerable to GoldenSAML manipulation.

In addition, the other main mode of attack, a back door program nicknamed Sunburst, was found by Kaspersky researchers to be similar to a piece of malware called Kazuar that was also first discovered by another Unit 8200-linked company, Palo Alto Networks, also in 2017. The similarities only suggest that those who developed the Sunburst backdoor may have been inspired by Kazuar and "they may have common members between them or a shared software developer building their malware." Kaspersky stressed that Sunburst and Kazuar are not likely to be one and the same. It is worth noting, as an aside, that Unit 8200 is known to have previously hacked Kaspersky and attempted to insert a back door into their products, per Kaspersky employees.

Crowdstrike claimed that this finding confirmed "the attribution at least to Russian intelligence," only because an allegedly Russian hacking group is believed to have used Kazuar before. No technical evidence linking Russia to the SolarWinds hacking has yet been presented.

Samanage and Sabotage

The implanted code used to execute the hack was directly injected into the source code of SolarWinds Orion. Then, the modified and bugged version of the software was "compiled, signed and delivered through the existing software patch release management system," per reports. This has led US investigators and observers to conclude that the perpetrators had direct access to SolarWinds code as they had "a high degree of familiarity with the software." While the way the attackers gained access to Orion's code base has yet to be determined, one possibility being pursued by investigators is that the attackers were working with employee(s) of a SolarWinds contractor or subsidiary.

US investigators have been focusing on offices of SolarWinds that are based abroad, suggesting that—in addition to the above—the attackers were likely working for SolarWinds or were given access by someone working for the company. That investigation has focused on offices in eastern Europe, allegedly because "Russian intelligence operatives are deeply rooted" in those countries.

It is worth pointing out, however, that Israeli intelligence is similarly "deeply rooted" in eastern European states both before and after the fall of the Soviet Union, ties well illustrated by Israeli superspy and media tycoon Robert Maxwell's frequent and close associations with Eastern European and Russian intelligence agencies as well as the leaders of many of those countries. Israeli intelligence operatives like Maxwell also had cozy ties with Russian organized crime. For instance, Maxwell enabled the access of the Russian organized crime network headed by Semion Mogilevich into the US financial system and was also Mogilevich's business partner. In addition, the cross-pollination between Israeli and Russian organized crime networks (networks which also share ties to their respective intelligence agencies) and such links should be considered if the cybercriminals due prove to be Russian in origin, as US intelligence has claimed.

Though some contractors and subsidiaries of SolarWinds are now being investigated, one that has yet to be investigated, but should be, is Samanage. Samanage, acquired by SolarWinds in 2019, not only gained automatic access to Orion just as the malicious code was first inserted, but it has deep ties to Israeli intelligence and a web of venture-capital firms associated with numerous Israeli espionage scandals that have targeted the US government. Israel is deemed by the NSA to be one of the top spy threats facing US government agencies and Israel's list of espionage scandals in the US is arguably the longest, and includes the Jonathan Pollard and PROMIS software scandals of the 1980s to the Larry Franklin/AIPAC espionage scandal in 2009.

Though much reporting has since been done on the recent compromise of SolarWinds Orion software, little attention has been paid to Samanage. Samanage offers what it describes as "an IT Service Desk solution." It was acquired by SolarWinds so Samanage's products could be added to SolarWinds' IT Operations Management portfolio. Though US reporting and SolarWinds press releases state that Samanage is based in Cary, North Carolina, implying that it is an American company, Samanage is actually an Israeli firm. It was founded in 2007 by Doron Gordon, who previously worked for several years at MAMRAM, the Israeli military's central computing unit.

Samanage was SolarWinds' first acquisition of an Israeli company, and, at the time, Israeli media reported that SolarWinds was expected to set up its first development center in Israel. It appears, however, that SolarWinds, rather than setting up a new center, merely began using Samanage's research and development center located in Netanya, Israel.

Several months after the acquisition was announced, in November 2019, Samanage, renamed SolarWinds Service Desk, became listed as a standard feature of SolarWinds Orion software, whereas the integration of Samanage and Orion had previously been optional since the acquisition's announcement in April of that year. This means that complete integration was likely made standard in either October or November. It has since been reported that the perpetrators of the recent hack gained access to the networks of US federal agencies and major corporations at around the same time. Samanage's automatic integration into Orion was a major modification made to the now-compromised software during that period.

Samanage appears to have had access to Orion following the announcement of the acquisition in April 2019. Integration first began with Orion version 2019.4, the earliest version believed to contain the malicious code that enabled the hack. In addition, the integrated Samanage component of Orion was responsible for "ensuring the appropriate teams are quickly notified when critical events or performance issues [with Orion] are detected," which was meant to allow "service agents to react faster and resolve issues before . . . employees are impacted."

In other words, the Samanage component that was integrated into Orion at the same time the compromise took place was also responsible for Orion's alert system for critical events or performance issues. The code that was inserted into Orion by hackers in late 2019 nevertheless went undetected by this Samanage-made component for over a year, giving the "hackers" access to millions of devices critical to both US government and corporate networks. Furthermore, it is this Samanage-produced component of the affected Orion software that advises end users to exempt the software from antivirus scans and group policy object (GPO) restrictions by providing a warning that Orion may not work properly unless those exemptions are granted.

Samanage, Salesforce, and the World Economic Forum

Around the time of Samange's acquisition by SolarWinds, it was reported that one of Samanage's top backers was the company Salesforce, with Salesforce being both a major investor in Samanage as well as a partner of the company.

Salesforce is run by Marc Benioff, a billionaire who got his start at the tech giant Oracle. Oracle was originally created as a CIA spin-off and has deep ties to Israel's government and the outgoing Trump administration. Salesforce also has a large presence in Israel, with much of its global research and development based there. Salesforce also recently partnered with the Unit 8200-linked Israeli firm Diagnostic Robotics to "predictively" diagnose COVID-19 cases using Artificial Intelligence.

Aside from leading Salesforce, Benioff is a member of the Vatican's Council for Inclusive Capitalism alongside Lynn Forester de Rothschild, a close associate of Jeffrey Epstein and the Clintons, and members of the Lauder family, who have deep ties to the Mega Group and Israeli politics.

Benioff is also a prominent member of the board of trustees of the World Economic Forum and the inaugural chair of the WEF's Centre for the Fourth Industrial Revolution (C4IR), making him one of the most critical players in the unfolding of the WEF-backed Great Reset. Other WEF leaders, including the organization's founder Klaus Schwab, have openly discussed how massive cyberattacks such as befell SolarWinds will soon result in "even more significant economic and social implications than COVID-19."

Last year, the WEF's Centre for Cybersecurity, of which Salesforce is part, simulated a "digital pandemic" cyberattack in an exercise entitled Cyber Polygon. Cyber Polygon's speakers in 2020 included former UK Prime Minister Tony Blair, the Prime Minister of Russia Mikhail Mishustin, WEF founder Klaus Schwab, and IBM executive Wendi Whitmore, who previously held top posts at both Crowdstrike and a FireEye subsidiary. Notably, just months before the COVID-19 crisis, the WEF had held Event 201, which simulated a global coronavirus pandemic that crippled the world's economy.

In addition to Samanage's ties to WEF big shots such as Marc Benioff, the other main investors behind Samanage's rise have ties to major Israeli espionage scandals, including the Jonathan Pollard affair and the PROMIS software scandal. There are also ties to one of the WEF's founding "technology pioneers," Isabel Maxwell (the daughter of Robert Maxwell and sister of Ghislaine), who has long-standing ties to Israel's intelligence apparatus and the country's hi-tech sector.

The Bronfmans, the Maxwells, and Viola Ventures

At the time of its acquisition by SolarWinds, Samanage's top investor was Viola Ventures, a major Israeli venture-capital firm. Viola's investment in Samanage, until its acquisition, was managed by Ronen Nir, who was also on Samanage's board before it became part of SolarWinds.

Prior to working at Viola, Ronen Nir was a vice president at Verint, formerly Converse Infosys. Verint, whose other alumni have gone on to found Israeli intelligence-front companies such as Cybereason. Verint has a history of aggressively spying on US government facilities, including the White House, and created the backdoors into all US telecommunications systems and major tech companies, including Microsoft, Google and Facebook, on behalf of the US' NSA.

In addition to his background at Verint, Ronen Nir is an Israeli spy, having served for thirteen years in an elite IDF intelligence unit, and he remains a lieutenant colonel on reserve duty. His biography also notes that he worked for two years at the Israeli embassy in Washington, DC, which is fitting given his

background in espionage and the major role that Israeli embassy has played in several major espionage scandals.

As an aside, Nir has stated that "thought leader" Henry Kissinger is his "favorite historical character." Notably, Kissinger was instrumental in allowing Robert Maxwell, Israeli superspy and father of Ghislaine and Isabel Maxwell, to sell software with a back door for Israeli intelligence to US national laboratories, where it was used to spy on the US nuclear program. Kissinger had told Maxwell to connect with Senator John Tower in order to gain access to US national laboratories, which directly enabled this action, part of the larger PROMIS software scandal.

In addition, Viola's stake was managed through a firm known as Carmel Ventures, which is part of the Viola Group. At the time, Carmel Ventures was advised by Isabel Maxwell, whose father had previously been directly involved in the operation of the front company used to sell bugged software to US national laboratories. As noted in a previous article at *Unlimited Hangout*, Isabel "inherited" her father's circle of Israeli government and intelligence contacts after his death and has been instrumental in building the "bridge" between Israel's intelligence and military-linked hi-tech sector to Silicon Valley.

Isabel also has ties to the Viola Group itself through Jonathan Kolber, a general partner at Viola. Kolber previously cofounded and led the Bronfman family's private-equity fund, Claridge Israel (based in Israel). Kolber then led Koor Industries, which he had acquired alongside the Bronfmans via Claridge. Kolber is closely associated with Stephen Bronfman, the son of Charles Bronfman who created Claridge and also cofounded the Mega Group with Leslie Wexner in the early 1990s.

Kolber, like Isabel Maxwell, is a founding director of the Peres Center for Peace and Innovation. Maxwell, who used to chair the center's board, stepped down following the Epstein scandal, though it's not exactly clear when. Other directors of the center include Tamir Pardo, former head of Mossad. Kolber's area of expertise, like that of Isabel Maxwell, is "structuring complex, cross-border and cross industry business and financial transactions," that is, arranging acquisitions and partnerships of Israeli firms by US companies. Incidentally, this is also a major focus of the Peres Center.

Other connections to Isabel Maxwell, aside from her espionage ties, are worth noting, given that she is a "technology pioneer" of the World Economic Forum. As previously mentioned, Salesforce—a major investor in Samanage—is deeply involved with the WEF and its Great Reset.

The links of Israeli intelligence and Salesforce to Samanage, and thus to SolarWinds, is particularly relevant given the WEF's "prediction" of a coming "pandemic" of cyberattacks and the early hints from former Unit 8200 officers that the SolarWinds hack is just the beginning. It is also worth mentioning the Israeli government's considerable ties to the WEF over the years, particularly last year when it joined the Benioff-chaired C4IR and participated in the October 2020 WEF panel entitled "The Great Reset: Harnessing the Fourth Industrial Revolution."

Start Up Nation Central, an organization aimed at integrating Israeli start-ups with US firms set up by Netanyahu's longtime economic adviser Eugene Kandel and American Zionist billionaire Paul Singer, have asserted that Israel will serve a "key role" globally in the 4th Industrial Revolution following the implementation of the Great Reset.

Gemini, the BIRD Foundation, and Jonathan Pollard

In addition to Viola, another of Samange's leading investors is Gemini Israel Ventures. Gemini is one of Israel's oldest venture-capital firms, dating back to the Israeli government's 1993 Yozma program.

The first firm created by Yozma, Gemini was put under the control of Ed Mlavsky, who Israel's government had chosen specifically for this position. As previously reported by *Unlimited Hangout*, Mlavsky was then serving as the executive director of the Israel-US Binational Industrial Research and Development (BIRD) Foundation, where "he was responsible for investments of $100 million in more than 300 joint projects between US and Israeli high-tech companies."

A few years before Gemini was created, while Mlavsky still headed BIRD, the foundation became embroiled in one of the worst espionage scandals in US history, the Jonathan Pollard affair.

In the indictment of US citizen Pollard for espionage on Israel's behalf, it was noted that Pollard delivered the documents he stole to agents of Israel at two locations, one of which was an apartment owned by Harold Katz, the then legal counsel of the BIRD Foundation and an adviser to Israel's military, which oversaw Israel's scientific intelligence-gathering agency, Lekem. US officials told the *New York Times* at the time that they believed Katz "has detailed knowledge about the [Pollard] spy ring and could implicate senior Israeli officials."

Subsequent reporting by journalist Claudia Wright pointed the finger at the Mlavsky-run BIRD Foundation as one of the ways Israeli intelligence funneled money to Pollard before his capture by US authorities.

One of the first companies Gemini invested in was CommTouch (now Cyren), which was founded by ex-IDF officers and later led by Isabel Maxwell. Under Maxwell's leadership, CommTouch developed close ties to Microsoft, partially due to Maxwell's relationship with its cofounder Bill Gates.

A Coming "Hack" of Microsoft?

If the SolarWinds hack is as serious as has been reported, it's difficult to understand why a company like Samanage would not be looked into as part of a legitimate investigation into the attack. The timing of Samanage employees gaining access to the Orion software and the company's investors including Israeli spies and those with ties to past espionage scandals where Israel used back doors to spy on the US and beyond raises obvious red flags. Yet, any meaningful investigation of the incident is unlikely to take place, especially given the considerable involvement of discredited firms like CrowdStrike, CIA fronts like FireEye and a consultancy firm led by former Silicon Valley executives with their own government/intelligence ties.

There is also the added fact that both of the main methods used in the attack were analogous or bore similarities to hacking tools that were both discovered by Unit 8200-linked companies in 2017. Unit

8200-founded cybersecurity firms are among the few "winners" from the SolarWinds hack, as their stocks have skyrocketed and demand for their services has increased globally.

While some may argue that Unit 8200 alumni are not necessarily connected to the Israeli intelligence apparatus, numerous reports have pointed out the admitted fusion of Israeli military intelligence with Israel's hi-tech sector and its tech-focused venture capital networks, with Israeli military and intelligence officials themselves noting that the line between the private cybersecurity sector and Israel's intelligence apparatus is so blurred, it's difficult to know where one begins and the other ends. There is also the Israeli government policy, formally launched in 2012, whereby Israel's intelligence and military intelligence agencies began outsourcing "activities that were previously managed in-house, with a focus on software and cyber technologies."

Samanage certainly appears to be such a company, not only because it was founded by a former IDF officer in the military's central computing unit, but because its main investors include spies on "reserve duty" and venture capital firms linked to the Pollard scandal as well as the Bronfman and Maxwell families, both of whom have been tied to espionage and sexual blackmail scandals over the years.

Yet, as the Epstein scandal has recently indicated, major espionage scandals involving Israel receive little coverage and investigations into these events rarely lead anywhere. PROMIS was covered up largely thanks to Bill Barr during his first term as Attorney General and even the Pollard affair has all been swept under the rug with Donald Trump allowing Pollard to move to Israel and, more recently, pardoning the Israeli spy who recruited Pollard during his final day as President. Also under Trump, there was the discovery of "stingray" surveillance devices placed by Israel's government throughout Washington DC, including next to the White House, which were quickly memory holed and oddly not investigated by authorities. Israel had previously wiretapped the White House's phone lines during the Clinton years.

Another cover up is likely in the case of SolarWinds, particularly if the entry point was in fact Samanage. Though a cover up would certainly be more of the same, the SolarWinds case is different as major tech companies and cybersecurity firms with ties to US and Israeli intelligence now insist that Microsoft is soon to be targeted in what would clearly be a much more devastating event than SolarWinds due to the ubiquity of Microsoft's products.

On Tuesday, CIA-linked firm FireEye, which apparently has a leadership role in investigating the hack, claimed thatthe perpetrators are still gathering data from US government agencies and that "the hackers are moving into Microsoft 365 cloud applications from physical, on-premises servers," meaning that changes to fix Orion's vulnerabilities will not necessarily deny hacker access to previously compromised systems as they allegedly maintain access to those systems via Microsoft cloud applications. In addition to Microsoft's own claims that some of its source code was accessed by the hackers, this builds the narrative that Microsoft products are poised to be targeted in the next high-profile hack.

Microsoft's cloud security infrastructure, set to be the next target of the SolarWinds hackers, was largely developed and later managed by Assaf Rappaport, a former Unit 8200 officer who was most recently the head of Microsoft's Research and Development and Security teams at its massive Israel branch. Rappaport left Microsoft right before the COVID-19 crisis began last year to found a new cybersecurity company called Wiz.

Microsoft, like some of Samanage's main backers, is part of the World Economic Forum and is an enthusiastic supporter of and participant in the Great Reset agenda, so much so that Microsoft CEO Satya

Nadella wrote the foreword to Klaus Schwab's book "Shaping the Fourth Industrial Revolution." With the WEF simulating a cyber "pandemic" and both the WEF and Israel's head of Israel's National Cyber Directorate warning of an imminent "cyber winter", SolarWinds does indeed appear to be just the beginning, though perhaps a scripted one to create the foundation for something much more severe. A cyberattack on Microsoft products globally would certainly upend most of the global economy and likely have economic effects more severe than the COVID-19 crisis, just as the WEF has been warning. Yet, if such a hack does occur, it will inevitably serve the aims of the Great Reset to "reset" and then rebuild electronic infrastructure.

Chris Krebs cia Council For Inclusive Capitalism Crowdstrike Cyber Polygon FireEye hack israel Jonathan Pollard Marc Benioff microsoft Orion Russiagate Samanage Solarwinds Unit 8200 World Economic Forum

Author

Whitney Webb

Whitney Webb has been a professional writer, researcher and journalist since 2016. She has written for several websites and, from 2017 to 2020, was a staff writer and senior investigative reporter for Mint Press News. She currently writes for The Last American Vagabond.

18 comments

Donald says:
January 25, 2021 at 4:43 pm

After the admittance of a public official that the synagogues are often used to spy on the rest of us, I wonder if perhaps these types of sabatoges on our National Securities are actually covert operations by the United States and Israel in order to transfer Intelligence Information with denialibility. Seems to be an on-going problem with very few arrests and convictions. For instance Mr. Pollard wasn't picked up until he was warned by his handler that the Information he was stealing wasn't related to Israel. Interesting Article as are most.
Reply

Brad Solo says:

January 27, 2021 at 8:17 am

This is incredible!
Reply

Richard Perron says:
January 31, 2021 at 9:09 pm

Miss Webb is WOWSUM & like modern age Joan of Arc. A carbon copy of Mr. Assange in her own way. Another great whistle blower like Sibel Edmonds! Bravo to super journalism and not a member of the "Presstitute"
Reply

AVA says:
February 1, 2021 at 7:15 am

I have to agree with Brendan O'Connell that Israel needs to go. It is not a legitimate state and should not exist. It is just a historical extension and intensification of the role that international Jewish gangsterism has played throughout history — which is to plague the world with strife for their sole benefit. The masses of Trump supporters, who are in spirit, patriots, need to see your work. You've been tagging Israel the whole time, and these idiots have been convinced by nefarious actors like Alex Jones that China is attacking them. I would like to see WW dig up some stuff on how Israel is running China's moves. I am most certain they are. I don't think China is globally savvy in any way. They, like the US, are Israeli tools. We must all wake up because this sh*t is going so far south, we will have no world at all to rescue or speak up. Great work.
Reply

serenus says:
February 25, 2021 at 3:42 am

Do you remember the cartoon? Spy vs. Spy…..
Reply