EXHIBIT 4

Declaration of Col. John R. Mills (USAR Ret.) (Nov. 21, 2021)

I, John R. Mills, declare under penalty of perjury that the following is true and correct:

1. I have personal knowledge of the matters set forth below and could and would testify competently to them if called upon to do so.

Introduction

2. I am Colonel, USAR, (Retired), John R. Mills and also Former Director of Cybersecurity Policy, Strategy, and International Affairs, Office of the Secretary of Defense, Senior Civilian (Retired). My dual career as an Active and Reserve member of the U.S. Army as well as a senior civilian in the Department of Defense has given me a unique opportunity for almost 40 years to participate directly, provide oversight, or be aware of a vast expanse of the planning and use of a wide range of U.S. cybersecurity-related instruments of national power. I have held Top Secret, Sensitive Compartmented Information (SCI) security clearances since approximately 1988. I have also been an adjunct Professor and have taught graduate level cybersecurity law and policy since 2013 at the University of Maryland, Global Campus. My last uniform position in the Department of Defense was in Homeland Defense and I often served as a liaison with Department of Homeland Security to coordinate the national response to complex emergencies and threats to the Homeland (real events and exercises).

3. I have been asked to testify on the development, capabilities, and uses of "remote access operations" for unlawful entry and purposes into networks. The information presented is unclassified and based upon my personal experiences, publicly available reporting, studies, events, incidents, best practices, and de-classified U.S. Government information. Remote access operations for nefarious purposes refer generally to the methods and activities used to access networks, data centers, and other

locations, often enabled by planted malware, enabling software, and/or algorithms, conducted in a manner to avoid detection or leaving behind of identifying forensic evidence of penetration.

4. Remote access operations are different than remote maintenance monitoring which is intended by network designers for transparent and auditable access to network enabled devices for maintenance and updates. Remote maintenance monitoring can also be employed or co-opted for reasons not in accordance with remote maintenance monitoring tenets, design intent, network owners/operators, or lawful access/purpose. Electronic election infrastructure is just one example of critical infrastructure which can be subjected to remote access operations. The U.S. Government conducts remote access operations through the entities described in Executive Order 12333[1], as described in the articulation of the U.S. Intelligence Community (IC)[2] roles, missions, and organization, and as directed by a sitting President (POTUS). The IC is also enabled by and often operates in close coordination with the Department of Defense and Federal Law Enforcement for these operations.

5. In addition, other countries, organizations, and individuals have also developed these remote access capabilities with varying degrees of sophistication. Such capabilities have been expanding at an accelerating rate in the past 20 years threatening critical infrastructure, such as election systems[3], in ways that threaten the very foundation of our Republic i.e. the foundational tenet that leaders in our Country are actually chosen by the People through a voting system based on "one person one vote" as opposed to an election system that is compromised by malign actors seeking to exploit an election for their own benefit.

---

[1] Presidential Executive Order 12333 United States Intelligence Activities (As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008));
https://irp.fas.org/offdocs/eo/eo-12333-2008.pdf
[2] EPIC.org, "Background on Executive Order 12333"; https://archive.epic.org/privacy/surveillance/12333/
[3] CISA Website, Election Infrastructure as Critical Infrastructure, https://www.cisa.gov/election-security

6. The employment of machine-based algorithms accessing electronic voting systems in the United States to attempt to achieve a pre-determined election outcome through remote access operations is well within the capabilities of many nation-state actors such as China, Russia, Iran, and Venezuela, as well as even non-nation state actors.

7. From the 1980s to the present, the capabilities, scope, and scale of remote access operations to collect or alter data have greatly expanded in their scale, access, and ability. These operations have become ubiquitous through nation state and private actors. The offense in remote access operations normally has a decided advantage against defenders.

Summary of Findings

8. The U.S. Government has pioneered and pushed the envelope on the art and techniques of remote access of critical infrastructure.

9. Based on my personal experience the United States Government has the capability to project significant effects[4] toward critical infrastructure worldwide—including election systems—if a complete decision process up to and including the President was conducted and completed. This same capability (to project effects) now exists in other countries, such as China, Russian, Iran, and Venezuela, and these foreign powers now use these same, similar, and improved remote access operation methodologies at will to assert their own national agendas.

10. These operations have created a growing talent base of personnel, software, and network enabled capabilities that are becoming ubiquitous in the hands of companies and personnel outside of the U.S. Government.

[4] "Effects" is an operator's and planner's term of art which implies the ability to degrade, exfiltrate, manipulate, change, or destroy.

11. The U.S. Government made strong statements on the maturity level of U.S. Government capabilities regarding election security during the November 2020 election. With my professional experience and my understanding of the election process in America (I have not yet found a U.S. Government national security professional who has also participated as a sworn election official and demonstrates an understanding of the election process at the county level), I have very low confidence in the security of American election critical infrastructure. In my professional opinion, assertions by the IC, Homeland Security, and other law enforcement officials that they have the situational awareness and capability to defend these environments, including the election environment as part of national critical infrastructure with a high level of confidence are unsupported and, in some cases, may be false. Several publicly known breaches of critical infrastructure are presented later in this document and one of the most damaging and egregious was the breach of the Office of Personal Management which created catastrophic results. The full resources and full spectrum of the U.S. Government were available to detect, prevent, stop, mitigate, or otherwise address the attack on this critical infrastructure, yet that is not what happened.

12. My professional opinion is that the statement "The November 3rd election was the most secure in American history" asserted in a November 12, 2020, posted on the Cybersecurity and Infrastructure Security Agency ("CISA") website, had little, if any, basis in fact.[5]

13. Moreover, in my professional opinion, the assertions by then-Director of CISA, Christopher Krebs, claiming the November 2020 election was secure had similarly little, if any basis in fact. Indeed, Mr. Krebs largely refuted his own November 2020 comments in his February 10, 2021,

[5] CISA, Joint Statement, November 12, 2020, https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election

testimony to Congress[6], and gravely injured his and the CISA's credibility on delivering a secure environment for the election systems employed in the United States.

14. In my professional opinion, based upon substantial experience on national cyber capabilities, cybersecurity, planning, policy, strategy, and with my knowledge of the election process, the statements made by CISA and Krebs referred to above, to be properly, independently, and holistically assessed must include a factual establishment and public release of the actual National Intelligence Collection priorities at the time of the November 2020 election, and the precise and specific signatures and indicators the national intelligence collection system (and law enforcement), and their capabilities were supposedly tuned to monitor, collect, and defend the 2020 election[7]. The broad assertions and statements by Mr. Krebs and others also presume an ability to detect these remote access operations in an extremely timely manner with extremely high confidence—which is simply not realistic at this point in time and have a poor track record.

Relevant Experience and Qualifications of Author

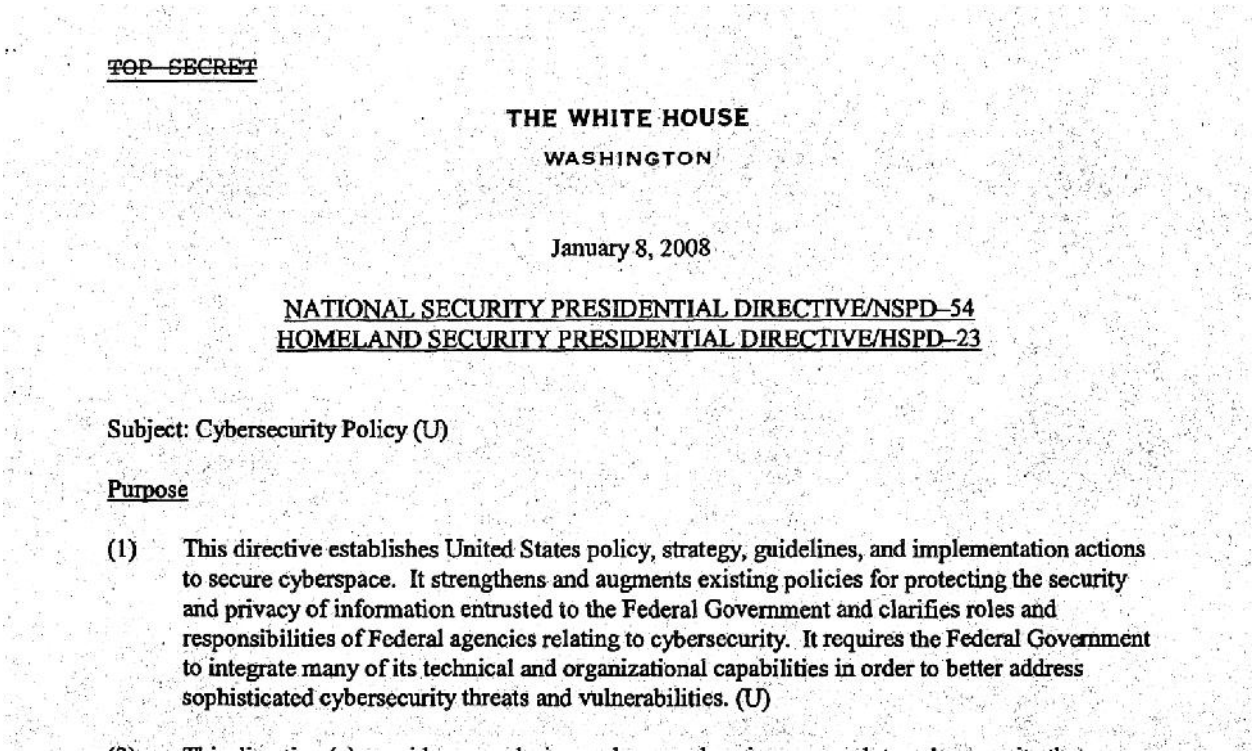
15. I have defended our Country since 1983. My service for our Nation ranges from the tactical level in combat to the strategic at the Office of the Secretary of Defense (DOD). I am a school trained and qualified Military Intelligence Officer, Psychological Operations Officer (PSYOP – a Special Operations Community Branch), Civil Affairs Officer (also a Special Operations Community Branch), and Public Affairs Officer. My role has essentially been as a national security strategic planner since approximately 2001. My service at the senior levels of the U.S. Government has included: complex inter-agency proceedings and deliberations on cyber and cybersecurity and other whole of government

---

[6] Christopher Krebs Testimony Committee on Homeland Security, February 10, 2021 https://docs.house.gov/meetings/HM/HM00/20210210/111152/HHRG-117-HM00-Wstate-KrebsC-20210210.pdf

[7] The code name of the operation(s), their planning documents, establishment of inter-agency roles and missions, and all coordinating instructions to include the detailed guidance on factual Intelligence Collection priorities, including signatures and indicators, must be made public.

operations across the whole spectrum of instruments of national power; international partner negotiation of sensitive information sharing agreements (including the Five Eyes (FVEYS[8])); and being the DOD representative at the National Security Council from mid 2008 to mid 2009 as NS/HSPD-54/23[9] when the Comprehensive National Cybersecurity Initiative (CNCI)[10] was brought to life as described in following official memorandum (a formal Presidential Directive of the President George W. Bush Administration).



~~TOP SECRET~~

THE WHITE HOUSE

WASHINGTON

January 8, 2008

NATIONAL SECURITY PRESIDENTIAL DIRECTIVE/NSPD–54
HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD–23

Subject: Cybersecurity Policy (U)

Purpose

(1) This directive establishes United States policy, strategy, guidelines, and implementation actions to secure cyberspace. It strengthens and augments existing policies for protecting the security and privacy of information entrusted to the Federal Government and clarifies roles and responsibilities of Federal agencies relating to cybersecurity. It requires the Federal Government to integrate many of its technical and organizational capabilities in order to better address sophisticated cybersecurity threats and vulnerabilities. (U)

Figure 1: NS/HSPD-54/23

[8] "The Five Eyes was formally founded in the aftermath of the Second World War, through the multilateral agreement for co-operation in signals intelligence (SIGINT), known as the UKUSA Agreement, on 5 March 1946." Since this original agreement, Canada, Australia, New Zealand have been added as well as other countries for unique functional topics. https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/

[9] Department of Homeland Security, Fact Sheet: Preventing and Defending Against Cyber Attacks, October 18, 2011; https://www.dhs.gov/news/2011/10/18/preventing-and-defending-against-cyber-attacks

[10] FAS.ORG; De-classified Text of HS/NSPD-54/23: Cybersecurity Policy; https://irp.fas.org/offdocs/nspd/nspd-54.pdf

Signed January 8, 2008, by President George W. Bush

16. CNCI represented a large-scale leap ahead in Cybersecurity of the American nation state as the title implies, but also developed significant new remote access capabilities submerged inside the program. Portions of paragraph 47 of the CNCI document (pages 12-13) are partially redacted and possibly point to additional capabilities. In layperson's terms, robust remote access operations can range across several functional activities and can possibly include exfiltration or manipulation of data on a large scale of critical infrastructure —including electronic voting systems. NS/HSPD-54/23 was a defining event in the history of U.S. Government remote access operations. The CNCI effort was a disruptive, historical inflection point for collection of information on a massive scale never seen before. From 2007 forward, the ability to penetrate networks, and manipulate or gain information on scale, expanded exponentially.

17. In both my uniformed service, civilian service, and post-U.S. Government service I have had several unique opportunities to work, plan, implement, observe, and make recommendations in both American elections and foreign elections. I have been a sworn election official in my home county, Prince William County Virginia, multiple times since the early 2000s, including the November 2020 election. Day of voting was almost irrelevant in my county. 74% of the votes in the November 2020 election were absentee in one of several forms. This meant that 74% of the ballots were handled at what is known as the Central Absentee Precinct (CAP), a first in Virginia and handled with very unclear guidance on chain of custody for thumb drives removed and moved around with little chain of

custody procedures. The use of a thumb drive is a key enabler in cyber intrusions based upon the Agent BTZ[11] and possibly Stuxnet[12].

18. While in uniform I have been personally responsible for information campaigns communicating the importance of a transparent and trustworthy election process and the compelling imperative of citizen involvement. This was during my service in Bosnia in 1997. In addition, I participated in the establishment of a clean election process in Iraq which was one of the first strategic imperatives in the post regime change environment. From 2003 to approximately 2009, I was routinely part of meetings and projects from the tactical to the Combatant Command, to the strategic level where issues, themes, processes, and conduct of elections in Iraq were discussed and formulated.

19. Out of office, I was asked for my actionable recommendations for the January 2020 elections in Taiwan. I made two basic recommendations. The first was the necessity for a new, national security law, prohibiting the acceptance of foreign money regarding elections in Taiwan. My second recommendation was to make the process as simple and transparent as possible and the critical importance of official ballot standards and the use of the "dumbest and simplest" ballot tabulation machines possible. The machine should have no other feature other than to simply tabulate the ballot. Such a configuration limits remote access operations to unique access methods such as 110- or 220-volt power cords (i.e., wall power that the machine is plugged into)[13]. The machines should have no features other than simple tabulation and should have no connectivity sub-components such as Bluetooth, modems, or anything else. Simply put, the Taiwanese executed flawlessly. A new law was

---

[11] Council on Foreign Relations, Cyber-Operations, "Agent.btz", November 2008 https://www.cfr.org/cyber-operations/agentbtz

[12] CNET, Stuxnet delivered to Iranian nuclear plant on thumb drive", April 12, 2012, https://www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/

[13] The Hacker News, "Hacker can steal data from air-gapped computers through Power Lines, April 12, 2018, https://thehackernews.com/2018/04/hacking-airgap-computers.html

passed[14], arrests were made of foreign influence operatives, and the election was conducted in a model of transparent processes using manual processes to the greatest extent possible, enabled by the simplest of election machines and technology. The outcome was magnificent and Chinese influence operations to throw the election were crushed.

20. In all my election work as an American sworn election officer in U.S. elections, in Bosnia and Iraq as a Uniformed Military Officer and senior civilian, and assessment of Taiwan elections as a private citizen (advice rendered to other American nationals), we have either been trained, told, looked to, or were supposed to abide by the principles of the Carter Center for Democracy, and their recommended best practices for free and fair elections. The Carter Center Manual, Chapters 8 – 10[15] are considered the gold standard in the conduct of democratic elections. In my professional opinion, American elections deviate substantively from the best practices endorsed by the Carter Center. Just a few of the examples include:

a. Right of the State to determine and enforce citizenship for voting (P.147): In Virginia I identified 8 -12% of registered voters in my county were unlawful based on 2019 rejection of voters for jury duty. There was no action by my Election Registrar or Board after being presented this apolitical, factual evidence.

b. Independent Body to review electronic voting technologies (P.152): There is no pervasive implementation of qualified independent bodies provided with uniform minimum standards at the county or state level to review election technologies that I am aware of. Currently, county election personnel cede sovereignty on all election technologies to their contractors. I have never come across a county situation where the sworn election officials know how to access or see network activity

[14] ABC News, "Taiwan passes law targeting Chinese Political Interference, December 31, 2019, https://abcnews.go.com/International/wireStory/taiwan-passes-law-targeting-chinese-political-interference-67996333
[15] The Carter Center, "Election Obligations and Standards"; https://www.cartercenter.org/resources/pdfs/peace/democracy/cc-OES-handbook-10172014.pdf

beyond the machine. There is no independent, 3rd party verification and validation I have ever come across. Contractors will often assert intellectual property rights or contractual terms and conditions to deny any third-party review of the network/cloud environment beyond the election machine. For example, it has been publicly reported that "a software update [was] installed to address a glitch in Georgia's voting machines" just a few weeks prior to the November 2020 election.[16] It does not appear that this "update", and it's purpose or effect, was ever reviewed by any qualified independent bodies in that State."

c. Unfettered observation of the election process (P.155): There were hundreds of affidavits submitted by election poll watchers attesting to being harassed, blocked, and excluded from observing the election process. Two examples are the reports from the Philadelphia Convention Center and the Detroit TCF Center during and after the November 2020 election.

d. Judicial reviews of the election process (P.257): Up to this point in time, the judicial branch has largely deferred on in-depth reviews of the election process and has largely asserted lack of standing from any group seeking election review or recourse.

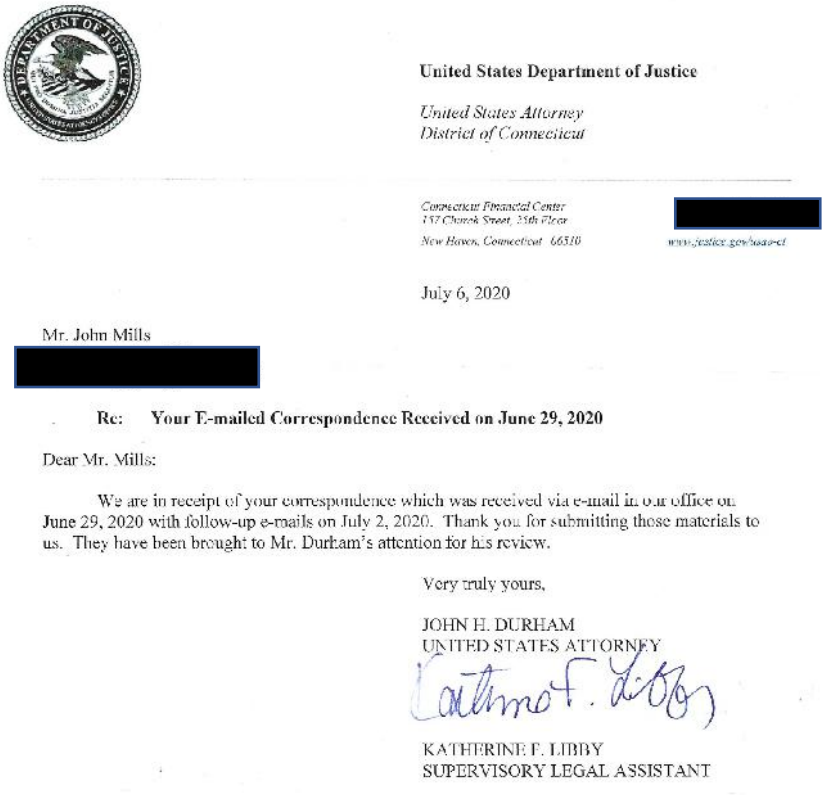
21. There is also a possible intersection between the expanding remote access operations and capabilities with the spying effort directed toward President Trump in 2016. I also was present and a witness to several events in what has become known as "Spygate" or "Russiagate". Within days of the November 2016 election, I was asked to participate in urgent inter-agency meeting to produce a Russian connection narrative, through the finalization of an Intelligence Community Assessment (ICA) which has now been established as being composed of false statements[17] from Mr. John Brennan and

---

[16] AP News, "With time short, judge mulls Georgia voting system changes", October 7, 2020, https://apnews.com/article/technology-senate-elections-georgia-elections-voting-machines-6a6be19f168a719e68c107c7426df9f3

[17] Cornell Law; 18 U.S. Code § 1001 - Statements or entries generally; https://www.law.cornell.edu/uscode/text/18/1001

Mr. James Comey. I have presented extensive evidence to U.S. Attorney for Connecticut, Mr. John Durham chronologizing these events.



United States Department of Justice

United States Attorney
District of Connecticut

Connecticut Financial Center
157 Church Street, 25th Floor
New Haven, Connecticut 06510
[redacted]
www.justice.gov/usao-ct

July 6, 2020

Mr. John Mills
[redacted]

Re: Your E-mailed Correspondence Received on June 29, 2020

Dear Mr. Mills:

We are in receipt of your correspondence which was received via e-mail in our office on June 29, 2020 with follow-up e-mails on July 2, 2020. Thank you for submitting these materials to us. They have been brought to Mr. Durham's attention for his review.

Very truly yours,

JOHN H. DURHAM
UNITED STATES ATTORNEY

KATHERINE F. LIBBY
SUPERVISORY LEGAL ASSISTANT

Figure 2: Mr. Durham Receipt of 27 Pages of names and events from Colonel (Ret) John Mills

An important attribute of the contemporary national security culture is a strong influence for conformance to an established narrative – this behavior undermines original thought, analysis, and innovation

22. In my professional experience, there often is a monoculture of singular narratives in the national security world that are established and rarely, if ever questioned, challenged, or further investigated. I have experienced this mentality in countless senior level meetings within the Pentagon, the Inter-Agency, and the White House. However, it appears that under President Trump, this strong conformance to a singular narrative changed to include outright hostility to the notion that China interfered in the November 2020 election. On January 7, 2021, the Director of National Intelligence

("DNI") concluded in an unclassified memorandum that "CIA Management took actions 'pressuring [analysts] to withdraw their support" for findings regarding China's actions to "interfere" in the election. [18] The DNI concluded that the CIA's actions violated Intelligence Community Tradecraft Standards.

The history and evolution of U.S. Government remote access operations

Compelling need for access to denied areas containing foreign actors with nuclear weapons

23. Since the Second World War and the 1947 and 1949 National Security Acts[19], the IC and the rest of the United States Government have rightly and assertively sought to attain access to denied areas[20] to defend the United States from the existential threat of the Soviet Union and others since the Second World War. The U-2, SR-71, the Corona Program[21], are but a few of the manifestations of grand and bold innovation to seek access to the true status, capabilities, and intent of a closed, secretive, and paranoid, totalitarian system with nuclear weapons at the ready to destroy the United States.

Era of Dial Up

24. In the early days of network connectivity which trace their lineage from the ARPANET[22] (Advanced Research Project Agency Network), original packet switching was often conducted through the common term of "dial up". The basic thesis was creating a resilient network for continuity of

---

[18] DNI John Ratcliffe Memo, January 7, 2021; Views on Intelligence Community Election Security Analysis; https://context-cdn.washingtonpost.com/notes/prod/default/documents/6d274110-a84b-4694-96cd-6a902207d2bd/note/733364cf-0afb-412d-a5b4-ab797a8ba154.#page=1

[19] DNI, "National Security Act of 1947", https://www.dni.gov/index.php/ic-legal-reference-book/national-security-act-of-1947

[20] Denied areas meaning totalitarian nations with hostile intent and an inability of the United States to obtain information on motives, agendas, and intent by traditional statecraft.

[21] National Aeronautics and Space Administration, "Corona"; https://space.jpl.nasa.gov/msl/Programs/corona.html

[22] Defense Advanced Research Projects Agency, "ARPANET"; https://www.darpa.mil/about-us/timeline/arpanet

communications during a nuclear exchange between the Soviet Union and America. In these early days of modern cyber (approximately 2007 being the critical year with CNCI, thus the BC/AD of cyber), computers and our personal computers had to reach out through common, copper, phone lines to knock and handshake in an analogue manner and establish a connection with another computer. During those days, it was a simple way to connect. There were no firewalls, gateways, or cybersecurity. There really was no thought to security at the time[23]. The thought of a non-compliant or hostile participant was not really considered. Why would anyone be malign?

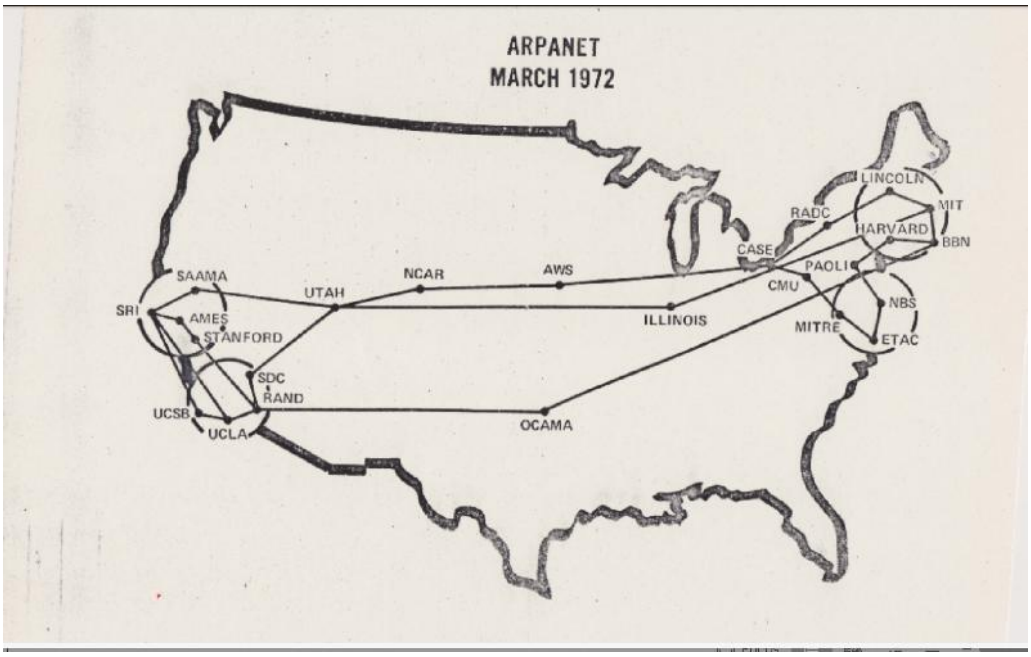


Figure 3: The original ARPANET network

[23] Washington Post, "Net of Insecurity", May 30, 2015; https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/

Major cyber intrusions enter the picture

25. As we now know, there are malign actors[24], many of them[25]. The threat actors have evolved since the early days where information technology engineers created worms[26] out of curiosity and early compartmented U.S. Government activities, possibly in participation with our Five Eyes (FVEYS) partners[27], began to poke, peek, and even fiddle with foreign networks and the Soviet Union and others did it right back.

26. In the 1980's the original concept of ARPANET began exponentially expanding, and threat actors (and American U.S. Government activities) began to realize the exploitation (i.e., exfiltrating or taking data from someone else) or mayhem they might be able to inflict on large scale. Much of the activity centered on intercepting and decrypting message traffic, but there also was deep interest and grave concern over the sanctity of our nuclear command and control systems. The CIA and NSA entered this world as well as the Department of Justice and the Federal Bureau of Investigation. The seminal statute in prosecuting computer intrusions was, and still is the Computer Fraud and Abuse Act (CFAA 18 USC 1030) from 1986[28], which gave DOJ lawyers[29] the foundational law to indict, charge, and prosecute computer crimes. The Soviet Union was the main nation state concern, China was silently organizing for the long game, non-nation state actors sometimes called "hacktivists" and organized crime were also beginning to learn, study, and exploit the rapidly developing internet.

---

[24] Cybercrime Magazine, "The History of Cybercrime And Cybersecurity, 1940 – 2020", November 30, 2020; https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/
[25] Center for Strategic and International Studies, "Significant Cyber Incidents"; https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[26] Norton, https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html
[27] Privacy International, "Five Eyes"; https://privacyinternational.org/learn/five-eyes
[28] Cornell Law School, "18 U.S. Code S. 1030 – Fraud and related activity in connection with computers"; https://www.law.cornell.edu/uscode/text/18/1030
[29] Department of Justice, "Prosecuting Computer Crimes"; https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

The visionary wisdom of Richard Clarke (and others) – but also the foundation for mass surveillance

27. Seminal national security visionary, Richard Clarke[30] began to understand the macro trend that while the American Government was establishing dominance in network enabled military warfare and intelligence collection as decisive Instruments of National Power, other forces were simultaneously exploiting our own networks.

28. Richard Clark along with others such as Admiral (Ret) Mike McConnell[31], and General (Ret) Mike Hayden[32] worked to develop the National Strategy to Secure Cyber Space[33]. This White House issuance in 2003, released while American and international partner forces were in Iraq to oust Saddam Hussain, established the future of both securing our networks and simultaneously ensuring decisive American freedom of movement at will through all other networks and the cyber environment. As with most unclassified, public facing national security issuances, there is normally voluminous Top Secret and compartmented activity behind such an issuance. The public facing document is merely the very tip of a much larger, concealed behemoth.

29. People, programs, and resources were being assembled, en masse to assert this 2003 strategy. In 2005, Secretary of Defense Donald Rumsfeld tasked General (GEN) James Cartwright, the Commander of Strategic Command, to establish the Joint Functional Component Command Network Warfare (JFCC-NW). GEN Cartwright turned around and tasked the NSA Director, Lieutenant General (LTG) at the time, Keith Alexander, to establish this entity.

30. In my office in the Pentagon, I established, what I called, my "Seminal Stack of Stuff" of documents, where I placed documents, I innately sensed as having enduring value, and placed hard

---

[30] Middle East Institute, "Richard A. Clarke"; https://www.mei.edu/profile/richard-clarke
[31] University of South Florida, "Former National Security Agency Director to lead Cyber Florida at USF"; https://www.usf.edu/news/2020/cyberflorida-gets-new-director.aspx
[32] National Security Institute, "General Michael Hayden (RET.)", https://nationalsecurity.gmu.edu/general-michael-hayden-ret/
[33] The White House, "The National Strategy to Secure Cyberspace", https://georgewbush-whitehouse.archives.gov/pcipb/

copies of them there, in addition to electronic storage. The three memos documenting the JFCC-NW arrangement were immediately placed into this stack. These documents were retrieved numerous times in the subsequent years, by myself, or my staff as core, historical artifacts for many more, future, follow-on branches, and sequels. Over the years, the "Seminal Stack of Stuff" grew voluminously.

31. All this work was the foundation of remote access at a massive scale – some of which overwhelmed, skirted, or was complicit with murkiness of the Foreign Intelligence Surveillance Court (FISA)[34] process. I knew and trusted many of the leaders overseeing these operations at the time but was also disturbed to find out later about the participation of some of these trusted, senior leaders in nefarious palace intrigue that leveraged these capabilities for personal political agendas. For example, in early 2018, General (Ret) Hayden sat 24 – 36 inches away from me coordinating his daily talking points in his almost daily phone call with James Comey, John Brennan, and others in their coordinated efforts to topple President Donald J. Trump.

32. The establishment of a mass remote access operations, while originally well intended, has now been rotated around to point at the American People. In 2010, the Washington Post presented a multi-part series entitled, "Top Secret America"[35]. We chuckled openly in Top Secret White House meetings and joked, "Well thank God they didn't find out about super double Top-Secret America" The Washington Post was on to something but didn't totally understand what they were seeing through the very foggy, windowpane.

Role of Remote Access Operations in dealing with dangerous regimes

33. Going a bit backwards to the immediate post 9/11 era, as we consolidated Coalition gains in Afghanistan, the American Instruments of National Power began to pivot and focus on chasing Al

[34] Foreign Intelligence Surveillance Court; https://www.fisc.uscourts.gov/
[35] Washington Post, "Top Secret America", July 21, 2010; https://www.washingtonpost.com/investigations/top-secret-america/2010/07/21/secrets-next-door/

Qaeda (AQ) throughout the world and working to factually establish the connectivity between AQ and Saddam Hussein – which was manifested in one trail by Abu Musab Al-Zarqawi (AMZ)[36]. In 2002, as AQ dispersed across the world from Afghanistan, one place some went to was Yemen. It was my Special Operations staff officer duty at this time, in the Chairman of the Joint Chiefs of Staff, J-3 Special Operations Division, to run a staffing action to resolve legal concurrence and recommend POTUS level approval and directive authority to eliminate an AQ cell in Yemen[37]. The gravity and scope of this action was immense, and it was my job, when necessary, be the scribe, negotiate, advocate, and receive the highest-level input for Secretary of Defense deliberation in the inter-agency on behalf of our immediate General, Stanley McChrystal[38], who will intersect again, later in this overview of remote access operations.

34. What does the Yemen event have to do with U.S. Government Remote Access Operations of critical infrastructure? A lot. Everything we knew on tagging, tracking, and locating these personnel with precision was based on the ability to establish remote access, full spectrum presence and dominance in all forms of critical infrastructure communications, networks, emissions, and signatures around the world. Part of this presence was the ability to deliver offensive, defensive, and exploitation effects. This nascent methodology worked, but it was labor and resource intensive, quite manual, and lacked automation to do this with multiple target tracks simultaneously.

35. In other words, presuming high precedence in the National Intelligence Collection priorities system, it could be done, but not on scale (scale meaning managing tens and hundreds of thousand simultaneous surveillance operations, not dozens. In IC idiom – moving out of the "hobby-shopped" micro-tailored solution culture of the IC, to surveilling at an exponential scale). This event was in the

---

[36] CRSR Report, "Al Qaeda in Iraq; Assessment and Outside Links", August 15, 2008; https://www.everycrsreport.com/reports/RL32217.html
[37] Journal of Conflict & Security Law, "'Targeted Killings' in an age of Terror: The legality of the Yemen Strike", Summer 2004; https://www.jstor.org/stable/26294308
[38] McChrystal Group; https://www.mcchrystalgroup.com/I

direct lineage of capabilities that led to remote access operations on scale as a normalized event. It was an iterative learning process and over time, this strategic reach became more routinized, efficient, and ubiquitous with greater numbers of personnel involved, but also with a dizzying exponential increase in "points of presence" (where information was gathered from) and simultaneous remote access operations. Conformance to law and mission guidance regarding civil liberties was being outpaced by the capability to conduct these remote access operations.

36. The intent of remote access operations was to establish full spectrum dominance of all forms of communication, information technology, and cyber in and around Iraq to project effects. Were these effects used to influence elections? According to a Foreign Affairs article[39], it was discussed but ultimately not implemented according to those interviewed. The wording in the article implies in my opinion, a declination of President Bush to approve a covert finding for the CIA to directly engage on the election and perhaps the direct method of manipulating vote tallies.

37. As time went on in Iraq and chaotic civil war broke out among several factions, we attempted different lines of effort to help establish civil society. Part of this was efficiently generating and delivering cyber effects into Iraq and relevant areas outside of Iraq. This was a complex inter-agency effort that revealed the conundrum between sharply focused and tailored Title 50 activities vis a vis the desire of Title 10 forces to conduct these operations on a much broader and routinized scale. These two different perspectives are a normal point of friction between these two worlds. At that time, Jen Easterly, now the Director of CISA at the Department of Homeland Security (DHS) appeared to have been a staff officer associated with the Tailored Access Office (TAO) of the National Security Agency (NSA) and was a key planner and integrator of the projection of capabilities. General Stan

[39] Foreign Affairs, "When the CIA Interferes in Foreign Elections A Modern-Day History of American Covert Action" June 21, 2020

McChrystal, who was now with the Joint Special Operations Command (JSOC) refined the art form of integrating Remote Access Operations to directly support his Commander's objectives.

38. I was working in this architecture of Military staffs, processes, and units as both a Joint Staff J-5 Middle East Staff Officer as well as an Office of the Secretary of Defense (OSD) Senior Civilian ensuring the achievement of national objectives as well as the deliberations to develop and approve the Execution Order for Countering the Adversary Use of the Internet ("CAUI,").[40], These efforts encapsulated the operational and directive authority for a family of worldwide remote access operations as well as what would become PPD-20[41] (the actual Top Secret PPD-20 may be on the internet, courtesy possibly of Edward Snowden), a follow on authority for the use of remote access operations which, in theory made the authority and approval of remote access more agile and responsive to a greater spectrum of senior leaders.

39. In a curious harbinger of issues with the 2020 election, retired General McChrystal made puzzling comments in May 2020 about his intent to use technology from this era[42], in coordination with the Lincoln Project to help ensure President Trump did not win the November 2020 election. This immediately received my attention and concern. His May 2020 announcement did not appear to receive much attention in the media. In my mind I had immediate questions – just what technologies? Were these remote access technologies from the Iraq era or beyond? Were these technologies lawfully obtained and used? Who was helping General (Ret) McChrystal? A retired General announces his intent to use US Government developed capabilities to influence a Presidential election and there is

---

[40] Committee on Armed Services, U.S. Senate, "Foreign Cyber Threats to the United States", January 5, 2017; https://irp.fas.org/congress/2017_hr/cyber-threats.pdf

[41] Executive Office of the President, "Fact Sheet on Presidential Policy Directive 20", January 2013; https://irp.fas.org/offdocs/ppd/ppd-20-fs.pdf

[42] Washington Post, "Technology once used to combat ISIS propaganda is enlisted by Democratic group to counter Trump's coronavirus messaging", May 1, 2020; https://www.washingtonpost.com/politics/technology-once-used-to-combat-isis-propaganda-is-enlisted-by-democratic-group-to-counter-trumps-coronavirus-messaging/2020/05/01/6bed5f70-8a5b-11ea-ac8a-fe9b8088e101_story.html

little intellectual curiosity from media or "experts" in the field? He certainly wasn't going to conduct these technical remote access-like operations personally. Exactly how were these capabilities going to be used and just how was he going to use them lawfully now that he was a private citizen running a private business?

40. This is one of many examples of the blurring of trained cyber personnel in government service, or under contract to the U.S. Government and the transition of this government developed tradecraft[43] for uses outside of statute-based activities. This work is supposed to be classified and controlled. Yet this transfer, seepage, and escapage is not an uncommon thing. Any use of these capabilities could implicate federal law starting with the CFAA. Nothing here made sense to me, despite a compelling obligation for the Department of Justice to issue a referral to the FBI to investigate a retired being in possession of software and technical access capabilities.

41. Sharyl Attkisson has had to deal with this as ex/former FBI personnel like Shaun Bridges[44] have allegedly used remote access capabilities developed in-house, in post government service. A culture of remote access capabilities has now become ubiquitous and perhaps commoditized. What was nurtured in classified environments has escaped, one way or another, into the wild.[45]

42. There is distinct mimicry of American efforts by great power competitors, China and Russia, and their sidekicks of Iran and Venezuela. From my almost 40 years of experience, I have seen this repeatedly – we lead and innovate, our competitors then copy us. A computer virus called Stuxnet[46],

---

[43] The Verge, "Hackers reportedly used a tool developed by the NSA to attack Baltimore's computer systems", May 25, 2019; https://www.theverge.com/2019/5/25/18639859/baltimore-city-computer-systems-cyberattack-nsa-eternalblue-wannacry-notpetya-cybersecurity

[44] Nittany Nation, "Former govt. agent admits illegally spying on Sharyl Attkisson, implicates govt. colleagues", January 9, 2020; https://bwi.forums.rivals.com/threads/former-govt-agent-admits-illegally-spying-on-sharyl-attkisson-implicates-govt-colleagues.257893/

[45] Atlantic Council, "Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets", November 8, 2021; https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/

[46] C/NET, "Stuxnet delivered to Iranian nuclear plant on thumb drive", April 12, 2012; https://www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/

was planted by someone into the Iranian nuclear environment, and Agent BTZ[47] was planted right back onto U.S. Government networks in a seemingly copycat attack, leveraging very similar techniques. Some may argue this as sheer coincidence, but in this gray shadow world, coincidences are often not.

43. The Chinese especially, fastidiously, laboriously, and almost to comic levels study and analyze everything, everything we say and do. If we possibly used remote access operations to enter critical infrastructure and influence events, the Chinese surely studied our efforts and applied these same capabilities and strategies. Totalitarian nations such as China, Russia, Iran, and Venezuela were always watching us, and starting with China's relentless intellectual property theft and destruction of the American economy since the 1990s and Russia's cyber aggression against Estonia in 2007, that's exactly what happened – and they have used remote access operation tactics, techniques, and procedures they often watched, studied, and learned from us.

Securing the American cyber world (and American dominance with absolute freedom of maneuver in cyber): The CNCI program established the BC/AD of remote access operations on scale

44. The CNCI effort was a grand, bold, and expensive move forward to help America re-establish dominance in the cyber arena as it was realized that threat actors were de-stabilizing and taking advantage of the American public and private information technology sectors. There were 12 publicly announced initiatives in the CNCI program[48].

[47] Council on Foreign Relations, "Agent.btz", November 2008, https://www.cfr.org/cyber-operations/agentbtz
[48] IT Law Wiki, "The Comprehensive National Cybersecurity Initiative (CNCI)", https://itlaw.wikia.org/wiki/Comprehensive_National_Cybersecurity_Initiative#Citation

Table 1: CNCI Projects and Lead Agencies

Project	Description
Trusted Internet Connections	Reduce and consolidate external access points with the goal of limiting points of access to the Internet for executive branch civilian agencies
Einstein 2	Deploy passive sensors across executive branch civilian systems that have the ability to scan the content of Internet packets to determine whether they contain malicious code
Einstein 3	Pursue deployment of intrusion prevention system that will allow for real-time prevention capabilities that will assess and block harmful code
Research and Development Efforts	Coordinate and redirect research and development (R&D) efforts with a focus on coordinating both classified and unclassified R&D for cybersecurity
Connecting the Centers (includes National Cyber Security Center)	Connect current cyber centers to enhance cyber situational awareness and lead to greater integration and understanding of the cyber threat
Cyber Counterintelligence Plan	Develop governmentwide cyber counterintelligence plan by improving the security of the physical and electromagnetic integrity of U.S. networks
Security of Classified Networks	Increase the security of classified networks to reduce the risk of information contained on the government's classified networks being disclosed
Expand Education	Expand education efforts by constructing a comprehensive federal cyber education and training program, with attention to offensive and defensive skills and capabilities
Leap-Ahead Technology	Define and develop enduring leap-ahead technology, strategies, and programs by investing in high-risk, high-reward research and development and by working with both private sector and international partners
Deterrence Strategies and Programs	Define and develop enduring deterrence strategies and programs that focus on reducing vulnerabilities and deter interference and attack in cyberspace
Global Supply Chain Risk Management	Develop multi-pronged approach for global supply chain risk management while seeking to better manage the federal government's global supply chain
Public and Private Partnerships "Project 12"	Define the federal role for extending cyber security into critical infrastructure domains and seek to define new mechanisms for the federal government and industry to work together to protect the nation's critical infrastructure

Figure 4: The 12 public facing "Initiatives" of CNCI

45. I was a key player in the de-classification of the 12 CNCI initiatives, which was a grueling and resource consuming bureaucratic exercise.

Figure 5: The "60 Day" Report under the Obama Administration, May 2009

46. The CNCI Program resided in the Intelligence Community (IC) under Title 50 and its budget, National Intelligence Program[49] (NIP), which is not publicly revealed except in aggregate at the end of the Fiscal Year. For the layperson, this is the world of "Black" programs. This is the budget for everything "off book", "black", or whatever other moniker is appropriate. It was my job from 2007 – 2014 to act as the senior DoD lead working in conjunction with OMB, the DNI, DHS, and the DOJ to ensure these CNCI funds were properly deployed, obligated, implemented, and effectiveness measured.

[49] Office of the Director of National Intelligence, U.S. Intelligence Community Budget; https://www.dni.gov/index.php/what-we-do/ic-budget

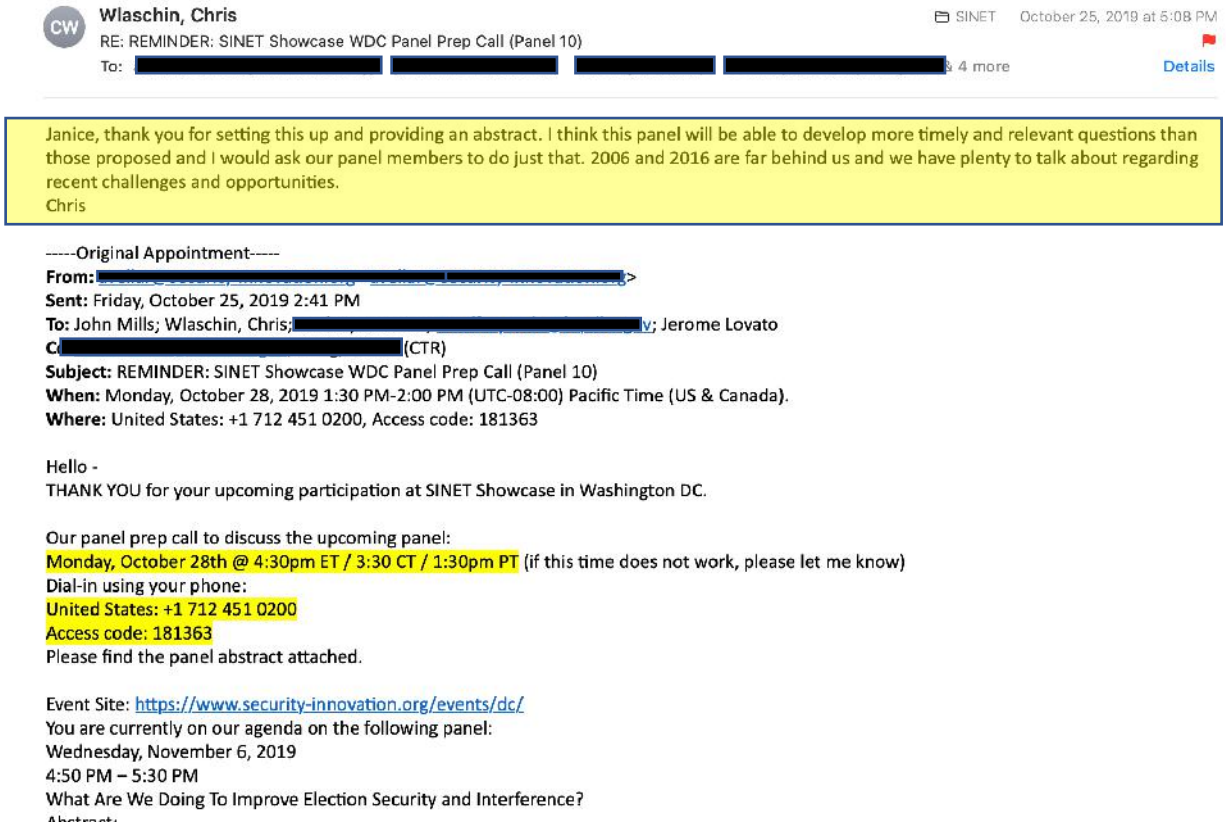
47. As the Obama Administration was seated after inauguration, they directed a sweeping "60 Day" review[50] of the CNCI effort. I participated in drafting the report which was well received in the Administration.[51] Again – behind the veil of the 12 announced initiatives shown above, other capabilities lurked involving big data collection, sorting, and analysis on a scale never seen—capabilities now seen as routine as with the public's addiction to Amazon and Google search. Simply put, these behind the veil programs established a historical inflexion point with an unprecedented ability to access, exfiltrate, analyze, and change information in critical infrastructure, which includes electronic election systems—on scale regardless of what it was or where it was. Our Great Power Competitors and their lackeys have once again, studied, and replicated our efforts.

48. One curious oddity of my time with CNCI and the White House was the reference to the cessation of the effort[52] to find out more about the Smartmatic Voting Machine System[53] and their curious footprint in Venezuela. At the time, it was one of many factoids/quick blurbs that came and went. In my professional viewpoint, Venezuela is acting as a foreign base camp and covert base of adventurist opportunities for China, Russia, and Iran in our home hemisphere, and it should be of significant intellectual interest as to why foreign powers are creating voting machine software in Venezuela[54]. In November 2019, I was asked to lead a cybersecurity panel on the security of Election Machines at a cyber investors event at the Washington Press Club. Jerome Lovato[55] of the Election Assistance Commission (EAC), was going to be part of the panel and he asked if Chris Wlaschin of

---

[50] Eric A. Greenwald, "History Repeats Itself: The 60-Day Cyberspace Policy Review in Context", https://jnslp.com/wp-content/uploads/2010/08/05_Greenwald.pdf
[51] Executive Office of the President, "Cyberspace Policy Review", May 2009, https://irp.fas.org/eprint/cyber-review.pdf
[52] https://www.nytimes.com/2006/10/29/washington/29ballot.html
[53] Voter Action, "SEQUOIA VOTING SYSTEMS, INC. USES VOTE-COUNTING SOFTWARE DEVELOPED, OWNED, AND LICENSED BY FOREIGN-OWNED SMARTMATIC, A COMPANY LINKED TO THE VENEZUELAN GOVERNMENT OF HUGO CHÁVEZ", June 12, 2008; https://www.nist.gov/system/files/documents/itl/vote/SequoiaSmartmaticReport61208.pdf
[54] G News, "The link Between Dominion, Sequoia, Smartmatic, and the CCP", November 21, 2020; https://gnews.org/577635/
[55] Fulcrum, "Federal slap on the wrist for a voting equipment maker's misleading claims", August 14, 2020; https://thefulcrum.us/election-security-2646984614

Election Systems & Software ("ES&S"), one of the election machines companies, could also be on the panel. It is interesting that Wlaschin, an invitee of Lovato, swiftly dismissed my proposed agenda to address Venezuela and election machine software development. Wlaschin's response shown below which included the reference to Venezuela and election machine software (Please see Figure 6 and 7 below).



Wlaschin, Chris SINET October 25, 2019 at 5:08 PM
RE: REMINDER: SINET Showcase WDC Panel Prep Call (Panel 10)
To: [redacted] & 4 more Details

Janice, thank you for setting this up and providing an abstract. I think this panel will be able to develop more timely and relevant questions than those proposed and I would ask our panel members to do just that. 2006 and 2016 are far behind us and we have plenty to talk about regarding recent challenges and opportunities.
Chris

-----Original Appointment-----
From: [redacted]>
Sent: Friday, October 25, 2019 2:41 PM
To: John Mills; Wlaschin, Chris;[redacted]v; Jerome Lovato
C[redacted](CTR)
Subject: REMINDER: SINET Showcase WDC Panel Prep Call (Panel 10)
When: Monday, October 28, 2019 1:30 PM-2:00 PM (UTC-08:00) Pacific Time (US & Canada).
Where: United States: +1 712 451 0200, Access code: 181363

Hello -
THANK YOU for your upcoming participation at SINET Showcase in Washington DC.

Our panel prep call to discuss the upcoming panel:
Monday, October 28th @ 4:30pm ET / 3:30 CT / 1:30pm PT (if this time does not work, please let me know)
Dial-in using your phone:
United States: +1 712 451 0200
Access code: 181363
Please find the panel abstract attached.

Event Site: https://www.security-innovation.org/events/dc/
You are currently on our agenda on the following panel:
Wednesday, November 6, 2019
4:50 PM – 5:30 PM
What Are We Doing To Improve Election Security and Interference?
Abstract:

Figure 6: Email Exchange where Mr. Wlaschin dismisses my proposed agenda points referencing Venezuela and Election Machine software development.

structure today is over seen by local jurisdictions and conducted mostly by volunteers. It was not designed or created in the context of delivering voting resilience in the face of determined adversaries – but that is the reality today. This panel will discuss some of the challenges – but also some of the reasonable ways ahead to provide higher levels of assurance and confidence in the voting system.

Scope and Scale of US Elections

Roughly 114,000 Polling Stations nationwide

Roughly 174,000 Precincts

Roughly 350,000 voting "machines" in the system

Precinct size is roughly 1,100 voters

Low end is roughly 437 in Kansas/2,704 in DC

Potential Questions:

Who here has helped run an election (been an "election official") in the US and/or overseas?

How can technology make things better?

A NYT October 29, 2006 article talked about a US investigation into Smartmatic/Sequoia and Venezuela – what ever happened to that?

Is diversity of voting machines and processes helpful or a vulnerability?

Would standardizing methodologies across all 174k precincts help or make things worse?

Figure 7: Agenda Attachment to Email Exchange where Mr. Wlaschin dismisses my proposed agenda points referencing Venezuela and Election Machine software development.

49. During my government service I witnessed the development of a close relationship between the Obama / Biden Administrations, the Federal Government and Big Tech in Silicon Valley. The beginnings of this relationship can be traced in part to the 2006 – 2007 timeframe when the Commander of a Combatant Command had his Facebook site hacked. At the time, the Department of Defense didn't really have firm policy on social media usage or protection of the public personae of senior personnel. I was called in and told by the senior, Senate Confirmed Assistant Secretary of Defense to figure it out and give control of the account back to the Combatant Commander. I simply picked up the phone and after a few calls was talking to former DOJ prosecutor, then Facebook Chief

Security Officer Joe Sullivan[56]. With no formal process or memorandum of agreement in place, within the day, the Commander had his Facebook account back. Establishing and formalizing the Silicon Valley and DOD/U.S. Government relationship became one of my core missions from 2009 to 2016 in addition to CNCI, and it has now been memorialized as the DIU[57].

Office of Personnel Management – a massive Chinese remote access operation with horrific and real results

50. While significant people, programs, and resources were being generated by CNCI, the Chinese conducted a massive remote access penetration and exfiltration operation focused on the obscure, and not well known, Office of Personnel Management ("OPM"). This was a brilliant flanking action by Chinese intelligence to "vacuum up" massive amounts of information and illustrates how American critical infrastructure involving electronic systems can be penetrated through remote access operations. The more recent Solar Winds breach is one more example of a nation state using remote access operations to penetrate a critical infrastructure network (including U.S. Government Departments and Agencies) and planting enabling malware (one may also say algorithms) to enable further distribution of the malware and embedding the malware/algorithm into updates which created broad and pervasive presence through many customer networks using Solar Winds Orion software. This was one more example of the relative ease of the offense penetrating the defense and spreading broadly, perhaps for years, and establishing a decisive position to monitor, surveil, steal, and manipulate data[58]. This breach also illustrates how thousands of systems can be hacked in a coordinated fashion, and shows how the

[56] Wired, "A Former Uber Exec's Indictment is a Warning Shot", August 21, 2020; https://www.wired.com/story/uber-exec-joe-sullivan-data-breach-indictment/
[57] Defense Innovation Unit; diu.mil
[58] Trenton System, "SolarWinds Orion Hack Explained", https://www.trentonsystems.com/blog/solarwinds-hack-overview-prevention

belief that our electronic voting systems are more secure by being purportedly decentralized is a false notion

51. The decisive way China conducted the OPM breach demonstrated the ease at which a peer competitor could access a U.S. Government "trusted" critical infrastructure network, install enabling malware, and exfiltrate data on a massive scale. The crown jewel of this massive theft through remote access[59] were the hundreds of thousands or more SF-86's[60]—the key U.S. Government form that comprehensively documents all of the information about a person's history and background for those seeking or renewing a security clearance that were taken. CNN reported 21.5 million Americans were exposed in this breach[61] which started, perhaps around 2013, just as CNCI was hitting full operational capability. These files contained expansive details about everyone who has or had security clearances. The FBI has made some arrests – one Chinese personality was so brazen as to be traveling in the U.S. at the time of his arrest[62], however the loss has been catastrophic.

52. According to one report – the CIA's agent network was destroyed in China[63] and the Chinese aggressively used the information derived in the breach for spying operations[64]. It is very likely Chinese nationals were arrested and dispensed with from this historic, catastrophic security breach. I lived through the response actions inside the Government. This episode must be highlighted as an

---

[59]CSO, "The OPM hack explained: Bad security practices meet China's Captain America
How the OPM hack happened, the technical details, and a timeline of the infiltration and response." February 12, 2020 https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

[60] Big data analytics can consume this information and cross reference, analyze and find interesting connections and lack of connections that can be ques for intelligence analysis. https://www.opm.gov/forms/pdf_fill/sf86-non508.pdf

[61] CNN, OPM Data Breach, July 9, 2015, https://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/index.html

[62] The Hill, FBI arrests Chinese national linked to OPM Hack Malware, https://thehill.com/policy/cybersecurity/347897-fbi-arrests-chinese-national-linked-to-opm-hack-malware-report

[63] CNN, "U.S. pulls spied from China after hack", https://money.cnn.com/2015/09/30/technology/china-opm-hack-us-spies/

[64] Schneier on Security, December 24, 2020, https://www.schneier.com/blog/archives/2020/12/how-china-uses-stolen-us-personnel-data.html

example showing the scope and effects of remote access operations. There is no reason to believe that our electronic election systems infrastructure could not be similarly penetrated and manipulated.

The Cyber Response Group (CRG) handles the hardest Cyber Problem Sets

53. From about 2008 – 2014, I was one of a small group of inter-agency players involved in a group called the CRG. The purpose of this group was to work the hardest problem set of weaknesses of the American cyber critical infrastructure to foreign remote access operations and turn these into opportunities for American counter moves back into the threat environment to hold our adversaries at risk. The name morphed over time and the small, inter-agency group appreciated my unique and actionable insights. In approximately 2014, because of shifting priorities, I no longer attended the CRG meetings, but I often heard updates of their work in in regular internal cyber coordination meetings. Usually, it was the representatives from Undersecretary of Defense for Policy, starting with Eric Rosenbach who would share these hints. In 2016, references to Russian and Chinese interference into the American election process began. The references identified their intrusions into campaign networks. Iran was also a regular threat nation identified.

54. At other times, I observed references being made by senior officials on the clever use of information FVEYES partners provided to spy on Americans. These FVEYES techniques were long standing and pre-existing as a possibly lawful end-around the FISA process, but rarely used. The unlawful un-masking operation against Trump Campaign personnel, revealed later, caused me to believe that the CRG Group was possibly the group and entry portal for compartmented activity to support spying on the Trump Candidacy and nominate names for un-masking. Several days after the election in November 2016, I was called by a group member on the classified phone and asked to participate in the production of the ICA to finalize the Russian Narrative with Trump as a Russian asset with the purpose of delaying the January 2017 inauguration of President Trump. Now we know

through the de-classifications by Mr. Richard Grennell and Mr. John Ratcliffe, that Comey and Brennan knew the Russia Story was false, but they personally pushed through an ICA (which I non-concurred with during my assigned review, due to the lack of substantiating detail) in late November 2016 to January 2017 to frame President Trump and potentially block his inauguration.

Failure of the U.S. Government to Secure the American Election Environment

54. One point of concern that is relevant are the assertions by U.S. Government Officials on the security of U.S. election critical infrastructure against remote access operations. Election security was a topic raised several times while I was in office. As I become knowledgeable of the election process in the United States, since leaving office, and knowing a fair amount about the maturity, ability, operations, and true, overall priorities of the different U.S. Government Cybersecurity Centers such as CISA, the NSA Threat Operations Center (NTOC), the FBI National Cyber Investigative Joint Task Force (NCIJTF)[65], and other U.S. Government entities, while the leaders and personnel are of high caliber and well meaning, they simply do not understand the election system, process, nor equipment.

55. Around the November 2020 election, representatives of CISA, including Mr. Chris Krebs, Director of CISA, made strong assertions of election security such as "[t]he November 3rd election was the most secure in American history." In my professional opinion, such statements are false because, in my observations and decades of experience within government, the U.S. Government does not have the people, programs, or resources to have a comment on the true resilience and security of the election critical infrastructure.

[65] FBI, NCIJTF, https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force

56. In addition, two things Mr. Krebs did, significantly undermined his credibility. First was his tweet on November 18, 2020, where Mr. Krebs backtracked on his previous assertion of that the November 2020 election was secure.

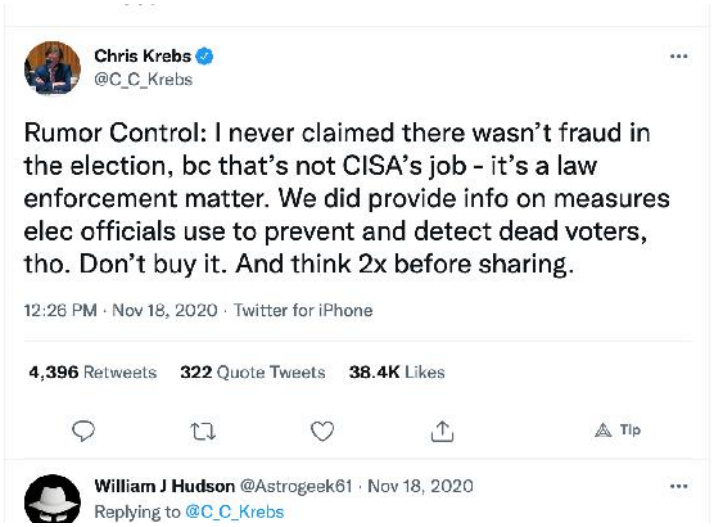


Figure 6: Mr. Chris Krebs Tweet on November 18, 2020

57. The second was Mr. Krebs congressional testimony on February 10, 2021[66], where his statement was replete with comments on the shortage of people, programs, or resources to provide effective cybersecurity of the American election environment. From Mr. Krebs statement, it is hard to reconcile his February 10, 2021, statement with the statement he approved from November 12, 2021:

> "It is hard to overstate the massive scope of the critical infrastructure security and resilience challenge. The levers government has at its disposal to change behaviors, on the other hand, is underwhelmingly small.

[66] Christopher C. Krebs Testimony before Committee on Homeland Security, February 10, 2021, https://docs.house.gov/meetings/HM/HM00/20210210/111152/HHRG-117-HM00-Wstate-KrebsC-20210210.pdf

This leads to three conditions limiting the ability of government and industry to collectively improve critical infrastructure cybersecurity: (1) lack of a deep understanding of what is truly systemically important across the economy, (2) a need for more meaningful methods for operational engagement with industry to address risk; and (3) insufficient funding and investment in security improvements. "

58. Knowing these things, and the maturity of CISA, in my professional opinion, Mr. Chris Krebs was in over his head with attempting to lead a U.S. Government agency. He should have been more transparent on the state of affairs, yet if he did, it likely would have revealed a political appointee unable to exercise effective leadership of an organization.

59. In my professional experience and opinion, it is of low probability that the national intelligence collection system was specifically looking for Chinese intervention into any election system infrastructure or components. The catastrophic Target Corporation (The Target retail store) breach[67] demonstrated how a threat actor can remotely obtain access into key information of an enterprise through related but different critical infrastructure such as facility climate control networks (i.e., HVAC Heating, Ventilation, Air Conditioning). The Target Corporation breach was closely followed and studied within the U.S. Government. It is of note that none other than Chris Krebs identified this capability of remote access through a related system in a 2014 article on the Target Breach[68].

In my professional opinion, assertions by state and federal officials that electronic election systems in our Country are secure from remote access operations have little basis in fact and are false. My

[67] ZDNet, "The Target Breech, two years later", November 27, 2015, https://www.zdnet.com/article/the-target-breach-two-years-later/

[68] KrebsonSecurity, Target hackers Broke in via HVAC Company, February 14, 2015, https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

opinion is further supported by other computer science experts such as University of Michigan Professor J. Alex Halderman.[69]

I declare under penalty of the perjury laws of the State of Virginia and the United Sates that the foregoing is true and correct and that this declaration was executed this 21st day of November 2021 in Woodbridge, Virginia

Colonel, USAR (Retired) John R. Mills
November 21, 2021

[69] Declaration of J. Alex Halderman in support of Motion for Preliminary Injunction, Civil Action No. 1:17-CV-2989-AT stating 16 states using Dominion machines can have votes "stolen" by "nefarious actors" and begging the court unseal his report on these issues to allow CISA to try and fix these vulnerabilities before the 2022 election.