SEPT. 11, 2001 TO RUSSIAGATE 2015-2020

Why Veteran Intelligence Professionals Demand Shutdown of the Illegal Surveillance State

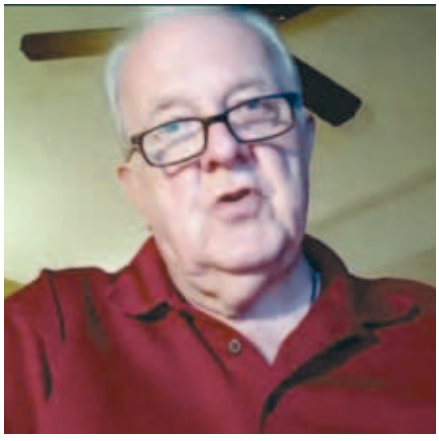
Dialogue with Bill Binney and Kirk Wiebe

This is the edited transcription of the prerecorded dialogue with Mr. Wiebe and Mr. Binney, for the Schiller Institute conference on September 5. Wiebe is a former Senior Analyst, National Security Agency. Binney is the former Technical Director of the World Geopolitical and Military Analysis and Reporting section, National Security Agency.

Q: Mr. Wiebe spent over 25 years at NSA [National Security Agency]. Then 9/11 occurred. Could it have been stopped by the ThinThread team?

Schiller Institute

Bill Binney



Schiller Institute

Kirk Wiebe

Kirk Wiebe: For most of my time at NSA from 1975 until we walked out of the building on Halloween Day 2001, I was involved in very interesting work. I used my language [skills], a lot of it doing what we call "transcription," which is rendering Russian speech into printed Russian or transliterated Russian, for analysis by others. And then, after putting in a good stint in the transcription area, I did some staff work on Five Eyes partnerships, the Five Eyes meaning NSA; Canada, CSE it's called; GCHQ of United Kingdom; New Zealand; and then Australia. Those are the Five Eyes that have a particularly close partnership on intelligence matters.

Then, after that bit of staff work, I went into collection, data collection and data processing, managing those things for analysts that were studying the Soviet Union, and that opened a whole lot of other channels in terms of experience, collection of data, different types of collection, different types of data, and all the processing requirements to go to the technical capabilities against various kinds of signals.

And then I was selected to move into analysis, and headed up a top-priority requirement that came down from President Reagan, called "National Security Decision Directive #178," which had to do with strategic relocatable targets, which is really a technology that you use to confuse targetting efforts by an enemy. In other words, rather than having stationary headquarters, you put your headquarters in mobile kinds of vehicles and things of that nature, maybe on a train, maybe on a plane. The whole issue of strategic, relocatable targets, including missiles put on trains and vehicles, was the subject for which I was eventually awarded the second-highest award that NSA confers, the "Meritorious Civilian Service Award"; also received the Director of Central Intelligence's "Meritorious Unit Award," recognizing my whole branch at NSA of about 70 people for their work on that topic.

And after that, I went into some other types of staff functions, associated with higher management, and it was about that time that Bill Binney bent my ear and said, "Why don't you come down to our little research center?" I knew who Bill was, but I didn't know what he was doing at the time. So, I went down and saw what they were doing, and to me, it was NSA's future, because they were dealing no longer with channel-switched networks, radiofrequency-based networks,

but packet-switched networks, in other words, the internet, TCPIP [Transmission Control Protocol/Internet Protocol]; and what did that mean for NSA's future in terms of a source of information, its breadth, what were the implications technologically, and so forth.

So, my last assignment was working with Bill on that particular vexing problem. I say "vexing," because the three issues with the internet are velocity of data—it's fast, it runs along a wire at the speed of light; the variety of data—a lot of different types of applications and uses; and the volume—huge volume, especially as the internet grew globally, and I'd hate to estimate that there's probably 60 terabytes generated every minute in global data. So, anyway, that was really fun.

But our solution that we developed, that a lot of people have heard of—it's called ThinThread—flew in the face of NSA's intentions to get a big budget from Congress and spend big dollars on the military-industrial complex, and it's a problem that we solved for a few hundred thousand or at least no more than a million or $2 million, and NSA wanted a $4 *billion* budget to solve the problem. So our little solution was squashed, in favor of big project mode that failed five years later under the director's Trailblazer program.

At that point, Bill and I and Ed Loomis walked out of the building on October 31, right after 9/11, because we were heartbroken that our little solution, that was very effective and efficient, had not been put into the fight against terror, and we saw the result. Am I 100 percent sure ThinThread would have prevented 9/11? Yeah. I am. We knew what to target. We knew where the sources were, what we needed to target, and to be honest with you, if you ask Tom Drake, another one of the NSA whistleblowers that came later, he'll tell you that after we left, he found 9/11 information in NSA's database that predicted the event. He also told us that an analyst at NSA, a group—not just one, but a small team—already knew that 9/11 was going to happen, and was going to put out a report, but was prevented from doing so by the Director of NSA, Michael V. Hayden. I wish I could tell you why; I have lots of guesses, but that's a topic for another day.

Q: *What was ThinThread?*

Wiebe: ThinThread began in a small research organization of about 12 people as an experiment. Whenever you have a technical problem to solve, you get some good people together and you talk about ways to try to attack it, and you have a bunch of failures, and then you begin to succeed in small steps. And so we advanced our understanding of how to go after the internet as a source of intelligence. And like I said, there were three main issues we had to solve: There's the velocity, the stuff's moving along a wire in real time; and there's a lot of variety in it, there's some text, there's some speech, there's some video, there's some this and that, and different layers of the internet involved, the seven OSI [Open Systems Interconnection] layers—which one of those layers is important for intel, which ones aren't so much, especially when you have small dollars and you're trying to make a research breakthrough, where are you going to put those dollars against what's in the internet?

And then the volume of data is horrendous, so it's like trying to sip from a firehose: How do you extract data intelligently, and not inundate your database? So, I think what they did in the SIGINT [Signals Intelligence] Automated Research Center, SARC, we called it, was absolutely amazing.

ThinThread was essentially a method of extracting data from the internet in real time—almost real time, there was a slight buffering. And sort it: We couldn't collect communications of U.S. sources, of U.S. persons, and so we had to understand the addressing system, the IP [Internet Protocol] allocations in order to build a filter that would shunt any data that was not to be surveilled, because of the law and the rights of Americans under the Constitution, but allow other things that were fair game, in other words, all other communications other than U.S., all foreign communications, because that's NSA's charter, foreign intelligence.

And then, having collected this data, that's not enough. So now you've got a bunch of data, you have to sort through it, organize it, and connect the dots where you can, so that the greater picture is understood. And so the name ThinThread is a little bit of a misnomer, and if you talk to the developer of ThinThread, Ed Loomis, he'll tell you it's a direct misnomer! But because the press have picked up on this name, Bill and others have felt, rather than go through the long explanation of how ThinThread is different from the analytic backend, and there are other names for those programs that Bill developed, he just decided to settle on ThinThread because it was in the public and it wouldn't lead him down a potentially sensitive path, where systems are still in use and you don't want the names of them in the public domain.

So, ThinThread is technically just the data grabber, if

you will, and the data sorter in terms of what's legal and what's not, and, the dictionary lookup, looking for topics in emails and/or attachments that hit a list of key words reflecting interests of analytics. Interesting topics.

And then, putting those filters against this data stream to cull out the stuff worth looking at, and then putting those communications in a connect-the-dots system, so that if José is talking to Dennis, you'll see the link between their two emails or their two phone calls, or whatever it may be. You need to link things up so that you can understand an activity and see who's involved in it at any given moment in time.

So that gives you a little bit of the flavor of ThinThread, and it was the initial breakthrough in the ability to take a large chunk—a fairly large, I mean, a reasonably large section of the internet, and exploit it.

Q: *Cyber-"personality" Guccifer 2 claimed to have hacked the Democratic National Committee [DNC]. Further, Guccifer 2 is the supposed "Russian link" that proved interference in the 2016 American Presidential elections. Who/what is Guccifer 2?*

Bill Binney: The Guccifer data that we looked at, we clearly showed the speeds of the downloads of that data to a thumb drive were possible, but it was not possible to send that data across the internet to Russia or anywhere else outside the United States basically—or even inside the United States to a lot of places. They couldn't get it because they don't have these high-speed lines to carry that kind of rate transfer. We proved that. Not only did we show the speeds that were involved, but we also showed you couldn't do it. We tried to do our transfer from Albania, from the Netherlands, from the UK. The further east we got, the less speed we got; the lower speed. We couldn't achieve the higher speeds going East, it went down.

But after that, also we looked at the data that Guccifer 2 published, both on the 15th of June, the 5th of July, and the 1st of September. The two files he published on the 1st of September and the 5th of July 2016, if you look at them and only look at the minutes, seconds, and milliseconds, you could shuffle them together like a deck of cards without conflict. That says the guy is playing a game with the data. He did one download, split it into two files, did a range change on the date and a range change on the hour. Because he couldn't do it on the minutes because it crossed many minutes, and he couldn't do it on the seconds or milliseconds because there were many of those. So, he could only do a range change on the date and the hour, which is apparently what he did, because those two files merge into one. That said, he was playing with the data.

Then on the 15th of June, he published some articles showing that the files had Russian fingerprints in it. Our affiliates doing the research with us in the UK looked at that data, and found that five of those files they also found in the Podesta email documentation by Wikileaks that was posted, I think, on the 21st of September. That was at least the time they had it. So, the point was, those files that were in the Wikileaks publication didn't have any Russian fingerprints. So that meant Guccifer 2 inserted those fingerprints.

Then we went back to the [WikiLeaks] Vault 7 material where the Vault 7 material said the program, Marble Framework, was a program that made it look like other countries did the hack, when in fact, the CIA did the hack. Well, they were able to mimic or make it look like the Russians, the Chinese, the North Koreans, the Iranians, or Arabs did the attack. So, they could attack anybody and leave fingerprints making it look like someone else did it. When you looked at it, that meant to us that Guccifer 2 was using some kind of program, or some kind of process to insert those fingerprints into the data from the DNC. On top of that, in the Vault 7 material, it said there that the Marble Framework program was used one time in 2016. Well, we think we found it. That says to us that all the evidence we've been accumulating forensically from the outside, is pointing back at CIA as the origin of Guccifer 2.

So, their entire allegation about you, and the Russians, and everybody has a false premise to start with. So, everything that they introduce as the reason they went after you—and also General [Michael] Flynn—was what I think lawyers call "fruit of the poisoned tree." They set it up; they manipulated it; they contrived it; and they executed it. You and General Flynn, and they tried to also put us in jail under the Espionage Act, by fabricating evidence against us, too. So, it's really how can we ever trust the FBI until [Attorney General William] Barr and [U.S. Attorney for the District of Connecticut John] Durham really clean it up?

Q: *What does the rise of the "illegal surveillance state" mean for the American people, and the world? What must be done about it?*

Binney: We Americans should be really concerned about the bulk acquisition of data by NSA and the "Five Eyes" and the other countries around the world, be-

cause what it's doing is capturing everything that everybody's doing electronically in the world, and tracking you wherever you are, as you move around, day by day, minute by minute.

Which means they can retroactively analyze anything that you've done in the past at least 19 years.

This has been done before. It's used against people to stop them from doing some things the government doesn't want, like for example, when Eliot Spitzer went against the bankers on Wall Street, trying to take them to court for defrauding people in the 2007-2008 financial crisis. They used that data to find something against him, to leverage him, and get rid of him.

The point is, that this data, when given to governments, or people in general, sooner or later, the power they have, *they use;* and they use it against *you.*

There are ways to fix this. The way to do it is to force them into doing a focussed, disciplined, targetted approach—just like the police do when they are investigating a crime. Here, all they have to do is use deductive, inductive and abductive logic, to look at people who are associated with or known to be bad people for whatever reason [such as] criminal activity, or leaders of countries, or governments, or military, things of that nature, and focus on them and one degree from them, as the basis for the investigation of content, as well as metadata.

But then, you need to look beyond that, to the next degree, as long as you don't go through a company or a government agency that would expand you into collecting *massive* numbers of people who aren't relevant to *anything.*

By doing this, what it will do, basically this approach would have found virtually all of the terrorist attacks and all of the criminal activity before 9/11, for 9/11, and after 9/11, still it would work.

The problem now is they have so much data—they're using dictionary select as a way of doing it—word searches, phrase searches, things like that. And when you go through the massive amounts of data they're collecting, it gets a ton of material dumped on people, they can't see the threats coming, and they're dysfunctional at that point.

So, the attacks happen, people die, and then they clean up the mess afterwards, and then go in and look. Once they know who did it, they can look at all the data they've compiled on him. That's a forensics job, not an intelligence job.

So, the idea is if you do that, and you also do things like inductive logic, where you're looking at people, where they're visiting sites on the web—are they looking at sites that advocate pedophilia, violence against the West, any kind of criminal activity. Then, that's an indication that they're in what I call the "zone of suspicion." And that's what people need to investigate, to see if they're also involved. If they are, then they can develop information to justify a warrant, based on probable cause behavior in the communities in which they are involved. And you can solve this.

This would give privacy to everybody in the United States and around the world. And also create a rich environment for intelligence analysts and the police to look at, to solve problems and prevent attacks.

So, it's solvable. We can do that. All we have to do is force our government to abide by our Constitution and make them do a focussed, disciplined, professional job.