



The Story Teller @IamTheStory__

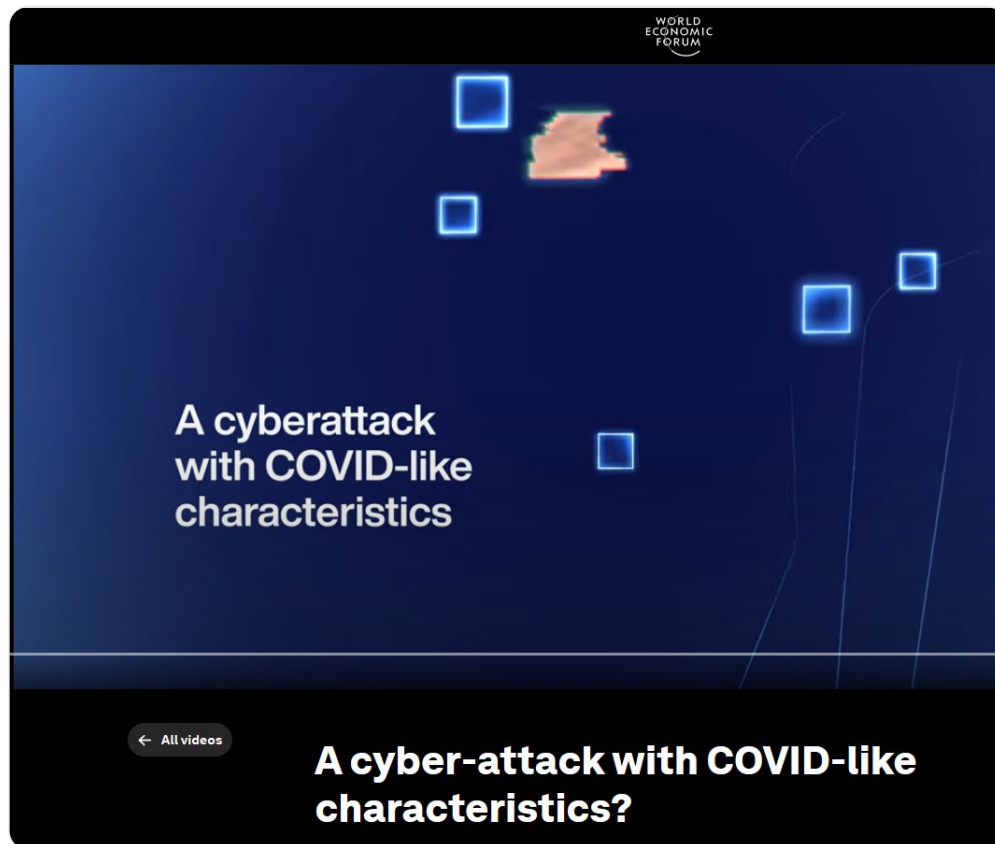
Jul 19, 2024 · 20 tweets · [IamTheStory__ /status/1814297871497249062](#)

CrowdStrike - The Deep state Backed Cyber security firm which led to Global IT Outage for Microsoft Windows OS based systems 📌

Do you think that CrowdStrike just updated a wrong endpoint update for Windows OS machines and brought down half of the world's IT systems?

Think again!!

Sometimes reality is more sinister than what it looks like!!





1. In late 2011, along with entrepreneur George Kurtz and Gregg Marston, Dmitri Alperovitch (Born in Russia) co-founded and became the chief technology officer of CrowdStrike, a security technology company focused on helping enterprises and governments protect their intellectual property and secrets against cyberespionage and cybercrime.

In 2015, CapitalG (formerly Google Capital), led a \$100 million capital drive for CrowdStrike. The firm brought on board senior FBI executives, such as Shawn Henry, former executive assistant director (EAD) of the FBI's Criminal, Cyber, Response and Services Branch, and Steve Chabinsky, former deputy assistant director of the FBI's Cyber Division. By May 2017, CrowdStrike had received \$256 million in funding from Warburg Pincus, Accel Partners, and Google Capital and its stock was valued at just under \$1 billion.

In June 2019, the company made an initial public offering (IPO) on the NASDAQ, which valued the company at over \$10 billion!!



SHAWN HENRY

CHIEF SECURITY OFFICER



Shawn Henry serves as chief security officer and is one of the company's longest tenured executive leaders, having joined in 2012 after retiring from the FBI senior executive service. Mr. Henry oversees all security aspects of CrowdStrike, including the company's information security, business continuity and resiliency, and risk reduction programs, as well as the physical security of CrowdStrike's global facilities, personnel, executive protection, and corporate events.

Having founded both CrowdStrike's security practice and its world-renowned incident response and professional services practice, Mr. Henry's legendary commitment to "One team. One Fight." resonates throughout the entire organization, unifying CrowdStrike's rapidly growing and geographically dispersed workforce.

Prior to joining CrowdStrike, Mr. Henry oversaw half of the FBI's investigative operations as Executive Assistant Director, including all FBI criminal and cyber investigations worldwide, international operations and the FBI's critical incident response to major investigations and disasters. He also managed compute crime investigations spanning the globe, established the National Cyber Investigative Joint Task Force, and received the Presidential Rank Award for Meritorious Executive for his leadership in enhancing the FBI's cyber capabilities.

Mr. Henry lectures at leading universities, serves on a number of strategic and advisory boards, and is a faculty member at the National Association of Corporate Directors. He serves as a keynote speaker at major cybersecurity conferences around the world and is regularly interviewed on cybersecurity issues by major broadcast, cable, online, and print media. Mr. Henry has been the recipient of multiple awards during his time at CrowdStrike, including the NACD Directorship 100, the Federal 100 Award as an impactful IT community leader, and the inaugural 2021 SC Award for Security Executive of the Year.



CARY DAVIS

MANAGING DIRECTOR, WARBURG PINCUS

Cary J. Davis is based in New York, joined Warburg Pincus in 1994 and is responsible for Technology investments in the Software and Financial Technology sectors. Prior to joining Warburg Pincus, Mr. Davis was an Executive Assistant to Michael Dell at Dell Computer and a Consultant at McKinsey & Company. He is a Director of Bitsight, Clearwater, eSentire, Infoblox, and Varo Bank, and previously served as a Director of Cyren. Mr. Davis is Chairman emeritus of the American Academy in Rome, a Director of the Andy Warhol Foundation and has been an adjunct Professor at the Columbia University Graduate School of Business, Chairman of the Jewish Community House of Bensonhurst and Chairman of the Boys Prep Charter School. Mr. Davis received a B.A. in Economics from Yale University and an MBA from Harvard Business School.





Steven Chabinsky

Steven Chabinsky serves as senior vice president of legal affairs and chief risk officer for **CrowdStrike**, where he advises the company on cyber, legal, privacy and reputation-related issues involving product development and execution.

Before joining the company, he served as deputy assistant director in the **FBI's** cyber division and led investigations, intelligence analysis, policy developments and outreach related to cyber attack, cyber espionage, online child exploitation and Internet fraud.

He has also served as chief of the **FBI's** cyber intelligence section, where he organized and led the **FBI's** analysis and reporting on terrorism, foreign intelligence and criminal matters related to cyber threats.

According to CrowdStrike, Chabinsky helped formulate the Homeland Security Act of 2002, the National Strategy to Secure Cyberspace in 2003 and National Security Presidential Directive 54 in 2008, which included the Comprehensive National Cybersecurity Initiative.

Between 2007 and 2009, Mr. Chabinsky served in the Office of the Director of National Intelligence in positions such as acting assistant deputy director of national intelligence for cyber, chairman of the National Cyber Study Group, and director of the Joint Interagency Cyber Task Force.

At ODNI, he was responsible for helping lead national intelligence efforts to coordinate, monitor and provide recommendations to the president on cyber strategy.

Chabinsky first joined the FBI in 1995 as an attorney in the Office of the General Counsel and initially focused on employment law and personnel litigation.

In 1998, he served as principal legal adviser to the National Infrastructure Protection Center and then in 2002 he assumed the senior counsel role in the FBI's cyber division.

The FBI says he helped expand the InfraGard program from 200 unvetted members in three cities to 500,000 vetted members in more than 85 cities.

InfraGard is a critical infrastructure partnership between the private sector, academia and government agencies.

Between 2002 and 2003, Chabinsky served in the White House's transition planning office to help create the Department of Homeland Security and oversaw legal matters associated with starting the department's information analysis and infrastructure protection directorate.

2. House Speaker Nancy Pelosi's husband, Paul Pelosi, has made over \$700,000 of unrealized gains in CrowdStrike stock!!

Nancy Pelosi the great US Congress Stock Trader is was on it again!!

Fox Business Flash top headlines for September 3

Check out what's clicking on FoxBusiness.com.

[House Speaker](#) Nancy Pelosi's husband is cashing in on his bet on [cybersecurity](#) firm CrowdStrike Holdings Inc.

Paul Pelosi, who runs a [real estate](#) and venture capital investment and consulting firm, purchased [5,000 CrowdStrike shares](#) on Sept. 3, 2020, according to regulatory filings.

[Shares](#) of the company, which closed at \$129.25 apiece on the day of Pelosi's purchase, have soared 111% over the past year, meaning he has a paper gain of more than \$700,000. The profit was first reported by [CongressTrading.com](#).

Ticker	Security	Last	Change	Change %
CRWD	CROWDSTRIKE HOLDINGS INC.	343.05	-11.89	-3.35%

Powered By

Paul Pelosi did not violate the STOCK Act unless he acted on nonpublic information. Members of Congress and their families are required to disclose any assets purchased or sold, the dates of such transactions and the dollar amount.

A spokesperson for Nancy Pelosi told FOX Business the House Speaker has never met with CrowdStrike officials regarding government business.

CrowdStrike was hired by the Democratic National Committee to look into the breach of its servers in 2016. The company blamed the incident on Russia but never handed its servers over to the FBI. The hack was used as part of the Trump-Russia collusion narrative that ultimately led to Robert Mueller's investigation and the first impeachment of former [President Donald Trump](#).

3. Dmitri Alperovitch, one of the founders of the CrowdStrike now runs a Washington DC Think Tank Silverado Policy Accelerator. One of the Chair of Silverado Policy Accelerator is General David Petraeus.

General David Petraeus is ex CIA chief, member of Bilderberg group (Rockefeller founded), Trilateral Commission (Rockefeller founded), Atlantic Council and Institute for the Study of War (Run by Kelly Kagan sister in law of Victoria Nuland).

General David Petraeus is now on the Board of KKR Holdings which is underwriter of the IPO of NXP as well a stakeholder in NXP. NXP is Netherlands based tech company which makes high end chips for various high end machines including missiles and Electronic Voting Machines (NXP Chips are used in India's EVMs also).

General David Petraeus (US Army, Ret.)

Partner, KKR and Chairman KKR Global Institute

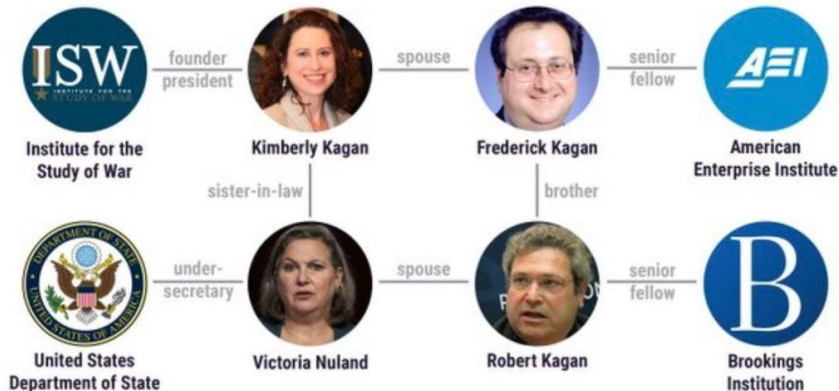
General David H. Petraeus (US Army, Ret.) is a Partner with the global investment firm KKR and Chairman of the KKR Global Institute, which he established in May 2013. He is also a member of the boards of directors of Optiv and FirstStream, a venture investor in more than 15 startups, and engaged in a variety of academic endeavors. Prior to joining KKR, General Petraeus served over 37 years in the U.S. military, culminating his career with six consecutive commands, five of which were in combat. Following retirement from the military and after Senate confirmation by a vote of 94-0, he served as Director of the CIA during a period of significant achievements in the global war on terror, the establishment of important Agency digital initiatives, and significant investments in the Agency's most important asset, its human capital. General Petraeus graduated with distinction from the U.S. Military Academy, and he is the only person in Army history to be the top graduate of both the demanding U.S. Army Ranger School and the U.S. Army's Command and General Staff College. He also earned a Ph.D. from Princeton University's School of Public and International Affairs. He is currently a Visiting Fellow at Yale University's Jackson Institute, Co-Chairman of the Global Advisory Council of the Woodrow Wilson Center for International Scholars, Senior Vice President of the Royal United Services Institute, and a Member of the Trilateral Commission, as well as a member of the boards of the Atlantic Council, the Institute for the Study of War, and over a dozen veterans service organizations. General Petraeus has earned numerous honors, awards, and decorations, including four Defense Distinguished Service Medals, the Bronze Star Medal for Valor, two NATO Meritorious Service Medals, the Combat Action Badge, the Ranger Tab, and Master Parachutist and Air Assault Badges. He has also been decorated by 13 foreign countries, and he is believed to be the only person who, while in uniform, threw out the first pitch of a World Series game and did the coin toss at a Super Bowl.

Honorary Chairs



**General David Petraeus
(US Army, Ret.)**

Partner, KKR and Chairman
KKR Global Institute



Our Board Members

General Jack Keane (US Army, Retired), *Chairman, Institute for the Study of War; President, GSI, LLC*

Dr. Kimberly Kagan, *Founder & President, Institute for the Study of War*

The Honorable Kelly Craft, *Former US Ambassador to UN and Canada*

Dr. William Kristol, *Director, Defending Democracy Together*

The Honorable Joseph I. Lieberman, *Senior Council, Kasowitz Benson Torres & Friedman, LLP*

Kevin Mandia, *Chief Executive Officer & Board Director, Mandiant*

Jack D. McCarthy, Jr., *Senior Managing Director & Founder, A&M Capital*

Bruce Mosler, *Chairman, Global Brokerage, Cushman & Wakefield, Inc.*


General David H. Petraeus (US Army, Retired), *Partner, KKR and Chairman, KKR Global Institute*

Dr. Warren Phillips, *Lead Director, CACI International*

Colonel William Roberti (US Army, Retired), *Managing Director, Alvarez & Marsal*

Hudson La Force, *former Chief Executive Officer of W. R. Grace & Co*


4. In 2016 US Democratic party's Democratic national council (DNC) hires CrowdStrike to investigate Russian meddling in the US Presidential elections which Hillary Clinton lost to Donald Trump. Agenda - To prepare a case against Donald Trump for his supposed collusion with Russian Govt. and Russian hackers to meddle in the US Presidential elections.



STATEMENT OF WORK

CROWDSTRIKE

This Statement of Work 1 ("SOW") is entered into by **CrowdStrike Services, Inc.** ("CrowdStrike") and **Perkins Coie LLP**, a limited liability partnership ("Firm"), with its principal place of business at 700 Thirteenth Street, NW, Washington, DC, 20005, and the **Democratic National Committee** ("Firm Client") (collectively, the "Parties") as of May 2, 2016 (the "SOW Effective Date") and forms a part of and is subject to the Master Services Agreement dated May 2, 2016 (the "Agreement") by and between: (i) CrowdStrike Services, Inc. and (ii) the Firm.



STATEMENT OF WORK

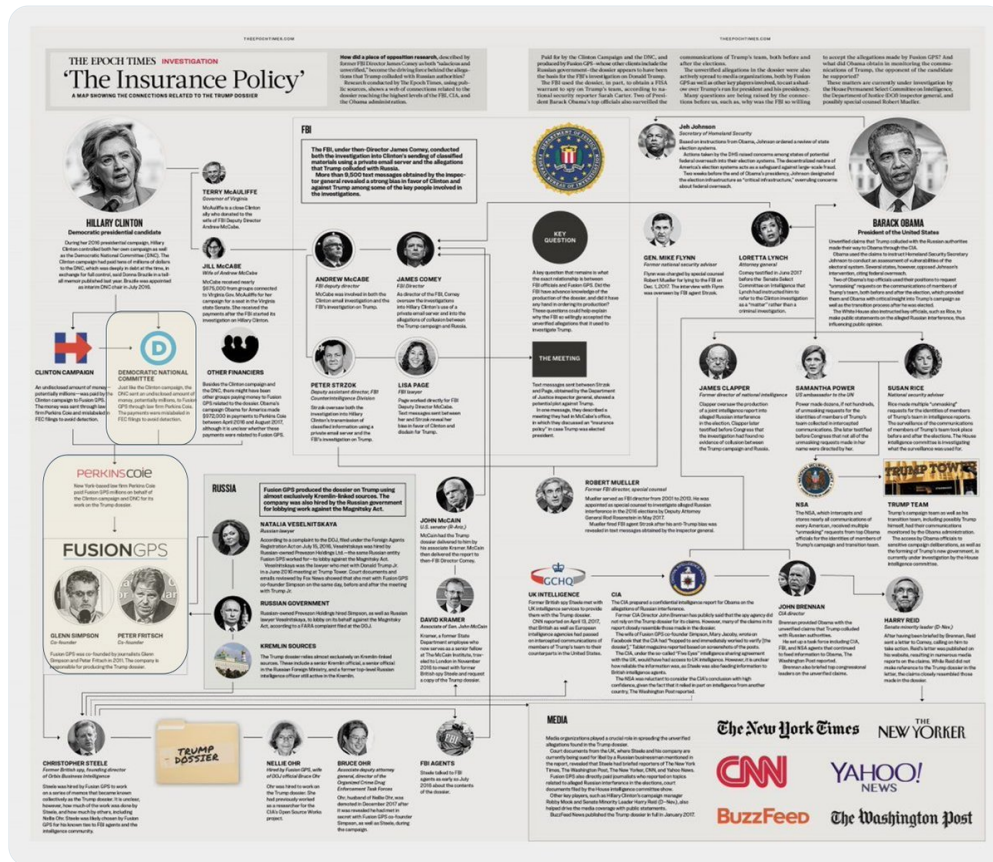
CROWDSTRIKE

This **Statement of Work 2** ("SOW") is entered into by **CrowdStrike Services, Inc.** ("CrowdStrike") and **Perkins Coie LLP**, a limited liability partnership ("Firm"), with its principal place of business at 700 Thirteenth Street, NW, Washington, DC, 20005, and the **Democratic Congressional Campaign Committee** ("Firm Client") (collectively, the "Parties") as of May 2, 2016 (the "SOW Effective Date") and forms a part of and is subject to the Master Services Agreement dated May 2, 2016 (the "Agreement") by and between: (i) CrowdStrike Services, Inc. and (ii) the Firm.

furtherance of his efforts with **SUSSMANN** and Campaign Lawyer-1 to disseminate allegations regarding Trump – Tech Executive-1 used his access at multiple organizations to gather and mine public and non-public Internet data regarding Trump and his associates, **with the goal of creating a "narrative" regarding the candidate's ties to Russia.**

5. Perkins Coie LLP hired CrowdStrike for services needed by the DNC and the DCCC. Sussman and his law firm, Perkins Coie, were essentially acting as the middlemen. At this point everybody in the "deep state" has gone all in on CREATING THE NARRATIVE that Trump is a Russian asset and they were trying to throw as much crap out there to "see what sticks."

They were fabricating evidence of Russian collusion through the dossier created by the CrowdStrike, Perkins



6. In nutshell

Michael Sussman is a former DOJ lawyer and former (as of 09/16/21) partner at Perkins Coie

Perkins Coie was the law firm representing the Hillary Clinton campaign and the DNC

Perkins Coie paid Fusion GPS to create the narrative that Trump was colluding with Russia

Separately, Michael Sussman, used "Tech Executive-1" from "Internet Company-1", which I believe are Shawn Henry and CrowdStrike, to create narrative regarding Trump's ties to Russia through the Alfa Bank story

Michael Sussman contracted CrowdStrike with the DNC for their cyber services for the DNC Hack

CrowdStrike used very shaky evidence to claim Russia hacked the DNC emails, again creating narrative of Trump's ties to Russia

A former NSA technical director studied the "hack" and claimed the DNC data was downloaded to a thumb drive

Multiple data points including Assange himself lead to a deeper story behind what happened with Seth Rich

CrowdStrike played an integral role in creating the narrative that Trump had ties to Russia.

Later in the Durham report which exonerated Donald Trump of any Russian collusion:

Crowdstrike Then President Shuan Henry an ex FBI Senior Staffer admitted that:

Shuan Henry: "We did not have concrete evidence that the data was exfiltrated from the DNC, but we have indicators that it was exfiltrated!!

Shaun Henry: "There are times when we can see data exfiltrated, and we can say conclusively. But in this case it appears it was set up to be exfiltrated, but we just don't have the evidence that says it actually left!!

Info Source:

0

<https://x.com/aaronjmate/status/1258572139504054274>

MR. SCHIFF: And, to the best of your recollection, when would that have been?

MR. HENRY: Counsel just reminded me that, as it relates to the DNC, we have indicators that data was exfiltrated. We did not have concrete evidence that data was exfiltrated from the DNC, but we have indicators that it was exfiltrated.

MR. SCHIFF: And the indicators that it was exfiltrated, when does it indicate that would have taken place?

MR. HENRY: Again, it's in the report. I believe -- I believe it was April of 2016. I'm confused on the date. I think it was April, but it's in the report.

MR. SCHIFF: It provides in the report on 2016, April 22nd, data staged for exfiltration by the Fancy Bear actor.

MR. HENRY: Yes, sir. So that, again, staged for, which, I mean, there's not -- the analogy I used with Mr. Stewart earlier was we don't have video of it happening, but there are indicators that it happened. There are times when we can see data exfiltrated, and we can say conclusively. But in this case, it appears it was set up to be exfiltrated, but we just don't have the evidence that says it actually left.

7. As usual a deep state funded and supported trash of newspaper Washington Post was used as a clickbait to announce that DNC server was hacked by Russian hackers.



Deep State Darling Ellen Nakashima: WaPo Writer Behind This Week's Trump-Grenell Fake News Hit Piece Was Also First to Report Russia Hacked the DNC in 2016

8. Meanwhile DCLeaks a hackers website supposedly based out of Russia had hacked George Soros Open Society Foundation database to download tons of documents about Soros's plans. On other hand Wikileaks announced that it is releasing emails from Hillary Clinton's private server!! This was the point where Hillary Clinton and Cabal linked DCLeaks, Wikileaks and Russian GRU for their supposed collusion to steal data and emails from the DNC server to help Donald Trump got elected as the president of the united states.

In fact, the report contains crucial gaps in the evidence that might support that authoritative account. Here is how it describes the core crime under investigation, the alleged GRU theft of DNC emails:

Between approximately May 25, 2016 and June 1, 2016, GRU officers accessed the DNC's mail server from a GRU-controlled computer leased inside the United States. During these connections, Unit 26165 officers *appear* to have stolen thousands of emails and attachments, which were later released by WikiLeaks in July 2016. [*Italics added for emphasis.*]

The GRU also stole documents from the DNC network shortly after gaining access. On April 22, 2016, the GRU copied files from the DNC network to GRU-controlled computers. Stolen documents included the DNC's opposition research into candidate Trump.¹³⁴ Between approximately May 25, 2016 and June 1, 2016, GRU officers accessed the DNC's mail server from a GRU-controlled computer leased inside the United States.¹³⁵ During these connections,

Unit 26165 officers **appear** to have stolen thousands of emails and attachments, which were later released by WikiLeaks in July 2016.¹³⁶

Mueller Report, March 2019, p. 41.

The report's use of that one word, "appear," undercuts its suggestions that Mueller possesses convincing evidence that GRU officers stole "thousands of emails and attachments" from DNC servers. It is a departure from the language used in his **July 2018 indictment**, which contained no such qualifier:

But a close examination of the report shows that none of those headline assertions are supported by the report's evidence or other publicly available sources. They are further undercut by investigative shortcomings and the conflicts of interest of key players involved:

- The report uses qualified and vague language to describe key events, indicating that Mueller and his investigators **do not actually know for certain whether Russian intelligence officers stole Democratic Party emails**, or how those emails were transferred to WikiLeaks.
- The report's timeline of events appears to defy logic. According to its narrative, WikiLeaks founder Julian Assange announced the publication of Democratic Party emails not only before he received the documents but before he even communicated with the source that provided them.
- There is strong reason to doubt Mueller's suggestion that an alleged Russian cutout called Guccifer 2.0 supplied the stolen emails to Assange.
- Mueller's decision not to interview Assange – a central figure who claims Russia was not behind the hack – suggests an unwillingness to explore avenues of evidence on fundamental questions.
- U.S. intelligence officials cannot make definitive conclusions about the hacking of the Democratic National Committee computer servers because **they did not analyze those servers themselves**. Instead, **they relied on the forensics of CrowdStrike, a private contractor for the DNC that was not a neutral party**, much as “Russian dossier” compiler Christopher Steele, also a DNC contractor, was not a neutral party. This puts two Democrat-hired contractors squarely behind underlying allegations in the affair – a key circumstance that Mueller ignores.
- Further, **the government allowed CrowdStrike and the Democratic Party's legal counsel to submit redacted records, meaning CrowdStrike and not the government decided what could be revealed or not regarding evidence of hacking**.

9. All this circus was denounced by Durham report to prove that there was no Russian collusion with Donald Trump and there was no Russian meddling in the US elections.

But in the 2020 elections Democrats used Arabella Advisors, largest leftist dark money peddling non profit which went full steam ahead to help Joe Biden defeat Donald Trump to become the President of the United states.

The Arabella Advisors pumped in millions of dollars of dark money into DNC (Democratic National Council) to help Joe Biden.

https://x.com/lamTheStory_/status/1627769512903966721

10. All this democratic circus takes us back to World economic forum and Klaus Schwab.

In his 2020 book, “COVID-19: The Great Reset.” Dr. Klaus Schwab of the WEF (World Economic Forum) and the “depopulation” Club of Rome confirms that mortality from COVID-19 is less than 0.006%.

Now as i said earlier he prophesized that next will be a Cyber Pandemic similar to the Covid pandemic.

0

Now you can stitch up the sequence:

World Economic Forum + Klaus Schwab + Bill Gates + Obama and Clintons + Club of Rome +
Rockefellers + Warburg Pincus + Arabella Advisors + George Soros + FBI + US Democrats

None of them want Trump to get elected as the President of the US, because he would just destroy
climate crisis, LGBTQ, BLM type deep state propagandas and that is exactly what worries deep state to
the core!!

They all colluded to create this narrative and who was the tool for creating this narrative?

OfCourse deep state digital darling - CrowdStrike !!

A cyber-attack with COVID-like characteristics?

The World Economic Forum is an independent international organization
committed to improving the state of the world by engaging business, political,
academic and other leaders of society to shape glo...

<https://www.weforum.org/videos/a-cyber-attack-with-covid-like-characteristics/>



familiarity become more natural. As social and physical distancing persist, relying more on digital platforms to communicate, or work, or seek advice, or order something will, little by little, gain ground on formerly ingrained habits. In addition, the pros and cons of online versus offline will be under constant scrutiny through a variety of lenses. If health considerations become paramount, we may decide, for example, that a cycling class in front of a screen at home doesn't match the conviviality and fun of doing it with a group in a live class but is in fact safer (and cheaper!). The same reasoning applies to many different domains like flying to a meeting (Zoom is safer, cheaper, greener and much more convenient), driving to a distant family gathering for the weekend (the WhatsApp family group is not as fun but, again, safer, cheaper and greener) or even attending an academic course (not as fulfilling, but cheaper and more convenient).

1.6.1.2. The regulator

This transition towards more digital "of everything" in our professional and personal lives will also be supported and accelerated by regulators. To date governments have often slowed the pace of adoption of new technologies by lengthy ponderings about what the best regulatory framework should look like but, as the example of telemedicine and drone delivery is now showing, a dramatic acceleration forced by necessity is possible. During the lockdowns, a quasi-global relaxation of regulations that had previously hampered progress in domains where the technology had been available for years suddenly happened because there was no better or other choice available. What was until recently unthinkable suddenly became possible, and we can be certain that neither those patients who experienced how easy and convenient telemedicine was nor the regulators who made it possible will want to see it go into reverse. New regulations will stay in place. In the same vein, a similar story is unfolding in the US with the Federal Aviation Authority, but also in other countries, related to fast-tracking regulation pertaining to drone delivery. The current imperative to propel, no matter what, the "contactless economy" and the subsequent willingness of regulators to speed it up means that there are no holds barred. What is true for until-recently sensitive domains like telemedicine and drone delivery is also true for more mundane and well-covered regulatory fields, like mobile payments. Just to provide a bare example, in the midst of the lockdown (in April 2020), European banking regulators decided to increase the amount that shoppers could pay using their mobile devices while also reducing the authentication requirements that made it previously difficult to make payments using platforms like PayPal or Venmo. Such moves will only accelerate the digital "prevalence" in our daily lives, albeit not without contingent cybersecurity issues.

1.6.1.3. The firm

In one form or another, social- and physical-distancing measures are likely to persist after the pandemic itself subsides, justifying the decision in many companies from different industries to accelerate automation. After a while, the enduring concerns about technological unemployment will recede as societies emphasize the restriction towards more tech and more digital. There is an additional phenomenon set to support the expansion of automation: when "economic distancing" might follow social distancing. As countries turn inward and global companies shorten their super-efficient but highly fragile supply chains, automation and robots that enable more local production, while keeping costs down, will be in great demand.

The process of automation was set in motion many years ago, but the critical issue once again relates to the accelerating pace of change and transition: the pandemic will fast-forward the adoption of

automation in the workplace and the introduction of more robots in our personal and professional lives. From the onset of the lockdowns, it became apparent that robots and AI were a "natural" alternative when human labour was not available. Furthermore, they were used whenever possible to reduce the health risks to human employees. At a time when physical distancing became an obligation, robots were deployed in places as different as warehouses, supermarkets and hospitals in a broad range of activities, from shelf scanning (an area in which AI has made tremendous forays) to cleaning and of course robotic delivery – a soon-to-be important component of healthcare supply chains that will in turn lead to the "contactless" delivery of groceries and other essentials. As for many other technologies that were on the distant horizon in terms of adoption (like telemedicine), businesses, consumers and public authorities are now rushing to turbocharge the speed of adoption. In cities as varied as Hangzhou, Washington DC and Tel Aviv, efforts are under way to move from pilot programmes to large-scale operations capable of putting an army of delivery robots on the road and in the air. Chinese e-commerce giants like Alibaba and JD.com are confident that, in the coming 12-18 months, autonomous delivery could become widespread in China – much earlier than anticipated prior to the pandemic.

Maximum attention is often focused on industrial robots as they are the most visible face of automation, but radical acceleration is also coming in workplace automation via software and machine learning. So-called Robotic Process Automation (RPA) makes businesses more efficient by installing computer software that rivals and replaces the actions of a human worker. This can take multiple forms, ranging from Microsoft's finance group consolidating and simplifying disparate reports, tools and content into an automated, role-based personalized portal, to an oil company installing software that sends pictures of a pipeline to an AI engine, to compare the pictures with an existing database and alert the relevant employees to potential problems. In all cases, RPA helps to reduce the time spent compiling and validating data, and therefore cuts costs (at the expense of a likely increase in unemployment, as mentioned in the "Economic reset" section). During the peak of the pandemic, RPA won its spurs by proving its efficiency at handling surges in volume; thus, ratiified, in the post-pandemic era the process will be rolled out and fine-tuned. Two examples prove this point: RPA solutions helped some hospitals to disseminate COVID-19 test results, saving nurses as much as three hours' work per day. In a similar vein, an AI digit device normally used to respond to customer requests online was adapted to help medical digital platforms screen patients online for COVID-19 symptoms. For all these reasons, Bain & Company (consultancy) estimates that the number of companies implementing this automation of business processes will double over the next two years, a timeline that the pandemic may shorten still further.¹²⁴¹

1.6.2. Contact tracing, contact tracking and surveillance

An important lesson can be learned from the countries that were more effective in dealing with the pandemic (in particular Asian nations): technology in general and digital in particular help. Successful contact tracing proved to be a key component of a successful strategy against COVID-19. While lockdowns are effective at reducing the reproduction of the coronavirus, they don't eliminate the threat posed by the pandemic. In addition, they come at injuriously high economic and societal cost. It will be very hard to fight COVID-19 without an effective treatment or a vaccine and, until then, the most effective way to curtail or stop transmission of the virus is by widespread testing followed by the isolation of cases, contact tracing and the quarantines of people exposed to the people infected. As will be seen below, in this process technology can be a formidable shortcut, allowing public-health officials to identify infected people very rapidly, thus containing an outbreak before it starts to spread.

Contact tracing and tracking are therefore essential components of our public-health response to COVID-19. Both terms are often used interchangeably, yet they have slightly different meanings. A tracking app gains insights in real time by, for example, determining a person's current location through geodata via GPS coordinates or radio cell location. By contrast, tracing consists in gaining insights in retrospect, like identifying physical contacts between people using Bluetooth. Neither offer a miracle solution that can stop in its entirety the spread of the pandemic, but they make it possible to almost immediately sound the alarm, permitting early intervention, thus limiting or containing the outbreak, particularly when it occurs in super-spreading environments (like a community or family gathering). For

reasons of convenience and ease of reading, we'll merge the two and will use them interchangeably (as articles in the press often do).

The most effective form of tracking or tracing is obviously the one powered by technology: it not only allows backtracking all the contacts with whom the user of a mobile phone has been in touch, but also tracking the user's real-time movements, which in turn affords the possibility to better enforce a lockdown and to warn other mobile users in the proximity of the carrier that they have been exposed to someone infected.

It comes as no surprise that digital tracing has become one of the most sensitive issues in terms of public health, raising acute concerns about privacy around the world. In the early phases of the pandemic, many countries (mostly in East Asia but also others like Israel) decided to implement digital tracing under different forms. They shifted from the retroactive tracing of chains of past contagion to the real-time tracking of movements in order to confine a person infected by COVID-19 and to enforce subsequent quarantines or partial lockdowns. From the outset, China, Hong Kong SAR and South Korea implemented coercive and intrusive measures of digital tracing. They took the decision to track individuals without their consent, through their mobile and credit card data, and even employed video surveillance (in South Korea). In addition, some countries required the mandatory wearing of electronic bracelets for travel arrivals and people in quarantine (in Hong Kong SAR) to alert those individuals susceptible of being infected. Others opted for "middle-ground" solutions, where individuals placed in quarantine are equipped with a mobile phone to monitor their location and be publicly identified should they breach the rules.

The digital tracing solution most lauded and talked about was the TraceTogether app run by Singapore's Ministry of Health. It seems to offer the "ideal" balance between efficiency and privacy concerns by keeping user data on the phone rather than on a server, and by assigning the login anonymously. The contact detection only works with the latest versions of Bluetooth (an obvious limitation in many less digitally advanced countries where a large percentage of mobiles do not have sufficient Bluetooth capability for effective detection). Bluetooth identifies the user's physical contacts with another user of the application accurately to within about two metres and, if a risk of COVID-19 transmission is incurred, the app will warn the contact, at which point the transmission of stored data to the ministry of health becomes mandatory (but the contact's anonymity is maintained). TraceTogether is therefore non-intrusive in terms of privacy, and its code, available in open source, makes it usable by any country anywhere in the world, yet privacy advocates object that there are still risks. If the entire population of a country downloaded the application, and if there were a sharp increase in COVID-19 infections, then the app could end up identifying most citizens. Cyber intrusions, issues of trust in the operator of the system and the timing of data retention pose additional privacy concerns.

Other options exist. These are mainly related to the availability of open and verifiable source codes, and to guarantees pertaining to data supervision and the length of conservation. Common standards and norms could be adopted, particularly in the EU where many citizens fear that the pandemic will force a trade-off between privacy and health. But as Margrethe Vestager, the EU Commissioner for Competition observed:

I think that is a false dilemma, because you can do so many things with technology that are not invasive of your privacy. I think that, very often, when people say it's only double in one way, it's because they want the data for their own purposes. We have made a set of guidelines, and with member states we have translated that into a toolbox, so that you can do a voluntary app with decentralized storage, with Bluetooth technology. You can use technology to track the virus, but you can still give people the freedom of choice, and, in doing that, people must trust that the technology is for virus tracking and not for any other purposes. I think it is essential that we show that we really mean it when we say that you should be able to trust technology when you use it, that this is not a start of a new era of surveillance. This is for virus tracking, and this can help us open our societies.¹²⁴²

Again, we want to emphasize that this is a fast-moving and highly volatile situation. The announcement made in April by Apple and Google that they are collaborating to develop an app that health officials could use to reverse-engineer the movements and connections of a person infected by the virus points to a possible way out for societies most concerned about data privacy and that fear digital surveillance above anything else. The person who carries the mobile would have to voluntarily download the app and would have to agree to share the data, and the two companies made it clear that their technology would not be provided to public-health agencies that do not abide by their privacy guidelines. But voluntary contact-tracing apps have a problem: they do preserve the privacy of their users but are only effective when the level of participation is sufficiently high – a collective-action problem that underlines once again the profoundly interconnected nature of modern life beneath the individualist façade of rights and contractual obligations. No voluntary contact-tracing app will work if people are unwilling to provide their own personal data to the governmental agency that monitors the system; if any individual refuses to download the app (and therefore to withhold information about a possible infection, movements and contacts), everyone will be adversely affected. In the end, citizens will only use the app if they regard it as trustworthy, which is itself dependent upon trust in the government and public authorities. At the end of June 2020, the experience with tracing apps was recent and mixed. Fewer than 30 countries had put them in place.¹²⁴³ In Europe, some countries like Germany and Italy rolled out apps based on the system developed by Apple and Google, while other countries, like France, decided to develop their own app, raising issues of interoperability. In general, technical problems and concerns with privacy seem to affect the app's use and rate of adoption. Just to offer some examples: the UK, following technical glitches and criticism from privacy activists, made a U-turn and decided to replace its domestically-developed contact-tracing app with the model offered by Apple and Google. Norway suspended the use of its app due to privacy concerns while, in France, just three weeks after being launched, the StopCovid app had simply failed to take off, with a very low rate of adoption (1.9 million people) followed by frequent decisions to uninstall it.

Today, about 5.2 billion smartphones exist in the world, each with the potential to help identify who is infected, where and often by whom. This unprecedented opportunity may explain why different surveys conducted in the US and Europe during their lockdowns indicated that a growing number of citizens seemed to favour smartphone tracking from public authorities (within very specific boundaries). But as always, the devil is in the detail of the policy and its execution. Questions like whether the digital tracking should be mandatory or voluntary, whether the data should be collected on an anonymized or personal basis and whether the information should be collected privately or publicly disclosed contain many different shades of black and white, making it exceedingly difficult to agree upon a unified model of digital tracing in a collective fashion. All these questions, and the unease they can provoke, were exacerbated by the rise of corporations tracking employees' health that emerged in the early phases of national reopenings. They will continuously grow in relevance as the corona pandemic lingers on and fears about other possible pandemics surface.

As the coronavirus crisis recedes and people start returning to the workplace, the corporate move will be towards greater surveillance; for better or for worse, companies will be watching and sometimes recording what their workforce does. The trend could take many different forms, from measuring body temperatures with thermal cameras to monitoring via an app how employees comply with social distancing. This is bound to raise profound regulatory and privacy issues, which many companies will reject by arguing that, unless they increase digital surveillance, they won't be able to reopen and function without risking new infections (and being, in some cases, liable). They will cite health and safety as justification for increased surveillance.

The perennial concern expressed by legislators, academics and trade unionists is that the surveillance tools are likely to remain in place after the crisis and even when a vaccine is finally found, simply because employers don't have any incentive to remove a surveillance system once it's been installed, particularly if one of the indirect benefits of surveillance is to check on employees' productivity.

This is what happened after the terrorist attacks of 11 September 2001. All around the world, new

CLIMATE ACTION


At Davos, Trump urges the world to ignore the 'prophets of doom'



Jan 21, 2020

11. Finally let's check the ownership of the CrowdStrike.

Where there is Blackrock

There are 1000s of shock !!

Who owns CrowdStrike Holdings? CRWD Stock Ownership 

[About featured snippets](#)  

People also ask :

Who are the investors in CrowdStrike?

Top Institutional Holders

Holder	Shares	Value
Blackrock Inc.	16.13M	5,725,434,956
Vanguard Group Inc	16.06M	5,700,833,355
Morgan Stanley	5.79M	2,053,611,156
Jennison Associates LLC	5.03M	1,785,269,060

[6 more rows](#)

Footnote-







Follow

Silverado Policy Accelerator

@SilveradoPolicy

A bipartisan nonprofit organization dedicated to advancing American prosperity and global competitiveness in the 21st century. Podcast: [@GeopolDecanted](#)

📍 Washington, D.C. [🌐 silverado.org](https://silverado.org)

📅 Joined February 2020

307 Following **3,162** Followers

Footnote:

Gregg Marston co-founded CrowdStrike



George Kurtz: CEO & Founder CrowdStrike



Footnote:

A great and simplified technical analysis of how CrowdStrike messed up a simple end point patch!!



Zach Vorhies / Google Whistleblower
 @Perpetualmaniac · Follow



Crowdstrike Analysis:

It was a NULL pointer from the memory unsafe C++ language.

Since I am a professional C++ programmer, let me decode this stack trace dump for you.

```

EXCEPTION_RECORD: fffffb0d18d3ec28 -- (.exr 0xfffffb0d18d3ec28)
ExceptionAddress: fffff8021df335a1 (csagent+0x00000000000e35a1)
ExceptionCode: c0000005 (Access violation)
ExceptionFlags: 00000000
NumberParameters: 2
  Parameter[0]: 0000000000000000
  Parameter[1]: 000000000000009c
Attempt to read from address 000000000000009c

CONTEXT: fffffb0d18d3e460 -- (.cxr 0xfffffb0d18d3e460)
rax=fffffb0d18d3f2b0 rbx=0000000000000000 rcx=0000000000000003
rdx=fffffb0d18d3f280 rsi=ffff9a81b59ef9a4 rdi=ffff9a81b59ef05c
rip=ffff8021df335a1 rsp=fffffb0d18d3ee60 rbp=fffffb0d18d3ef60
r8=000000000000009c r9=0000000000000000 r10=0000000000000000
r11=0000000000000014 r12=fffffb0d18d3ef28 r13=fffffb0d18d3f0d0
r14=000000000000001a r15=0000000000000004
nopl=0          nv up es pl nz na po nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00050206
csagent+0xe35a1
ffff8021df335a1 45b08          mov     r9d,dword ptr [r8] ds:002b:00000000'0000009c-????????
Resetting default scope

BLACKBOXBSD: 1 (!blackboxbsd)
BLACKBOXNTFS: 1 (!blackboxntfs)
BLACKBOXWFP: 1 (!blackboxwfp)
BLACKBOXWINLOGON: 1
PROCESS_NAME: System
READ_ADDRESS: 000000000000009c
ERROR_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%p referenced memory at 0x%p. The memory could not
EXCEPTION_CODE_STR: c0000005
EXCEPTION_PARAMETER1: 0000000000000000
EXCEPTION_PARAMETER2: 000000000000009c
EXCEPTION_STR: 0xc0000005

STACK_TEXT
fffffb0d18d3ee60 fffff8021df09152 : 00000000'00000000 00000000'e01f008d fffffb0d18d3f202 fffff8021e
fffffb0d18d3f000 fffff8021df0a3e9 : 00000000'00000000 00000000'00000010 00000000'00000000 fffff8a1b5
fffffb0d18d3f130 fffff8021e1494f4 : 00000000'00000000 00000000'00000000 00000000'00000000 00000000'00
fffffb0d18d3f260 fffff8021e145d9b : fffff8a1'93735280 fffffb0d18d3f5d0 00000000'00000000 00000000'00
fffffb0d18d3f4d0 fffff8021deb8fd0 : 00000000'000030f1 fffffb0d18d3f790 fffff8a1'992cbb30 fffff809'b7
  
```

7:08 PM · Jul 19, 2024

91.9K Reply Copy link

[Read 2.8K replies](#)

Foot note:

Seth Rich was cited by Julian Assange and Wikileaks as their source of DNC Dump of Hillary Clinton emails.

The murder of Seth Rich occurred on July 10, 2016, at 4:20 a.m. in the Bloomingdale neighborhood of Washington, D.C. Rich died about an hour and a half after being shot twice in the back. The perpetrators were never apprehended; police suspected he had been the victim of an attempted robbery.





Footnote: The interview which changed the destiny of the US forever!!

In August 2016, Assange gave a TV interview with a Dutch TV program. WikiLeaks had published thousands of stolen DNC emails, throwing the presidential race into chaos and leading to the resignations of top officials at the Democratic National Committee, including Chairwoman Rep. Debbie Wasserman Schultz (D-Fla.).

In the Dutch TV interview, Assange demurred on how he obtained the DNC emails, then dropped a tantalizing hint. “There’s a 27-year-old who works for the DNC who was shot in the back, murdered, just a few weeks ago, for unknown reasons as he was walking down the street in Washington.”



<https://www.youtube.com/embed/Kp7FkLBRpKg>

Footnote:

Here is that Julian Assange interview



<https://www.youtube.com/embed/Kp7FkLBRpKg>

Footnote:

Strangely family declined yonbelieve what Assange said and sued media outlets including Fox news for private settlement to redact the name of Seth Ritch from any of DNC Email hack stories swirling around!!

For them and Democrats everything was a conspiracy theory when it came to the murder of Seth Ritch.

Fox News Settles With Seth Rich's Parents For False Story Claiming Clinton Leaks

NOVEMBER 24, 2020 · 6:05 PM ET



David Folkenflik



People pass the News Corporation headquarters building and Fox News studios in New York.

Richard Drew/AP

The Fox News Channel has reached a private settlement with the parents of the slain Democratic National Committee staffer Seth Rich. The network had baselessly reported in May 2017 that Rich leaked thousands of Democratic party emails to Wikileaks during the height of the 2016 presidential campaign.

...