CN Radio—Episode 3: Gareth Porter on DHS Deception & Bi-Partisan Fear of Revolt

The DHS deceptively pushed the story that Russia hacked U.S. voter databases; and both Democratic & Republican elites fear popular revolt against their failed polices but refuse to change, as Gareth Porter explains.

The guest on Episode 3 of Consortium News Radio is Gareth Porter, a long time contributor to Consortium News. Gareth is an independent investigative journalist and historian who has been studying the national security state for nearly two decades and is the author of two books on the subject: *Perils of Dominance* on the U.S. going to war in Vietnam and *Manufactured Crisis*, on the false narrative about the Iranian nuclear program.

Gareth speaks about two of his articles recently published on Consortium News. The first is an original piece about how the Department of Homeland Security Created a Deceptive Tale of Russia Hacking US Voter Sites. The second story was originally published on Truthout. We gave it the title: The Establishment's Bi-Partisan Fear of Popular Revolt.

The runtime is 23 minutes and 46 seconds. The episode is also available as a podcast on Consortium's podcast page.

And now Gareth Porter on Consortium News Radio:

If you enjoyed this original interview please consider making a donation to Consortium News so we can bring you more stories like this one.

How the Department of Homeland Security Created a Deceptive Tale of Russia Hacking US Voter Sites

The narrative about Russian cyberattacks on American election infrastructure is a self-interested abuse of power by DHS based on distortion of evidence, writes Gareth Porter.

By Gareth Porter
Special to Consortium News

The narrative of Russian intelligence attacking state and local election boards and threatening the integrity of U.S. elections has achieved near-universal acceptance by media and political elites. And now it has been accepted by the Trump administration's intelligence chief, Dan Coats, as well.

But the real story behind that narrative, recounted here for the first time, reveals that the Department of Homeland Security (DHS) created and nurtured an account that was grossly and deliberately deceptive.

DHS compiled an intelligence report suggesting hackers linked to the Russian government *could* have targeted voter-related websites in many states and then leaked a sensational story of Russian attacks on those sites without the qualifications that would have revealed a different story. When state election officials began asking questions, they discovered that the DHS claims were false and, in at least one case, laughable.

The National Security Agency and special counsel Robert Mueller's investigating team have also claimed evidence that Russian military intelligence was behind election infrastructure hacking, but on closer examination, those claims turn out to be speculative and misleading as well. Mueller's indictment of 12 GRU military intelligence officers does not cite any violations of U.S. election laws though it claims Russia interfered with the 2016 election.

A Sensational Story

On Sept. 29, 2016, a few weeks after the hacking of election-related websites in Illinois and Arizona, ABC News carried a sensational headline: "Russian Hackers Targeted Nearly Half of States' Voter Registration Systems, Successfully Infiltrated 4." The story itself reported that "more than 20 state election systems" had been hacked, and four states had been "breached" by hackers suspected of working for the Russian government. The story cited only sources "knowledgeable" about the matter, indicating that those who were pushing the story were eager to hide the institutional origins of the information.

Behind that sensational story was a federal agency seeking to establish its leadership within the national security state apparatus on cybersecurity, despite its limited resources for such responsibility. In late summer and fall 2016, the Department of Homeland Security was maneuvering politically to designate state and local voter registration databases and voting systems as "critical infrastructure." Such a designation would make voter-related networks and websites under the protection a "priority sub-sector" in the DHS "National Infrastructure Protection Plan, which already included 16 such sub-sectors.

DHS Secretary Jeh Johnson and other senior DHS officials consulted with many state election officials in the hope of getting their approval for such a designation. Meanwhile, the DHS was finishing an intelligence report that would both highlight the Russian threat to U.S. election infrastructure and the role DHS could play in protecting it, thus creating political impetus to the designation. But several secretaries of state—the officials in charge of the election infrastructure in their state—strongly opposed the designation that Johnson wanted.

On Jan. 6, 2017—the same day three intelligence agencies released a joint "assessment" on Russian interference in the election—Johnson announced the designation anyway.

Media stories continued to reflect the official assumption that cyber attacks on state election websites were Russian-sponsored. Stunningly, *The Wall Street Journal* reported in December 2016 that DHS was itself behind hacking attempts of Georgia's election database.

The facts surrounding the two actual breaches of state websites in Illinois and Arizona, as well as the broader context of cyberattacks on state websites, didn't support that premise at all.

In July, Illinois discovered an intrusion into its voter registration website and the theft of personal information on as many as 200,000 registered voters. (The 2018 Mueller indictments of GRU officers would unaccountably put the figure at 500,000.) Significantly, however, the hackers only had copied the information and had left it unchanged in

the database.

That was a crucial clue to the motive behind the hack. DHS Assistant Secretary for Cyber Security and Communications Andy Ozment told a Congressional committee in late September 2016 that the fact hackers hadn't tampered with the voter data indicated that the aim of the theft was not to influence the electoral process. Instead, it was "possibly for the purpose of selling personal information." Ozment was contradicting the line that already was being taken on the Illinois and Arizona hacks by the National Protection and Programs Directorate and other senior DHS officials.

In an interview with me last year, Ken Menzel, the legal adviser to the Illinois secretary of state, confirmed what Ozment had testified. "Hackers have been trying constantly to get into it since 2006," Menzel said, adding that they had been probing every other official Illinois database with such personal data for vulnerabilities as well. "Every governmental database—driver's licenses, health care, you name it—has people trying to get into it," said Menzel.

In the other successful cyberattack on an electoral website, hackers had acquired the username and password for the voter database Arizona used during the summer, as Arizona Secretary of State Michele Reagan learned from the FBI. But the reason that it had become known, according to Reagan in an interview with Mother Jones, was that the login and password had shown up for sale on the dark web—the network of websites used by cyber criminals to sell stolen data and other illicit wares.

Furthermore, the FBI had told her that the effort to penetrate the database was the work of a "known hacker" whom the FBI had monitored "frequently" in the past. Thus, there were reasons to believe that both Illinois and Arizona hacking incidents were linked to criminal hackers seeking information they could sell for profit.

Meanwhile, the FBI was unable to come up with any theory about what Russia might have intended to do with voter registration data such as what was taken in the Illinois hack. When FBI Counterintelligence official Bill Priestap was asked in a June 2017 hearing how Moscow

might use such data, his answer revealed that he had no clue: “They took the data to understand what it consisted of,” said the struggling Priestap, “so they can affect better understanding and plan accordingly in regards to possibly impacting future elections by knowing what is there and studying it.”

The inability to think of any plausible way for the Russian government to use such data explains why DHS and the intelligence community adopted the argument, as senior DHS officials Samuel Liles and Jeanette Manfra put it, that the hacks “could be intended or used to undermine public confidence in electoral processes and potentially the outcome.” But such a strategy could not have had any effect without a decision by DHS and the U.S. intelligence community to assert publicly that the intrusions and other scanning and probing were Russian operations, despite the absence of hard evidence. So DHS and other agencies were consciously sowing public doubts about U.S. elections that they were attributing to Russia.

DHS Reveals Its Self-Serving Methodology

In June 2017, Liles and Manfra testified to the Senate Intelligence Committee that an October 2016 DHS intelligence report had listed election systems in 21 states that were “potentially targeted by Russian government cyber actors.” They revealed that the sensational story leaked to the press in late September 2016 had been based on a draft of the DHS report. And more importantly, their use of the phrase “potentially targeted” showed that they were arguing only that the cyber incidents it listed were *possible* indications of a Russian attack on election infrastructure.

Furthermore, Liles and Manfra said the DHS report had “catalogued suspicious activity we observed on state government networks across the country,” which had been “largely based on suspected malicious tactics and infrastructure.” They were referring to a list of eight IP addresses an August 2016 FBI “flash alert” had obtained from the Illinois and Arizona intrusions, which DHS and FBI had not been able to attribute to the Russian government.

The DHS officials recalled that the DHS began to “receive reports of

cyber-enabled scanning and probing of election-related infrastructure in some states, some of which appeared to originate from servers operated by a Russian company." Six of the eight IP addresses in the FBI alert were indeed traced to King Servers, owned by a young Russian living in Siberia. But as DHS cyber specialists knew well, the country of ownership of the server doesn't prove anything about who was responsible for hacking: As cybersecurity expert Jeffrey Carr pointed out, the Russian hackers who coordinated the Russian attack on Georgian government websites in 2008 used a Texas-based company as the hosting provider.

The cybersecurity firm ThreatConnect noted in 2016 that one of the other two IP addresses had hosted a Russian criminal market for five months in 2015. But that was not a serious indicator, either. Private IP addresses are reassigned frequently by server companies, so there is not a necessary connection between users of the same IP address at different times.

The DHS methodology of selecting reports of cyber incidents involving election-related websites as "potentially targeted" by Russian government-sponsored hackers was based on no objective evidence whatever. The resulting list appears to have included any one of the eight addresses as well as any attack or "scan" on a public website that could be linked in any way to elections.

This methodology conveniently ignored the fact that criminal hackers were constantly trying to get access to every database in those same state, country and municipal systems. Not only for Illinois and Arizona officials, but state electoral officials.

In fact, 14 of the 21 states on the list experienced nothing more than the routine scanning that occurs every day, according to the Senate Intelligence Committee. Only six involved what was referred to as a "malicious access attempt," meaning an effort to penetrate the site. One of them was in Ohio, where the attempt to find a weakness lasted less than a second and was considered by DHS's internet security contractor a "non-event" at the time.

State Officials Force DHS to Tell the Truth

For a year, DHS did not inform the 21 states on its list that their election boards or other election-related sites had been attacked in a presumed Russian-sponsored operation. The excuse DHS officials cited was that it could not reveal such sensitive intelligence to state officials without security clearances. But the reluctance to reveal the details about each case was certainly related to the reasonable expectation that states would publicly challenge their claims, creating a potential serious embarrassment.

On Sept. 22, 2017, DHS notified 21 states about the cyber incidents that had been included in the October 2016 report. The public announcement of the notifications said DHS had notified each chief election officer of "any potential targeting we were aware of in their state leading up to the 2016 election." The phrase "potential targeting" again telegraphed the broad and vague criterion DHS had adopted, but it was ignored in media stories.

But the notifications, which took the form of phone calls lasting only a few minutes, provided a minimum of information and failed to convey the significant qualification that DHS was only suggesting targeting as a possibility. "It was a couple of guys from DHS reading from a script," recalled one state election official who asked not to be identified. "They said [our state] was targeted by Russian government cyber actors."

A number of state election officials recognized that this information conflicted with what they knew. And if they complained, they got a more accurate picture from DHS. After Wisconsin Secretary of State Michael Haas demanded further clarification, he got an email response from a DHS official with a different account. "[B]ased on our external analysis," the official wrote, "the WI [Wisconsin] IP address affected belongs to the WI Department of Workforce Development, not the Elections Commission."

California Secretary of State Alex Padilla said DHS initially had notified his office "that Russian cyber actors 'scanned' California's Internet-facing systems in 2016, including Secretary of State websites." But under further questioning, DHS admitted to Padilla that

what the hackers had targeted was the California Department of Technology's network.

Texas Secretary of State Rolando Pablos and Oklahoma Election Board spokesman Byron Dean also denied that any state website with voter- or election-related information had been targeted, and Pablos demanded that DHS "correct its erroneous notification."

Despite these embarrassing admissions, a statement issued by DHS spokesman Scott McConnell on Sept. 28, 2017 said the DHS "stood by" its assessment that 21 states "were the target of Russian government cyber actors seeking vulnerabilities and access to U.S. election infrastructure." The statement retreated from the previous admission that the notifications involved "potential targeting," but it also revealed for the first time that DHS had defined "targeting" very broadly indeed.

It said the category included "some cases" involving "direct scanning of targeted systems" but also cases in which "malicious actors scanned for vulnerabilities in networks that may be connected to those systems or have similar characteristics in order to gain information about how to later penetrate their target."

It is true that hackers may scan one website in the hope of learning something that could be useful for penetrating another website, as cybersecurity expert Prof. Herbert S. Lin of Stanford University explained to me in an interview. But including any incident in which that motive was theoretical meant that any state website could be included on the DHS list, without any evidence it was related to a political motive.

Arizona's further exchanges with DHS revealed just how far DHS had gone in exploiting that escape clause in order to add more states to its "targeted" list. Arizona Secretary of State Michele Reagan tweeted that DHS had informed her that "the Russian government targeted our voter registration systems in 2016." After meeting with DHS officials in early October 2017, however, Reagan wrote in a blog post that DHS "could not confirm that any attempted Russian government hack occurred whatsoever to any election-related system in Arizona, much less the

statewide voter registration database."

What the DHS said in that meeting, as Reagan's spokesman Matt Roberts recounted to me, is even more shocking. "When we pressed DHS on what exactly was actually targeted, they said it was the Phoenix public library's computers system," Roberts recalled.

In April 2018, a CBS News "60 Minutes" segment reported that the October 2016 DHS intelligence report had included the Russian government hacking of a "county database in Arizona." Responding to that CBS report, an unidentified "senior Trump administration official" who was well-briefed on the DHS report told Reuters that "media reports" on the issue had sometimes "conflated criminal hacking with Russian government activity," and that the cyberattack on the target in Arizona "was not perpetrated by the Russian government."

NSA Finds a GRU Election Plot

NSA intelligence analysts claimed in a May 2017 analysis to have documented an effort by Russian military intelligence (GRU) to hack into U.S. electoral institutions. In an intelligence analysis obtained by *The Intercept* and reported in June 2017, NSA analysts wrote that the GRU had sent a spear-phishing email—one with an attachment designed to look exactly like one from a trusted institution but that contains malware design to get control of the computer—to a vendor of voting machine technology in Florida. The hackers then designed a fake web page that looked like that of the vendor. They sent it to a list of 122 email addresses NSA believed to be local government organizations that probably were "involved in the management of voter registration systems." The objective of the new spear-phishing campaign, the NSA suggested, was to get control of their computers through malware to carry out the exfiltration of voter-related data.

But the authors of *The Intercept* story failed to notice crucial details in the NSA report that should have tipped them off that the attribution of the spear-phishing campaign to the GRU was based merely on the analysts' own judgment—and that their judgment was faulty.

The Intercept article included a color-coded chart from the original

NSA report that provides crucial information missing from the text of the NSA analysis itself as well as *The Intercept*'s account. The chart clearly distinguishes between the elements of the NSA's account of the alleged Russian scheme that were based on "Confirmed Information" (shown in green) and those that were based on "Analyst Judgment" (shown in yellow). The connection between the "operator" of the spear-phishing campaign the report describes and an unidentified entity confirmed to be under the authority of the GRU is shown as a yellow line, meaning that it is based on "Analyst Judgment" and labeled "probably."

A major criterion for any attribution of a hacking incident is whether there are strong similarities to previous hacks identified with a specific actor. But the chart concedes that "several characteristics" of the campaign depicted in the report distinguish it from "another major GRU spear-phishing program," the identity of which has been redacted from the report.

The NSA chart refers to evidence that the same operator also had launched spear-phishing campaigns on other web-based mail applications, including the Russian company "Mail.ru." Those targets suggest that the actors were more likely Russian criminal hackers rather than Russian military intelligence.

Even more damaging to its case, the NSA reports that the same operator who had sent the spear-phishing emails also had sent a test email to the "American Samoa Election Office." Criminal hackers could have been interested in personal information from the database associated with that office. But the idea that Russian military intelligence was planning to hack the voter rolls in American Samoa, an unincorporated U.S. territory with 56,000 inhabitants who can't even vote in U.S. presidential elections, is plainly risible.

The Mueller Indictment's Sleight of Hand

The Mueller indictment of GRU officers released on July 13 appeared at first reading to offer new evidence of Russian government responsibility for the hacking of Illinois and other state voter-related websites. A close analysis of the relevant paragraphs,

however, confirms the lack of any real intelligence supporting that claim.

Mueller accused two GRU officers of working with unidentified “co-conspirators” on those hacks. But the only alleged evidence linking the GRU to the operators in the hacking incidents is the claim that a GRU official named Anatoly Kovalev and “co-conspirators” deleted search history related to the preparation for the hack after the FBI issued its alert on the hacking identifying the IP address associated with it in August 2016.

A careful reading of the relevant paragraphs shows that the claim is spurious. The first sentence in Paragraph 71 says that both Kovalev and his “co-conspirators” researched domains used by U.S. state boards of elections and other entities “for website vulnerabilities.” The second says Kovalev and “co-conspirators” had searched for “state political party email addresses, including filtered queries for email addresses listed on state Republican Party websites.”

Searching for website vulnerabilities would be evidence of intent to hack them, of course, but searching Republican Party websites for email addresses is hardly evidence of any hacking plan. And Paragraph 74 states that Kovalev “deleted his search history”—not the search histories of any “co-conspirator”—thus revealing that there were no joint searches and suggesting that the subject Kovalev had searched was Republican Party emails. So any deletion by Kovalev of his search history after the FBI alert would not be evidence of his involvement in the hacking of the Illinois election board website.

With this rhetorical misdirection unraveled, it becomes clear that the repetition in every paragraph of the section of the phrase “Kovalev and his co-conspirators” was aimed at giving the reader the impression the accusation is based on hard intelligence about possible collusion that doesn’t exist.

The Need for Critical Scrutiny of DHS Cyberattack Claims

The DHS campaign to establish its role as the protector of U.S. electoral institutions is not the only case in which that agency has

used a devious means to sow fear of Russian cyberattacks. In December 2016, DHS and the FBI published a long list of IP addresses as indicators of possible Russian cyberattacks. But most of the addresses on the list had no connection with Russian intelligence, as former U.S. government cyber-warfare officer Rob Lee found on close examination.

When someone at the Burlington, Vt., Electric Company spotted one of those IP addresses on one of its computers, the company reported it to DHS. But instead of quietly investigating the address to verify that it was indeed an indicator of Russian intrusion, DHS immediately informed *The Washington Post.* The result was a sensational story that Russian hackers had penetrated the U.S. power grid. In fact, the IP address in question was merely Yahoo's email server, as Rob Lee told me, and the computer had not even been connected to the power grid. The threat to the power grid was a tall tale created by a DHS official, which the Post had to embarrassingly retract.

Since May 2017, DHS, in partnership with the FBI, has begun an even more ambitious campaign to focus public attention on what it says are Russian "targeting" and "intrusions" into "major, high value assets that operate components of our Nation's critical infrastructure", including energy, nuclear, water, aviation and critical manufacturing sectors. Any evidence of such an intrusion must be taken seriously by the U.S. government and reported by news media. But in light of the DHS record on alleged threats to election infrastructure and the Burlington power grid, and its well-known ambition to assume leadership over cyber protection, the public interest demands that the news media examine DHS claims about Russian cyber threats far more critically than they have up to now.

Gareth Porter is an independent investigative journalist and winner of the 2012 Gellhorn Prize for journalism. His latest book is *Manufactured Crisis: The Untold Story of the Iran Nuclear Scare*.

Foisting Blame for Cyber-hacking on Russia

Exclusive: Cyber-criminal efforts to hack into U.S. government databases are epidemic, but this ugly reality is now being exploited to foist blame on Russia and fuel the New Cold War hysteria, reports Gareth Porter.

By Gareth Porter

Recent hearings by the Senate and House Intelligence Committees reflected the rising tide of Russian-election-hacking hysteria and contributed further to it. Both Democrats and Republicans on the two committees appeared to share the alarmist assumptions about Russian hacking, and the officials who testified did nothing to discourage the politicians.

On June 21, Samuel Liles, acting director of the Intelligence and Analysis Office's Cyber Division at the Department of Homeland Security, and Jeanette Manfra, acting deputy under secretary for cyber-security and communications, provided the main story line for the day in testimony before the Senate committee – that efforts to hack into election databases had been found in 21 states.

Former DHS Secretary Jeh Johnson and FBI counter-intelligence chief Bill Priestap also endorsed the narrative of Russian government responsibility for the intrusions on voter registration databases.

But none of those who testified offered any evidence to support this suspicion nor were they pushed to do so. And beneath the seemingly unanimous embrace of that narrative lies a very different story.

The Department of Homeland Security (DHS) has a record of spreading false stories about alleged Russian hacking into U.S. infrastructure, such as the tale of a Russian intrusion into the Burlington, Vermont electrical utility in December 2016 that DHS later admitted was untrue. There was another bogus DHS story about Russia hacking into a Springfield, Illinois water pump in November 2011.

So, there's a pattern here. Plus, investigators, assessing the notion that Russia hacked into state electoral databases, rejected that suspicion as false months ago. Last September, Assistant Secretary of DHS for Cybersecurity Andy Ozment and state officials explained that the intrusions were not carried out by Russian intelligence but by criminal hackers seeking personal information to

sell on the Internet.

Both Ozment and state officials responsible for the state databases revealed that those databases have been the object of attempted intrusions for years. The FBI provided information to at least one state official indicating that the culprits in the hacking of the state's voter registration database were cyber-criminals.

Illinois is the one state where hackers succeeded in breaking into a voter registration database last summer. The crucial fact about the Illinois hacking, however, was that the hackers extracted personal information on roughly 90,000 registered voters, and that none of the information was expunged or altered.

The Actions of Cybercriminals

That was an obvious clue to the motive behind the hack. Assistant DHS Secretary Ozment testified before the House Subcommittee on Information Technology on Sept. 28 (at 01:02.30 of the video) that the apparent interest of the hackers in copying the data suggested that the hacking was "possibly for the purpose of selling personal information."

Ozment 's testimony provides the only credible motive for the large number of states found to have experienced what the intelligence community has called "scanning and probing" of computers to gain access to their electoral databases: the personal information involved – even e-mail addresses – is commercially valuable to the cybercriminal underworld.

That same testimony also explains why so many more states reported evidence of attempts to hack their electoral databases last summer and fall. After hackers had gone after the Illinois and Arizona databases, Ozment said, DHS had provided assistance to many states in detecting attempts to hack their voter registration and other databases.

"Any time you more carefully monitor a system you're going to see more bad guys poking and prodding at it," he observed, "*because they're always poking and prodding.*" [Emphasis added]

State election officials have confirmed Ozment's observation. Ken Menzel, the general counsel for the Illinois Secretary of State, told this writer, "What's new about what happened last year is not that someone tried to get into our system but that they finally succeeded in getting in." Menzel said hackers "have been trying constantly to get into it since 2006."

And it's not just state voter registration databases that cybercriminals are after, according to Menzel. "Every governmental data base – driver's licenses,

health care, you name it – has people trying to get into it," he said.

Arizona Secretary of State Michele Reagan told Mother Jones that her I.T. specialists had detected 193,000 distinct attempts to get into the state's website in September 2016 alone and 11,000 appeared to be trying to "do harm."

Reagan further revealed that she had learned from the FBI that hackers had gotten a user name and password for their electoral database, and that it was being sold on the "dark web" – an encrypted network used by cyber criminals to buy and sell their wares. In fact, she said, the FBI told her that the probe of Arizona's database was the work of a "known hacker" who had been closely monitored "frequently."

James Comey's Role

The sequence of events indicates that the main person behind the narrative of Russian hacking state election databases from the beginning was former FBI Director James Comey. In testimony to the House Judiciary Committee on Sept. 28, Comey suggested that the Russian government was behind efforts to penetrate voter databases, but never said so directly.

Comey told the committee that FBI Counterintelligence was working to "understand just what mischief Russia is up to with regard to our elections." Then he referred to "a variety of scanning activities" and "attempted intrusions" into election-related computers "beyond what we knew about in July and August," encouraging the inference that it had been done by Russian agents.

The media then suddenly found unnamed sources ready to accuse Russia of hacking election data even while admitting that they lacked evidence. The day after Comey's testimony ABC headlined, "Russia Hacking Targeted Nearly Half of States' Voter Registration Systems, Successfully Infiltrating 4." The story itself revealed, however, that it was merely a suspicion held by "knowledgeable" sources.

Similarly, NBC News headline announced, "Russians Hacked Two U.S. Voter Databases, Officials Say." But those who actually read the story closely learned that in fact none of the unnamed sources it cited were actually attributing the hacking to the Russians.

It didn't take long for Democrats to turn the Comey teaser – and these anonymously sourced stories with misleading headlines about Russian database hacking – into an established fact. A few days later, the ranking Democrat on the House Intelligence Committee, Rep. Adam Schiff declared that there was "no doubt" Russia was behind the hacks on state electoral databases.

On Oct. 7, DHS and the Office of the Director of National Intelligence issued a joint statement that they were "not in a position to attribute this activity to the Russian government." But only a few weeks later, DHS participated with FBI in issuing a "Joint Analysis Report" on "Russian malicious cyber activity" that did not refer directly to scanning and spearphishing aimed of state electoral databases but attributed all hacks related to the election to "actors likely associated with RIS [Russian Intelligence Services]."

Suspect Claims

But that claim of a "likely" link between the hackers and Russia was not only speculative but highly suspect. The authors of the DHS-ODNI report claimed the link was "supported by technical indicators from the U.S. intelligence community, DHS, FBI, the private sector and other entities." They cited a list of hundreds of I.P. addresses and other such "indicators" used by hackers they called "Grizzly Steppe" who were supposedly linked to Russian intelligence.

But as I reported last January, the staff of Dragos Security, whose CEO Rob Lee, had been the architect of a U.S. government system for defense against cyber attack, pointed out that the vast majority of those indicators would certainly have produced "false positives."

Then, on Jan. 6 came the "intelligence community assessment" – produced by selected analysts from CIA, FBI and National Security Agency and devoted almost entirely to the hacking of e-mail of the Democratic National Committee and Hillary Clinton's campaign chairman John Podesta. But it included a statement that "Russian intelligence obtained and maintained access to elements of multiple state or local election boards." Still, no evidence was evinced on this alleged link between the hackers and Russian intelligence.

Over the following months, the narrative of hacked voter registration databases receded into the background as the drumbeat of media accounts about contacts between figures associated with the Trump campaign and Russians built to a crescendo, albeit without any actual evidence of collusion regarding the e-mail disclosures.

But a June 5 story brought the voter-data story back into the headlines. The story, published by The Intercept, accepted at face value an NSA report dated May 5, 2017, that asserted Russia's military intelligence agency, the GRU, had carried out a spear-phishing attack on a U.S. company providing election-related software and had sent e-mails with a malware-carrying word document to 122 addresses believed to be local government organizations.

But the highly classified NSA report made no reference to any evidence

supporting such an attribution. The absence of any hint of signals intelligence supporting its conclusion makes it clear that the NSA report was based on nothing more than the same kind of inconclusive “indicators” that had been used to establish the original narrative of Russians hacking electoral databases.

A Checkered History

So, the history of the U.S. government’s claim that Russian intelligence hacked into election databases reveals it to be a clear case of politically motivated analysis by the DHS and the Intelligence Community. Not only was the claim based on nothing more than inherently inconclusive technical indicators but no credible motive for Russian intelligence wanting personal information on registered voters was ever suggested.

Russian intelligence certainly has an interest in acquiring intelligence related to the likely outcome of American elections, but it would make no sense for Russia’s spies to acquire personal voting information about 90,000 registered voters in Illinois.

When FBI Counter-intelligence chief Priestap was asked at the June 21 hearing how Moscow might use such personal data, his tortured effort at an explanation clearly indicated that he was totally unprepared to answer the question.

“They took the data to understand what it consisted of,” said Priestap, “so they can affect better understanding and plan accordingly in regards to possibly impacting future election by knowing what is there and studying it.”

In contrast to that befuddled non-explanation, there is highly credible evidence that the FBI was well aware that the actual hackers in the cases of both Illinois and Arizona were motivated by the hope of personal gain.

Gareth Porter is an independent investigative journalist and winner of the 2012 Gellhorn Prize for journalism. He is the author of the newly published *Manufactured Crisis: The Untold Story of the Iran Nuclear Scare.*

Mainstream Media’s Russian Bogeymen

Exclusive: The mainstream hysteria over Russia has led to dubious or downright false stories that have deepened the New Cold War, as Gareth Porter notes regarding last month’s bogus tale of a hack into the U.S. electric grid.

By Gareth Porter

In the middle of a major domestic crisis over the U.S. charge that Russia had interfered with the U.S. election, the Department of Homeland Security (DHS) triggered a brief national media hysteria by creating and spreading a bogus story of Russian hacking into U.S. power infrastructure.

DHS had initiated the now-discredited tale of a hacked computer at the Burlington, Vermont Electricity Department by sending the utility's managers misleading and alarming information, then leaked a story they certainly knew to be false and continued to put out a misleading line to the media.

Even more shocking, however, DHS had previously circulated a similar bogus story of Russian hacking of a Springfield, Illinois water pump in November 2011.

The story of how DHS twice circulated false stories of Russian efforts to sabotage U.S. "critical infrastructure" is a cautionary tale of how senior leaders in a bureaucracy-on-the-make take advantage of every major political development to advance its own interests, with scant regard for the truth.

The DHS had carried out a major public campaign to focus on an alleged Russian threat to U.S. power infrastructure in early 2016. The campaign took advantage of a U.S. accusation of a Russian cyber-attack against the Ukrainian power infrastructure in December 2015 to promote one of the agency's major functions – guarding against cyber-attacks on America's infrastructure.

Beginning in late March 2016, DHS and FBI conducted a series of 12 unclassified briefings for electric power infrastructure companies in eight cities titled, "Ukraine Cyber Attack: implications for U.S. stakeholders." The DHS declared publicly, "These events represent one of the first known physical impacts to critical infrastructure which resulted from cyber-attack."

That statement conveniently avoided mentioning that the first cases of such destruction of national infrastructure from cyber-attacks were not against the United States, but were inflicted on Iran by the Obama administration and Israel in 2009 and 2012.

Beginning in October 2016, the DHS emerged as one of the two most important players – along with the CIA—in the political drama over the alleged Russian effort to tilt the 2016 election toward Donald Trump. Then on Dec. 29, DHS and FBI distributed a "Joint Analysis Report" to U.S. power utilities across the country with what it claimed were "indicators" of a Russian intelligence effort to penetrate and compromise U.S. computer networks, including networks related to the presidential election, that it called "GRIZZLY STEPPE."

The report clearly conveyed to the utilities that the “tools and infrastructure” it said had been used by Russian intelligence agencies to affect the election were a direct threat to them as well. However, according to Robert M. Lee, the founder and CEO of the cyber-security company Dragos, who had developed one of the earliest U.S. government programs for defense against cyber-attacks on U.S. infrastructure systems, the report was certain to mislead the recipients.

“Anyone who uses it would think they were being impacted by Russian operations,” said Lee. “We ran through the indicators in the report and found that a high percentage were false positives.”

Lee and his staff found only two of a long list of malware files that could be linked to Russian hackers without more specific data about timing. Similarly a large proportion of IP addresses listed could be linked to “GRIZZLY STEPPE” only for certain specific dates, which were not provided.

The Intercept discovered, in fact, that 42 percent of the 876 IP addresses listed in the report as having been used by Russian hackers were exit nodes for the Tor Project, a system that allows bloggers, journalists and others – including some military entities – to keep their Internet communications private.

Lee said the DHS staff that worked on the technical information in the report is highly competent, but the document was rendered useless when officials classified and deleted some key parts of the report and added other material that shouldn’t have been in it. He believes the DHS issued the report “for a political purpose,” which was to “show that the DHS is protecting you.”

Planting the Story, Keeping it Alive

Upon receiving the DHS-FBI report the Burlington Electric Company network security team immediately ran searches of its computer logs using the lists of IP addresses it had been provided. When one of IP addresses cited in the report as an indicator of Russian hacking was found on the logs, the utility immediately called DHS to inform it as it had been instructed to do by DHS.

In fact, the IP address on the Burlington Electric Company’s computer was simply the Yahoo e-mail server, according to Lee, so it could not have been a legitimate indicator of an attempted cyber-intrusion. That should have been the end of the story. But the utility did not track down the IP address before reporting it to DHS. It did, however, expect DHS to treat the matter confidentially until it had thoroughly investigated and resolved the issue.

“DHS wasn’t supposed to release the details,” said Lee. “Everybody was supposed to keep their mouth shut.”

Instead, a DHS official called The Washington Post and passed on word that one of the indicators of Russian hacking of the DNC had been found on the Burlington utility's computer network. The Post failed to follow the most basic rule of journalism, relying on its DHS source instead of checking with the Burlington Electric Department first. The result was the Post's sensational Dec. 30 story under the headline "Russian hackers penetrated U.S. electricity grid through a utility in Vermont, U.S. officials say."

DHS official evidently had allowed the Post to infer that the Russians hack had penetrated the grid without actually saying so. The Post story said the Russians "had not actively used the code to disrupt operations of the utility, according to officials who spoke on condition of anonymity in order to discuss a security matter," but then added, and that "the penetration of the nation's electrical grid is significant because it represents a potentially serious vulnerability."

The electric company quickly issued a firm denial that the computer in question was connected to the power grid. The Post was forced to retract, in effect, its claim that the electricity grid had been hacked by the Russians. But it stuck by its story that the utility had been the victim of a Russian hack for another three days before admitting that no such evidence of a hack existed.

The day after the story was published, the DHS leadership continued to imply, without saying so explicitly, that the Burlington utility had been hacked by Russians. Assistant Secretary for Pubic Affairs J. Todd Breasseale gave CNN a statement that the "indicators" from the malicious software found on the computer at Burlington Electric were a "match" for those on the DNC computers.

As soon as DHS checked the IP address, however, it knew that it was a Yahoo cloud server and therefore not an indicator that the same team that allegedly hacked the DNC had gotten into the Burlington utility's laptop. DHS also learned from the utility that the laptop in question had been infected by malware called "neutrino," which had never been used in "GRIZZLY STEPPE."

Only days later did the DHS reveal those crucial facts to the Post. And the DHS was still defending its joint report to the Post, according to Lee, who got part of the story from Post sources. The DHS official was arguing that it had "led to a discovery," he said. "The second is, 'See, this is encouraging people to run indicators.'"

Original DHS False Hacking Story

The false Burlington Electric hack scare is reminiscent of an earlier story of Russian hacking of a utility for which the DHS was responsible as well. In November 2011, it reported an "intrusion" into a Springfield, Illinois water

district computer that similarly turned out to be a fabrication.

Like the Burlington fiasco, the false report was preceded by a DHS claim that U.S. infrastructure systems were already under attack. In October 2011, acting DHS deputy undersecretary Greg Schaffer was quoted by The Washington Post as warning that “our adversaries” are “knocking on the doors of these systems.” And Schaffer added, “In some cases, there have been intrusions.” He did not specify when, where or by whom, and no such prior intrusions have ever been documented.

On Nov. 8, 2011, a water pump belonging to the Curran-Gardner township water district near Springfield, Illinois, burned out after sputtering several times in previous months. The repair team brought in to fix it found a Russian IP address on its log from five months earlier. That IP address was actually from a cell phone call from the contractor who had set up the control system for the pump and who was vacationing in Russia with his family, so his name was in the log by the address.

Without investigating the IP address itself, the utility reported the IP address and the breakdown of the water pump to the Environmental Protection Agency, which in turn passed it on to the Illinois Statewide Terrorism and Intelligence Center, also called a fusion center composed of Illinois State Police and representatives from the FBI, DHS and other government agencies.

On Nov. 10 – just two days after the initial report to EPA – the fusion center produced a report titled “Public Water District Cyber Intrusion” suggesting a Russian hacker had stolen the identity of someone authorized to use the computer and had hacked into the control system causing the water pump to fail.

The contractor whose name was on the log next to the IP address later told Wired magazine that one phone call to him would have laid the matter to rest. But the DHS, which was the lead in putting the report out, had not bothered to make even that one obvious phone call before opining that it must have been a Russian hack.

The fusion center “intelligence report,” circulated by DHS Office of Intelligence and Research, was picked up by a cyber-security blogger, who called The Washington Post and read the item to a reporter. Thus the Post published the first sensational story of a Russian hack into a U.S. infrastructure on Nov. 18, 2011.

After the real story came out, DHS disclaimed responsibility for the report, saying that it was the fusion center’s responsibility. But a Senate subcommittee investigation revealed in a report a year later that even after the initial report had been discredited, DHS had not issued any retraction or correction to

the report, nor had it notified the recipients about the truth.

DHS officials responsible for the false report told Senate investigators such reports weren't intended to be "finished intelligence," implying that the bar for accuracy of the information didn't have to be very high. They even claimed that report was a "success" because it had done what "what it's supposed to do – generate interest."

Both the Burlington and Curran-Gardner episodes underline a central reality of the political game of national security in the New Cold War era: major bureaucratic players like DHS have a huge political stake in public perceptions of a Russian threat, and whenever the opportunity arises to do so, they will exploit it.

Gareth Porter is an independent investigative journalist and winner of the 2012 Gellhorn Prize for journalism. He is the author of the newly published *Manufactured Crisis: The Untold Story of the Iran Nuclear Scare.*

Fretting the Wrong Entry Program

Politicians are scoring points with a frightened U.S. population by hyping the supposed danger of letting in up to 10,000 Syrian refugees, but a much greater or actual risk exists in the current gaps in a visa-waiver program, write Coleen Rowley and Georgianne Nienaber. (Clarification added on Dec. 18, 2015.)

By Coleen Rowley and Georgianne Nienaber

All the hyped political angst regarding the possible resettling of a few thousand Syrian refugees stands in stark contrast to the relative lack of congressional concern about the equally, if not more inherently problematic Visa Waiver Program (VWP). This longstanding, historically-proven dangerous, but little understood Department of Homeland Security (DHS)-administered program, allowed 21,231,396 foreign visitors from 38 countries to pass through U.S. ports of entry with minimal to no screening according to 2013 official records (the most recent data published).

The numbers should give pause, since visitors admitted ***each year*** via the VWP are over ***2,000 times greater*** than the "up to 10,000" Syrian refugees proposed a few months ago by President Barack Obama for eventual resettlement in the U.S. The number of VWP entrants is nearly ***20,000 times greater*** than the 1,300 Syrians previously allowed into the U.S. since the conflict began over four years ago. The VWP program allows 300 times more foreign visitors into the U.S. than

refugees from all countries combined.

Of those entering under the VWP: 293,217 came from Belgium; 1,804,035 from France; and 512,299 from Sweden. Even before the more recent "Charlie Hebdo" and Nov. 13 attacks in Paris, it was known that the United Kingdom, France, Belgium and Sweden were emerging as home bases for Islamic extremists joining the Islamic State (also known as ISIL, ISIS or Daesh). So do these countries, among others in the waiver program, offer potentially easy access to the United States for some of their increasingly radicalized citizens now supporting known terrorist organizations?

What We Know and Don't Know

We suggested last year that the United States has a gaping hole in its DHS and Immigration and Customs Enforcement (ICE) monitoring. There had been little public discussion of the VWP, a program that 38 countries currently participate in. Participating countries agree to loosen travel restrictions in order to encourage tourism, trade and business travel.

Before traveling to the U.S. by sea or air, VWP participants must fill out an Electronic System for Travel Authorization (ESTA) form online. It costs a modest $14 and assumes that the applicant is telling the truth about previous visa denials and run-ins with the law.

Since November 2014, new information, including additional passport data, contact information, and potential names or aliases, is required. Once the applicant has the ESTA application completed, he/she needs no other paperwork other than a valid passport from one of the participating countries.

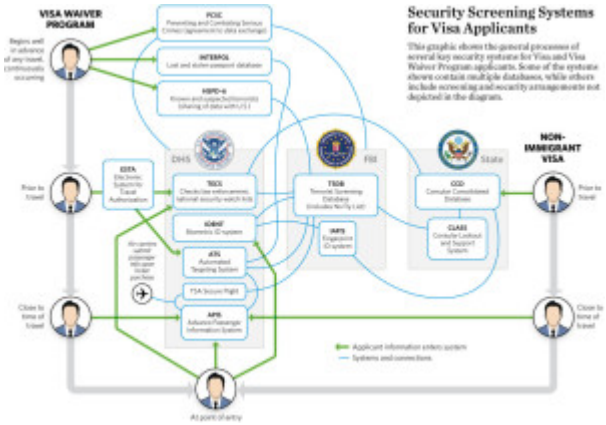
"Upon landing in the U.S.," according to the optimistic March 2015 testimony of the Director of the Heritage Foundation Steven P. Bucci, "individuals must provide biographic and biometric information that is checked against additional sets of biometric databases controlled by DHS (Automated Biometric Identification System or IDENT) and the FBI (Integrated Automated Fingerprint Identification System or IAFIS). The individual is once again checked through TECS, the ATS, and the APIS and undergoes additional inspection if necessary. At any point in this process, security officials can prevent an individual from entering the U.S. if they are deemed a security risk or ineligible for travel to the U.S."

Testifying before the Subcommittee on Border and Maritime Security, Committee on Homeland Security, in the U.S. House of Representatives, Bucci made it sound like a "robust screening process" but what we don't know, what is critically missing from his rosy prognosis, is how many of the over 1.1 million terrorist

suspects that have made it onto key “terrorist watch lists” can be conclusively identified by biometric data alone, as Bucci’s testimony suggests.

Could it be more likely that the only real barrier to entrance to the United States is the Customs and Border Protection officer at the port of entry, who stamps the passport, with or without a few questions, and with little means of verification? Unless a match comes up with someone entered on the Terrorist Watch List or the no-fly list, the VWP traveler is free to enter for up to 90 days or vanish underground.

The Heritage Foundation director’s testimony included an impressively complicated chart (below) about how the VWP system is ***supposed to work,*** but the chart raises as many questions as it answers. It certainly doesn’t answer the most important questions about the actual effectiveness of the watch listing, checking and flagging process.



The ESTA regulations also have gaping enforcement holes. In 2010 (the latest data available), 364,000 travelers were able to travel under the VWP program without even the minimum verified ESTA approval by airlines, according to the Government Accountability Office (GAO). No one knows to what extent these passengers presented a security risk or if they left the country after the required 90-day limit on their stays.

Historically, it must be noted that Al Qaeda- aligned terrorists have already used the VWP to gain access to soft targets in the United States. French citizen and later convicted 9/11 participant Zacarias Moussaoui traveled on the VWP before he enrolled in Oklahoma and Minneapolis flight training schools prior to 9/11.

Richard Reid, the "Shoebomber," along with Ahmed Ajaj, also traveled on the VWP. In December 2001, Reid used an Amsterdam-issued British passport to board an American Airlines flight from Paris to Miami. In a separate incident, border agents caught Ajaj with bomb-making materials and a cheat sheet explaining how to lie to border officials. Ajaj was using a Swedish passport on the VWP.

Ramzi Yousef, one of the main perpetrators of the 1993 World Trade Center bombing and a co-conspirator in the Bojinka (airline bombing) plot to blow up 11 American jumbo jets, used the VWP on a fraudulent British passport:

"Yousef had boarded in Peshawar with a fraudulent British passport, presumably with no U.S. visa, and when he arrived at JFK [Airport in New York], presented an Iraqi passport in his own name, with no visa. Yousef was sent to secondary inspections where he requested political asylum; he was released on his own recognizance and went on to finish organizing the WTC bombing."

Despite the fact that both Youssef and Ajaj were caught in 1992 with numerous false passports, Youssef was not even detained, but was released in the U.S., and Ajaj was also later released. These egregious examples all occurred before or shortly after "9/11 changed everything." Some of these problems were likely remedied, but no one knows if the post 9/11 collection and management of "big data" did not create new snafus.

A 2004 OIG evaluation of the VWP still found significant problems and asked for reforms in 14 areas. One reform involved development of a process to check all Lost and Stolen Passport (LASP) data provided by participating VWP governments against entry and exit data in U.S. systems.

A 2014 report, prepared for Congress by the Congressional Research Service, says the 2008 reform mandates, which were required because of the 2004 OIG evaluation, are not complete. DHS has completed the pilot programs, but according to the Government Accountability Office (GAO), "DHS cannot reliably commit to when and how the work will be accomplished to deliver a comprehensive exit solution to its almost 300 ports of entry."

In 2012, testimony to the GAO by Rebecca Gambler, Acting Director of Homeland Security and Justice, revealed that data is being collected by some VWP countries ***but not shared by any***.

“As of January 2011, 18 of the 36 Visa Waiver Program countries had met the PCSC (Preventing Combating Serious Crime) and information-sharing agreement requirement, but the networking modifications and system upgrades required to enable this information sharing to take place have not been completed for any Visa Waiver Program countries.”

In July 2015, DHS, in collaboration with DOJ and the Department of State (DOS), completed PCSC Agreements, “or their equivalent with 35 (VWP) countries and two additional countries to share biographic and biometric information about potential terrorists and serious criminals.” The agreements are in place, but information is vague about data sharing. Would complete data sharing make a difference? Or are officials creating an even bigger haystack of unusable data?

More recently, on Nov. 18, Sen. Mark Warner, D-Virginia, told *Federal Computer Week* that the information travelers supply to the waiver program does not “necessarily include off-the-books travel to territory controlled by the Islamic State group.” Warner added that VWP doesn’t record where passport holders travel beyond their initial destinations:

“We don’t know how many European nationals have gone from France or elsewhere to Turkey or where they’ve gone from there, and [they] come here with virtually no screening. Literally 10 million people with German passports last year traveled to Turkey because there’s such an enormous Turkish population in Germany and many travel back to see relatives.”

More Questions than Answers

Far from inspiring confidence, this history and limited available information should raise more questions, including the following:

–Are the “Terrorist Identities Datamart Environment” (TIDE) and the Terrorist Screening Database (TSDB), the main or only “terrorist watch lists” checked for the names and passport identifiers of VWP applicants and/or entrants in order to detect any terrorist suspects seeking to enter? (TIDE is the U.S. Government’s central repository of information on international terrorist identities, but the list has grown to an unwieldy 1.1 million persons.)

–Does the over-inclusiveness of mostly non-relevant, non-biometrically (and even non-biographically) identified data in the larger “total information awareness” primary U.S. and foreign agency databases, where trillions of pieces of metadata have been vacuumed and stored, help or hinder the accuracy of the complicated winnowing or “nomination” process to compile TIDE/TSDB and the “No Fly” and “Selectee” lists?

Before Dec. 25, 2009, the Terrorist Screening Center (TSC) did not watch-list

the “underwear bomber” Umar Farouk Abdulmutallab. Since he was not on the Terrorist Watch List (TSDB), he was allowed to board a flight to Detroit. The failure was never fully made clear, but getting on the list, it seems, is more art than science as it requires “nomination” from “originator” intelligence and law enforcement agencies possessing “reasonable suspicion” and biographical identifying info for the person nominated.

Of course officials will always tend to err on the side of caution, which means the list of 1.1 million on TIDE ends up containing many false positives, or incorrectly identified “persons.” This is why, after years of complaints, officials had to devise a way for incorrectly listed individuals to challenge the listing and get their names off the “no fly list.”

The government counters – probably rightly – that it’s far better to tolerate the problem of “false positive” inaccurate listings than to err by not including a true “needle in the haystack” terrorist suspect. What’s left unsaid is the degree to which the list of 1.1 million persons is still under-inclusive as well as being over-inclusive.

–We realize that the pre- and circa-9/11 examples of egregious failures now ***should be*** moot in light of the vast changes initiated in data-collection, data-mining and refining the watch listing processes after 9/11. These failures occurred before “Top Secret America” began vacuuming up trillions of pieces of data on people all over the world, including that done by the NSA’s massive communication interception programs; before TIDE or the no-fly list even existed. Congress needs to learn whether any of the recent participants in the Mideast or the European terrorist attacks could have used the waiver program to enter the U.S.

–The new “$64 million question” becomes what is the actual, current track record of the watch listing process? How many, if any, of the dozens of citizens of any of the 38 participating countries who have, in hindsight, been identified as participating in recent terrorist incidents were NOT listed in TIDE or the TSDB so would not have been flagged if they had sought to enter the U.S. through the VWP? How accurate is the actual operation of the tiered nomination process in its attempts to accurately strain the wheat from the chaff, i.e., to get more “needles” and less “hay?”

DHS and NCTC will invariably know the full answers to these important questions while the public must rely on reporters’ limited prying. In all fairness, it’s been reported that brothers Said and ChÃ©rif Kouachi, who shot 12 “Charlie Hebdo” employees, were on the U.S. terrorist watch list for years. One of the brothers was known to have traveled to Yemen, possibly for training with Al Qaida in the Arabian Peninsula. Also on the plus side, *Reuters* reported that

four of the Nov. 13 attackers in Paris were listed in TIDE and at least one of the attackers was also on the U.S. no-fly list.

The US Refugee Program

Last week, the House of Representatives voted to tighten restrictions on the resettlement of Syrian refugees into the United States based on their concerns about national security. With a veto-proof majority, the bill passed 289-137 as Democrats joined Republicans, pointing to the fact that one of the participants in the Nov. 13 Paris attacks was a Syrian who entered Europe with a fake passport while posing as a refugee.

The House bill requires that the FBI and Department of Homeland Security devise rigorous background checks on refugees, guaranteeing that they pose no threat. But the current process of so thoroughly vetting refugees can take years before approval, since it requires repeated interviews, applicants' furnishing of full biometric data ***before traveling*** to the U.S. (in contrast to the VWP), and much more rigorous screening than merely checking terrorist watch lists. Further legislative restrictions would almost invariably prove so onerous as to effectively block almost all Syrian refugees from resettling in the U.S.

In 2013, DHS recorded a total of 69,909 persons admitted to the United States as refugees. The leading countries of nationality for refugees were Iraq, Burma, and Bhutan. This is almost seven times the number of proposed Syrian refugees, but no one raised an eyebrow about these refugees.

Of course, the bigger the haystack, the harder it is to find a terrorist. It is counter-intuitive to the "collect it all" mentality, yet whistleblowers, even before Edward Snowden, have been trying to make the public aware of the problems that inherently undercut the meaningfulness of "big data" gathering and analysis.

"The problem with mass surveillance is when you collect everything, you understand nothing," said Snowden, a former National Security Agency contractor. Data collection, even with biometric identifiers added, will inherently prove far less useful for predicting or preventing terrorism or any crime, than it will be in identifying a perpetrator, i.e., solving a crime, after the crime has been committed. That's essentially how the FBI's fingerprint repository works. A fingerprint identified one of the dead Paris attackers AFTER he died in the attack.

Yet no one would accuse the fingerprint database of having failed. That is because, unlike the massive data collection undertaken after 9/11, no one ever claimed or justified the fingerprint repository as the ultimate solution that

could detect criminals/terrorists and prevent would-be crimes/terrorist attacks before they happen.

A similar realistic appreciation of the benefits, difficulties and vulnerabilities of terrorist watch listing based on big data collection, along with honest answers instead of government secrecy is necessary to justify continuation or possible expansion of the VWP.

Clarification: A Daily Mail article is making the rounds that 102,313 Syrians were granted admission to the U.S. as legal permanent residents; a counterpoint to the Syrian refugee discussion. The headline reads: “Figures show more than 100,000 Syrians have come to America since 2012.”
See: http://www.dailymail.co.uk/…/Figures-100-000-Syrians…

Definitions are in order to understand the meaning behind the numbers. A Refugee is a person who has been forced to leave their country in order to escape war, persecution or natural disaster.
A legal permanent resident or “green card” recipient is defined by immigration law as a person who has been granted lawful permanent residence in the United States.

A total of 60,010 Syrian visa holders have entered the U.S. since 2012. A Visa holder can be anyone from a student, tourist, B-I employment Visa, spouse, fiancÃ©e or refugee. Another 42,303 Syrians were granted citizenship since 2012, according to the article. A total of 1309 Syrian refugees entered the U.S. in 2013 according to the 2013 U.S. Yearbook of Immigration Statistics.https://www.dhs.gov/…/files/publications/ois_yb_2013_0.pdf

Georgianne Nienaber is a regular contributor to the Huffington Post as well as regional and international publications. She is a member of the Society of Professional Journalists and Independent Reporters and Editors. In May of 2002, the co-writer of this article and former FBI Agent and Minneapolis Division Legal Counsel, Coleen Rowley, brought some of the pre-9/11 security lapses to light and testified to the Senate Judiciary Committee about the endemic problems facing the FBI and the intelligence community.