## II. United States

# Behind 'Twittergate': The NSA Meddles in Americans' Right To Vote, Speak, Think

by David Christie and Paul Gallagher

Dec. 9—The ongoing revelations from Elon Musk about Twitter, are essentially a revisiting of the now nearly forgotten revelations in 2014 of Edward Snowden about the near-universal surveillance of Americans by the National Security Agency (NSA) using telecommunications companies and Internet "social media" conglomerates. Whereas Snowden exposed, with undeniable evidence, that the NSA surveils Americans' communications and whereabouts on a large scale, Musk is exposing evidence leading to the conclusion that the NSA also controls what Americans are allowed to learn, to be informed of, or to say on social media.

No one, not even the most skillful journalist, can treat these revelations lightly or with tongue in cheek. What is being exposed is the deployment of military intelligence agencies and powers to perform Caesar's 2,000-year-old trick: the transformation of a republic into an imperial oligarchy—and to do that in the aftermath of economic calamity, the Great Financial Crash of 2007–08. The formation of teams of NSA and military officials to *control the discourse of national elections* has been part of that trick since the immediate aftermath of that crash and the economic collapse of 2009–10.

Edward Snowden made his evidence massive and airtight before he disclosed it, intending to explode inveterate lying to the American people at the highest levels of officialdom, and then to become as anonymous as he could. Elon Musk, the world's wealthiest and best-known businessman, is taking even greater chances, disclosing the evidence as he finds it at Twitter. But otherwise, the evidence is exposing precisely the same upper echelon of "big liars" in the military and intelligence agencies, "hustling liars" in the media conglomerates, and "local liars" on the university campuses.

A central element of the "government of lies" exposed neither by Snowden nor thus far by Musk, will be investigated by *EIR* here: the Election Security Group, made up entirely of military and intelligence officials and "experts" under the aegis of U.S. Cyber Command, and also sometimes given names like "Russia Small Group" and "White House Small Group."

CC/Laura Poitras/Praxis Films

NASA/Kim Shiflett

*A central element of the "government of lies" exposed by neither Edward Snowden (left), nor thus far by Elon Musk (right), is the Election Security Group of military and intelligence officials under the aegis of the U.S. Cyber Command.*

This suggests how—for example—when some contents of Hunter Biden's found laptop were reported in the *New York Post* in early October 2020, just before the Presidential election involving his father, more than 50 "present and former U.S. intelligence officials and experts" could be brought together within two days to decry "all the hallmarks of a Russian disinformation operation." There were no such hallmarks, nor have any been found since. This is merely one example in the evolution of Twitter into an amplifier of military-intelligence lies and a suppressor of those who contradicted them, whether an ordinary citizen or the nation's oldest continuously-published newspaper, the *New York Post*, whose Twitter account was shut down as a result.

### Five Million Cyber Command Fakes

A disclosure from the immediate past, the NATO-Russia conflict in Ukraine, provides an introductory illustration. Since Musk began the process of his takeover of Twitter, he has been charging that the social media platform was chock full of "bots," apparent human beings, using Twitter accounts that were actually phantoms machine-generated by computer systems. Thus, Twitter, the business Musk was taking over, did not have the claimed 350 million accounts for advertisers to target. Where did the bots come from?

Unconnected entirely to Musk, a team of computer sciences experts at Adelaide University in Australia, had conducted months of careful research and study of Twitter bots. Peter Cronau reported their work at great length in *Declassified Australia* Nov. 3 in an article called "Massive Anti-Russian 'Bot Army' Exposed By Australian Researchers."

We make short here, the very long story of this article, which readers can go through for themselves.

More than 90% of all Twitter "bots" (automated fake accounts) activated shortly after the Russian intervention in Ukraine began, were anti-Russian, pro-Ukraine "individuals" tweeting about the war. Twitter did not block or remove any of these *5 million-plus* fake accounts and acted as if its content moderators did not notice them. (We can infer that neither did it use against them the "tools" Musk is now exposing, such as "search blacklisting," "trend blacklisting," "visibility filtering" and so forth.) Only about 7% of bots were explicitly "pro-Russian," and they were launched more gradually after the start of Russia's military intervention. Twitter blocked or removed outright, the accounts of most of these bots.

Moreover, the Adelaide University researchers strongly imply a conclusion that U.S. Cyber Command, headed by Gen. Paul Nakasone, was the source of the bots which virtually took over Twitter in late February and March, but which Twitter moderators affected not to see. Rather than state this conclusion outright, the researchers connect the mass of bots to the comments of Nakasone (also NSA Director and chief of its Central Security Service) to *Sky News* in late May:

> Cyber Command had been conducting offensive Information Operations in support of Ukraine. "We've conducted a series of operations across the full spectrum: offensive, defensive, [and] information operations," Nakasone said.

U.S. Army/Joe Lacdan

*Lt. Gen. Paul Nakasone heads the Army Cyber Command, the probable source of the anti-Russia, pro-Ukraine bots which virtually took over Twitter in late February and March, but which Twitter moderators affected not to see.*

### Biden a War VP and War President

Information that allegedly showed corrupt influence peddling within the Biden family should have been something the voters of 2020 had access to. So why was the content of Hunter Biden's laptop so heavily censored across nearly all media and social media platforms—admittedly by Mark Zuckerberg's Facebook, most aggressively by Parag Agrawal's Twitter? Perhaps that censorship has more to do with wartime propaganda, given that Vice President Joe Biden's role in Ukraine on behalf of Barack Obama, and his own policy now, was and is so central to the unfolding world war.

It is highly likely that a Trump Administration would not have blocked the very idea that Ukraine NATO membership be ruled out in negotiations with Russia, nor joined the UK in early April in pushing Ukraine's President Volodymyr Zelensky to stop negotiating with Russia. Biden as Vice President had played a central role in the putsch which evicted the Ukrainian government of Viktor Yanukovych in 2014 to create an anti-Russia marcher-state.

There was no question in the Fall of 2020 that Joe Biden, as President, would be no JFK to resolve a missiles crisis, but rather would be ready for a military confrontation with Russia over the Ukraine which had been Biden's vassal state in 2014–16.

The narrative surrounding "Twittergate" presently, falsely, centers on partisan operatives there; and only somewhat more accurately on corrupt "Foreign Interference Task Force" agents from the FBI led by FBI General Counsel become Twitter's Deputy General Counsel James Baker. But the role of the Department of Defense's "Election Security Group" should be considered, given the present information warfare surrounding the unfolding war against Russia (and China next).

Twitter Deputy General Counsel Baker, who while at FBI had allegedly worked with Michael Sussman of the Perkins Coie law firm on key aspects that began the "Russiagate" fraud, was the person responsible at Twitter who made the decision to label the Hunter Biden laptop material as "hacked." We do not know whether Baker was a part of the Election Security Group that was announced in the run-up to the 2018 midterms, and had been previously known as the NSA's "Russia Small Group" and appears similar in leadership to the 2016 "White House 'small group'." However, we do know that the FBI and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) were key partners of the Election Security Group (ESG).

## The Election Security Group

We can find in the Twitter internal communications which Elon Musk is disseminating now, that the national security agencies and their Election Security Group were all over Twitter in that period of its suppression of news before Election Day 2020, and of then-President Trump's tweets and then his Twitter account in the months after. One finds in a message from the Twitter executive who headed its "Trust and Safety" department, Yoel Roth, the following on Oct. 16, 2020:

> Weekly sync with FBI/DHS/DNI re: election security. The meeting happened about 15 minutes after the aforementioned Hacked Materials implosion; the government declined to share anything useful when asked.

Blocking publication of "hacked materials" had been Twitter's claimed justification for suppressing the *New York Post* in the matter of Hunter Biden's computer; but that cover story was false and had already "imploded," as Roth was admitting.

Again, five days later, on Oct. 21, 2020, Roth informed an executive, "I have to miss the FBI and DHS meetings today, unfortunately."

The Election Security Group (ESG), in the run-up to the 2018 midterms, had been known as the NSA's "Russia Small Group." The ESG has operated subsequently in the 2020 General Election, and was promoted by the Defense Department again for the 2022 midterms, to "counter foreign interference" and foreign disinformation campaigns.

The ESG and Russia Small Group also bear a striking resemblance to an earlier group known as the "White House 'small group'." That was formed in 2016 by high-level officials from the U.S. intelligence community and Department of Defense, in the aftermath of the director-level meeting between the UK Director of Government Communications Headquarters (GCHQ), Robert Hannigan, and CIA Director John Brennan, to introduce the concocted "Steele Dossier."

The successive iterations of the Election Security Group have repeatedly initiated claims of hacking by foreign groups, and backed them with statements and "conclusions" of the intelligence community, which have subsequently been proven false. This began with the defensive claim suddenly raised during the 2016 Democratic National Convention, when Wikileaks had published Democratic Party leadership emails showing the intentions of Hillary Clinton and top Democratic

National Committee operatives to suppress the campaign of Sen. Bernie Sanders for the Party's Presidential nomination.

"DNC hacked by the Russian GRU to help Trump" was heard everywhere, supported by top intelligence officials like James Clapper, the Director of National Intelligence whom Edward Snowden had shown to be a sworn liar already two years earlier. This media storm effectively removed the Democratic Party's suppression against Sanders' campaign from public consciousness as an issue, and Senator Sanders himself acquiesced.

But Sunday, Dec. 4, 2022, marked five years since the 2017 Congressional testimony that there was *no sign* of such a hack—by Shawn Henry, the president of the IT firm called CrowdStrike which had "discovered" the hack! That testimony from 2017 was kept classified by committee chair Rep. Adam Schiff for two-and-a-half years, and has then been suppressed for just as long by Twitter and the other social media giants, as well as the "legacy media."

## The Military-Intelligence Election Manipulators

Nonetheless, here is how the Defense Department, in the press release linked above, explains what the Election Security Group does:

> The joint CYBERCOM-NSA Election Security Group, stood up again in early 2022, aligns both organizations' efforts to disrupt, deter and degrade foreign adversaries' ability to interfere and influence how U.S. citizens vote and how those votes are counted.
>
> As in previous election cycles, CYBERCOM and NSA are closely partnered across the government and industry and are one critical component of a whole-of-government effort. The group directly supports partners, like the Department of Homeland Security and the FBI, in collecting, declassifying, and sharing vital information about foreign adversaries to enable domestic efforts in election security.
>
> The U.S. government is actively defending against foreign interference and influence operations in U.S. elections, specifically, by focusing on how adversaries seek to undermine U.S. interests and prosperity, the will to vote of the populace, as well as their belief in the sanctity and security of their elections.
>
> Leveraging on past successes, the ESG has increased its whole-of-society engagement with industry to share threats and potential vulnerabilities.

Some reports indicate that the Russia Small Group/Election Security Group (ESG) numbers around 75–80 personnel, but there is no published account of the actual membership. The ESG is known to have two coleads—one each from the NSA and CYBERCOM. These Department of Defense agencies collaborate with numerous other domestic security agencies, particularly the FBI/DHS Cybersecurity and Infrastructure Security Agency (CISA), for a "whole of government" approach. The ESG also partners with "industry"—the leading IT platforms and companies of Silicon Valley and other locales, such as the Dulles Corridor outside of Washington D.C.—for a "whole of society" approach.

Moreover, the ESG also works with "foreign partners." This can be assumed to include the sister agency of the NSA, the UK's GCHQ, given that NSA and GCHQ have been nearly inseparable since the various iterations of the March 4, 1946, BRUSA (now known as UKUSA) Agreement. They constitute the nerve center of the U.S.-UK "special relationship" and its connection to the broader Five Eyes (Australia, Canada, New Zealand, UK, United States) intelligence services.

## 'The Band Is Already Back Together'

At Vanderbilt University's May 4–5 "Summit on Modern Conflict and Emerging Threats," in response to a question regarding foreign threats to the 2022 midterms, Gen. Paul Nakasone, Director of the NSA, Commander of CYBERCOM and Chief of the Central Security Service, said that "the band was already back together," in a reference to the Election Security Group (ESG).

While one might infer from Nakasone that his reference to the "band" related to the 2018 midterms and the 2020 general election, perhaps his reference was more specifically to a small group of personnel that has been collaborating since the formation of CYBERCOM.

It turns out, that the small team that created CYBERCOM back in 2010, now have leading roles in the present cyber team in the Biden White House, and are

Executive Office of the President/Stephanie Chasez

Executive Office of the President

Cybersecurity and Infrastructure Security Agency

*Anne Neuberger, Deputy National Security Advisor for Cyber & Emerging Technology (left); Chris Inglis, National Cyber Director; and Jen Easterly, current Director of Homeland Security's Cybersecurity and Infrastructure Security Agency (right).*

leading personalities of the agencies that comprise the Election Security Group!

Biden's White House cyber team has been described as the "Big Three": Anne Neuberger, Deputy National Security Advisor for Cyber & Emerging Technology; Jen Easterly, present Director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA); and Chris Inglis, National Cyber Director.

Anne Neuberger was the NSA's lead for the Russia Small Group, and the NSA's first co-lead of the Election Security Group in 2018. Her background in leading security matters related to cyber, began in the aftermath of the 2007–08 financial crisis. According to her LinkedIn profile, Neuberger in 2007 left her family's Wall Street firm, American Stock Transfer & Trust, as Senior Vice President and Director of Operations, to join the Bush Administration as a White House fellow for the Department of the Navy. She became Special Advisor to the Secretary of the Navy during the transition period of the outgoing Bush and incoming Obama administrations. Leaving the Obama White House in the Summer of 2009, she joined the NSA and, still in her early 30s, became the Team Lead for implementing the Department of Defense's newest command, U.S. Cyber Command.

U.S. Air Force

*Lt. Gen. Stephen L. Davis, Director of Global Operations of STRATCOM (2018-2020).*

Neuberger's role in the formation of CYBERCOM began her public working relationship with Gen. Paul Nakasone. Since its 2010 establishment, heading CYBERCOM has been a dual-hat role of the NSA Director. Nakasone was one of the military personnel dubbed as the "Four Horsemen" that formed CYBERCOM, along with then-Army Lt. Col. Jen Easterly, chief of the Army's first cyber battalion and currently head of the DHS's CISA; then-Navy Capt. T.J. White; and then-Air Force Col. Stephen Davis.[1] CYBERCOM

[1] Navy Capt. Timothy J. White, who was serving in the Department of Defense's offensive computer network operations wing and went on to become the head of the Cyber National Mission Force of USCYBERCOM (2016–2018); and Air Force Col. Stephen Davis from U.S. Strategic Command (STRATCOM), who would go on to become the Director of Global Operations at STRATCOM (2018–2020), had authored in 2003, "Speed Kills: Implications of Prompt Global Strike."

was a sub-unified command of U.S. Strategic Command (STRATCOM) until it gained its full operational status in 2018.

It should be noted that 2018 was also the year that the Nuclear Posture Review and the National Defense Authorization Act (NDAA) discussed whether nuclear weapons could be deployed in response to cyber-attacks.

The formation of CYBERCOM was overseen by its first head, Gen. Keith Alexander, NSA Director in 2010. Chris Inglis was a top aide to Alexander and was the Deputy Director of NSA (2006–2014).

Clearly, the "Big Three" of Biden's cyber team at the White House were already a top NSA team before Biden's election, and were instrumental there in overseeing the Election Security Group.

The present concerns of censorship by "Big Tech" should be seen in the context of the revelations by Edward Snowden in 2014. Snowden's documents showed that NSA was being integrated with the leading IT firms of Silicon Valley through programs like PRISM, Enduring Security Framework, and the Defense Industrial Base. Anne Neuberger oversaw the Enduring Security Framework[2] and the Defense Industrial Base (2010–2013). After Snowden's revelations made public the NSA-Silicon Valley collusion in 2013, Neuberger became the NSA's first Chief Risk Officer, which according to media reports, handled the fallout from the Snowden revelations.

## Control the 'Cognitive Infrastructure'

Foreign interference in elections and foreign disinformation campaigns are central to the justification of the existence of the NSA-CYBERCOM Election Security Group that partners with the FBI and CISA, even though some of the foreign cyber-attacks, or alleged "hacks," have been proven not to have occurred. Perhaps that is why, as *The Intercept* has reported, Jen Easterly, under the Biden Administration, has now changed the name of CISA's "Countering Foreign Influence Task Force" to "MDM teams" (MDM: Misinformation, Disinformation, Malinformation).

To combat MDM, Easterly discusses the need for "resilience," which has now become the catchword for Global Britain's allies engaged in behavior modification and thought control. From *The Intercept*:

> Jen Easterly, Biden's appointed director of CISA, swiftly made it clear that she would continue to shift resources in the agency to combat the spread of dangerous forms of information on social media. "One could argue we're in the business of critical infrastructure, and the most critical infrastructure is our cognitive infrastructure, so building that resilience to misinformation and disinformation, I think, is incredibly important," said Easterly, speaking at a conference in November 2021.

[2] From "When Google Met WikiLeaks," by WikiLeaks founder, Julian Assange: "Around the same time, Google was becoming involved in a program known as the 'Enduring Security Framework' (ESF), which entailed the sharing of information between Silicon Valley tech companies and Pentagon-affiliated agencies 'at network speed.' Emails obtained in 2014 under Freedom of Information requests show [Google CEO Eric] Schmidt and his fellow Googler Sergey Brin corresponding on first-name terms with NSA chief General Keith Alexander about ESF. Reportage on the emails focused on the familiarity in the correspondence: 'General Keith … so great to see you…!' Schmidt wrote. But most reports overlooked a crucial detail. 'Your insights as a key member of the Defense Industrial Base,' Alexander wrote to Brin, 'are valuable to ensure ESF's efforts have measurable impact'."