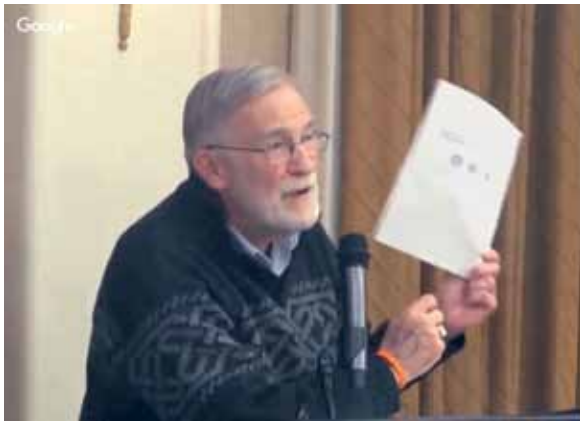
BINNEY TO LAROUCHE PAC IN MANHATTAN

The Russian 'Hack' Is an Obvious Fake

William E. Binney was formerly NSA (National Security Agency) Technical Director for World Geopolitical and Military Analysis, and Co-founder of NSA's Signals Intelligence Automation Research Center. He resigned from the NSA on Oct. 31, 2001, after more than 30 years with the agency. The following is an edited transcript of Binney's presentation to the special LaRouche PAC Manhattan Town Hall Meeting of Jan 5.

William Binney: Thank you. I'd like to make a comment about some of the British intelligence and how they were the "experts of the world." That was true until about the late 50s, early 60s, and then I came to NSA. I was never impressed with anything they did. On matters concerning the Soviet Union and the Warsaw Pact—they referred to me as the "Bottom Line." So, I had the title of being the Bottom Line. I thought that was a cute title. I used to send them "woozlegrams" all the time; every time I would solve a system, I would take it through, step by step, how the solution worked and how you could figure it out, so that they could do it, too. That was part of the reason they called me the Bottom Line. That is, I figured out so many things; I figured out all kinds of secret things that nobody ever saw and didn't know about. Even the Russians didn't know they had it. But if you did the things I did, which was a lot of fun, you could figure out all the things they had in their secret safes and envelopes inside the safes, things they didn't even know they had. But I could figure that out, and it was pretty straightforward and easy. Unfortunately, there were not too many people at NSA who understood or wanted to follow that process. That means there's nobody there knowing or doing that kind of thing any more, and it's why they were surprised when the Russians moved more troops into Crimea. That's also why they were surprised when the Russians moved into eastern Ukraine. None of that would have been a surprise to me, considering all the techniques I used and the understanding that I had of the Russian military and how they operated. And also the Russian mind, the way they think, which is very important, too, because that gives you the idea of how to solve things. So, that's a little background.



Ray McGovern

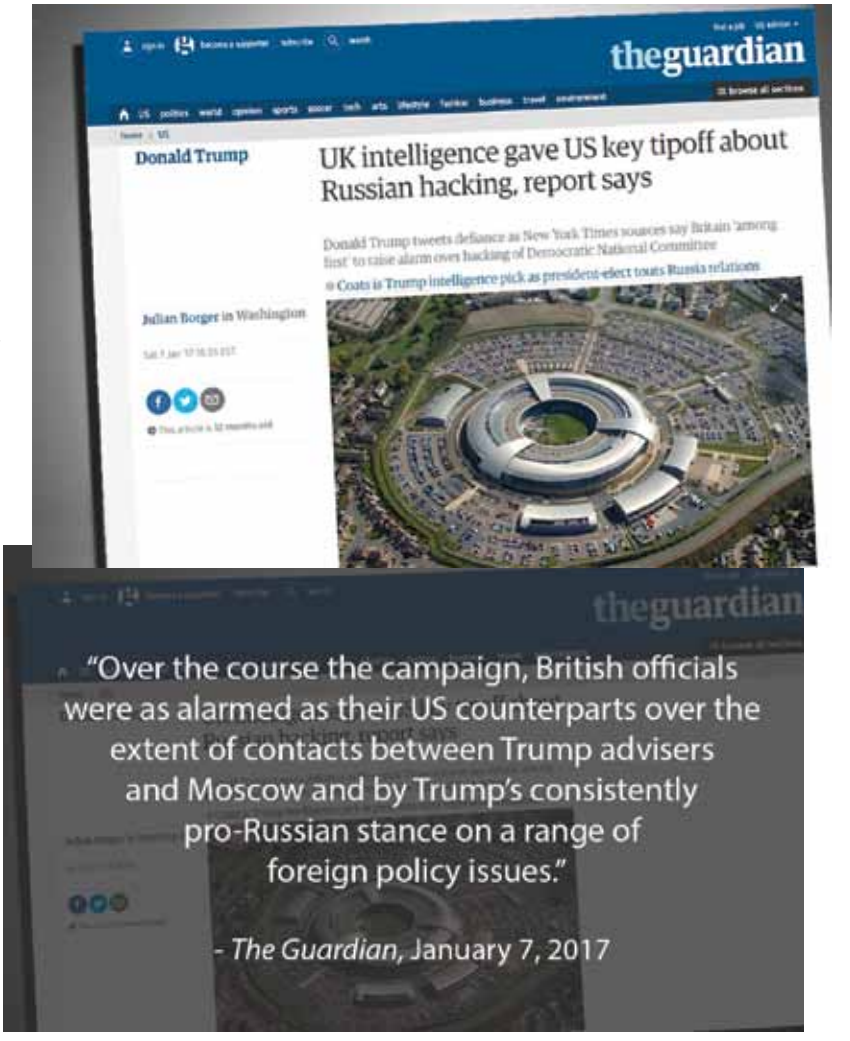
William E. Binney

Ray McGovern: Tell us about those indicators, Bill.

The Failure of U.S. Intelligence

Binney: I had five indicators, none of which were on the U.S. indicator list. They were the real ones, the ones that had meaning, the way you could separate training from real things in the world. And I watched it happen in Czechoslovakia, the Yom Kippur War, Af-

ghanistan, even the Chernobyl events, even the threat to Poland. All of that surfaced with those five warning indicators, none of which were on the U.S. official list of warning indicators—so! And then, when I figured it out and laid it all out, everybody inside NSA who was involved said, "We can't tell anybody about this. We have to keep this secret." Well, that's contrary to the way I thought. I thought we should share everything, so that everybody knew how to do things, and if they could also do it, they'd get effective on a wider scale. My policy inside NSA was "share, share, share," and theirs was, "shut up, shut up, shut up."



So, "don't share, don't share, don't share." Because their policy was pretty simple; if you share knowledge that you have, what that means is that everybody's got your knowledge, and you're not special. You don't have anything up on them, so you're no longer the leader, the person that somebody looks to for the answer. You know, everybody else can get the answer, too. Well, I thought that was counterproductive.

After I got to NSA, I had a lot of fun sending out "woozlegrams" to GCHQ (the British version of the NSA). Then, I looked at—and Ray and I had been discussing this—the alleged hack, which I understood to be a fabrication from the very beginning, because, first of all, NSA wasn't telling you where the packets went, and *they would know—if they were hacked—where those packets went,* because the TCP/IP packet format gives you a way of reconstructing a data transfer session, by a number—giving a specific number to a whole series of packets that belong together. So that gives you the idea how to repackage each session. And then internally in there is the IP number of the originator, and of the terminal where the packets are supposed to go.

That's what the machines do that manage the distribution of data to the Net; that's how they pass the data around. All you need is one packet to tell where it came from and where it is going. NSA has trace route programs mapping all the packet transfers around the world. They've got hundreds of trace route packets in switches and servers all around the world. In fact, the count on one of the slides released by former NSA contractor Edward Snowden shows in the computer network exploitation that the NSA had over 50,000 implants in switches and servers around the world. That means switches everywhere. The slide shows the distribution of it from the old Soviet Union, across all of Europe, through Asia, all over—and in the United States, too.

But those implants are also tied in with tapping points, where they actually use a PRISM type program, where it takes a fiber input and splits it into two and duplicates it. Then they send one to the NSA, Narus or Verint devices, depending upon whether it's AT&T or Verizon, or some other company. And then that sessionizes everything, reconstructs everything on those fiber networks, and they pass it to the storage facilities in Utah, or where-have-you—that's where they're storing all this data. My estimate of the storage facility in Utah

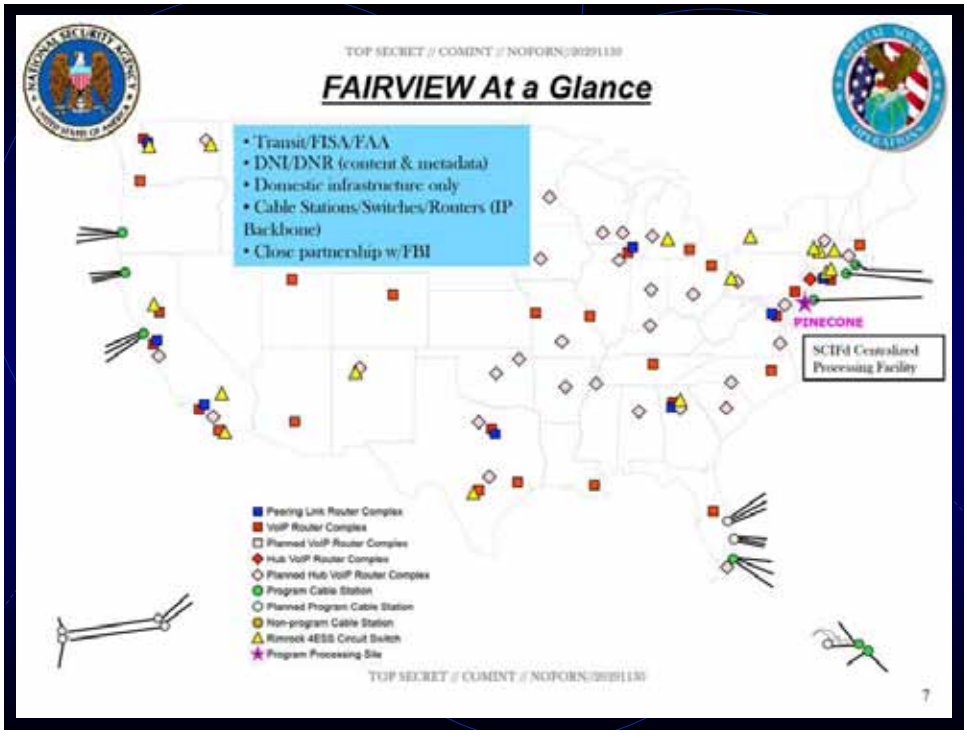
was that it could hold 5 zettabytes of data, which is 5x10 to the 21st power bytes.

McGovern: That's a lot!

The Surveillance State

Binney: Yes it is. In fact, it's probably something like 100 times the total knowledge of everything man has ever created. But the point is, that storage facility is a million square feet, and 100,000 square feet of that is devoted to actual storage; the rest of it is power and cooling and stuff like that. But now they're planning ahead, they're planning for it to be full. If you try to collect everything—which was NSA Director General Keith Alexander's policy, he said, "let's just collect it." That means an ever increasing amount year after year. That means, year after year, you have to keep building bigger facilities to store it, because there is going to be more and more data.

FIGURE 1



They broke ground last summer for a is a 2.8 million square foot facility at Fort Meade, Md., which will be about three times the size of the one in Utah. That's the planning, to replace, once the Utah facility's full. Then they'll have that one to fill up. Because they're collecting more data every year, they need a bigger facility. And that one's probably going to cost $5-$6 billion, and it's all going to come out of our taxpayers—or else we're going to borrow it from China.

"I've been distributing information about this to all kinds of news agencies, TV, radio, and various newspapers. I've been distributing the 'Fairview at a Glance' map (**Fig. 1**) to all of these agencies, so that they could see where the tap points are inside the U.S.A. This one is for AT&T. It's called the Fairview program. If you looked at it, they keep claiming—and this is what I call the "obvious lie," the obvious lie that the American public is being told by our government—"we're only after foreigners, and that's why we have these taps and are copying all this data."

Well, if you look at this, that's distributed throughout the population centers of the United States at tap points. If the NSA only wanted foreign communications, see those green points along the coasts? There's 11 of them, on the West Coast and the East Coast. That's where all the foreign communications come through. That's where the transoceanic cables surface: All foreign communications are coming into the United States through those points, or going out from the United States, or they're transiting foreign communications coming in, going then through the U.S.A. to Canada or Mexico, or even Asia somewhere. Any transit and communication—into or out of—foreign locations, is at those green points. That's where they should be tapping if they're after foreign communications. So why do you have the rest of those tap points distributed with the population of the U.S.A.? It's because *we are the target,* that's why.

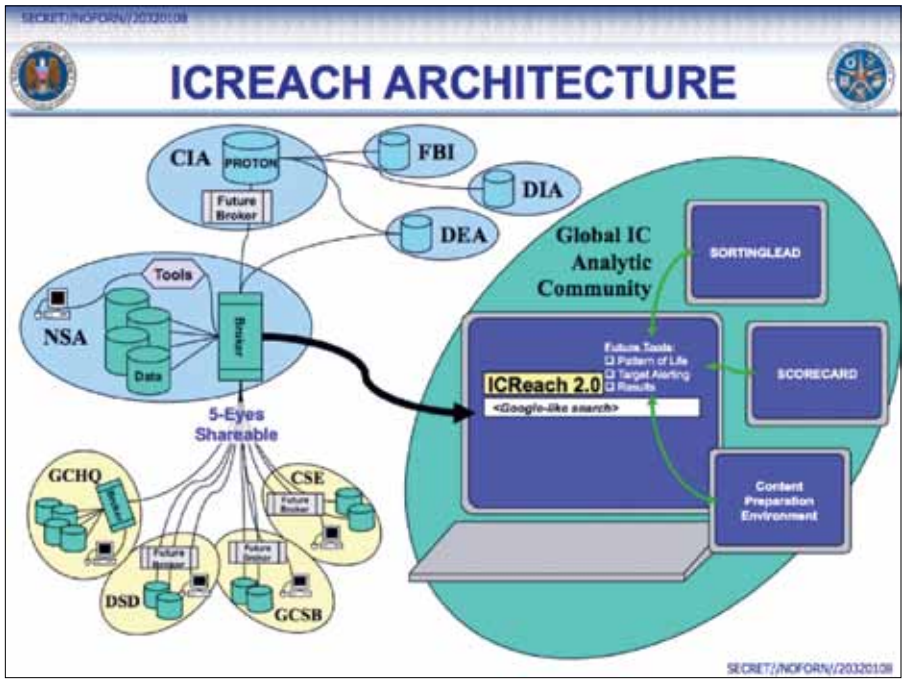
If they just want foreign communications, they have the green points already. So what's all the rest of this stuff? That's why they're building the Utah center. I, of course, was a witness at the start of this in October 2001, when they started pulling all the billing data from AT&T. It was about 400 million total average per day of long-distance calls, 320 million of those were U.S. to U.S. calls—so it was all internal to the U.S.A.

All of this was being graphed, and it was a violation of the First Amendment. Eventually the NSA could

figure out a lot of things, and that would be a violation of the Fourth Amendment. Then they started using the information to prosecute people, and that was a violation of the Fifth and Sixth Amendments to the Constitution. So they kept scrapping the Constitution in doing this.

I went on the Web, using Google, and looked at this. I decided I was going to go find out where these points are. So I now have the locations of all of them, down to the building and address. I've shared this with any number of people; I gave it to the documentary film producer Laura Poitras, if she wanted to publish it, and she in turn gave it to the *New York Times*. She told me that she gave it over to them, and they refused to publish. They said if they published it and one of those points was attacked, they would be blamed. So much for the intention of the First Amendment, to have a free press that would inform the public of what their government's doing on their behalf. *Like, spying on them*.

FIGURE 2



And *this is not simply metadata*; this includes all content, too. They've been lying about that from the beginning. I mean, how could you even look at something, how could you even conceive of spying on your lover to see if she or he is cheating on you—how can you do that with metadata? You have to have a *little content* to see if somebody's messin' around. OK? The point is, they had that in the NSA storage. That's a local phone call, between people locally—I mean, if you're going to have an affair you can't go too far, you know? You have to be in a reasonable proximity. [laughter]

This is what I call the "big lie," and we're all buying into this. That's why Section 702 of the Foreign Intelligence Surveillance Act (FISA) is a joke. Section 702 and oversight of it is a joke! That's not what they're doing. This is all done under Executive Order 12333, section 2.3c, where it says: If you are after a target, an international criminal or some target like militaries or things like that, or leaders of countries—like Merkel or others—it's OK to collect information and to try to find them; that's OK, and you can store it—and oh, by the way, you can search it, too, if you want. They say, "On every fiber line, there's a probability of having a dope dealer internationally, *so let's copy them all.*" And, oh, by the way, we can keep all the data on U.S. citizens and all their communications, and we'll call it "coincidental collection," and we'll store it and interrogate it.

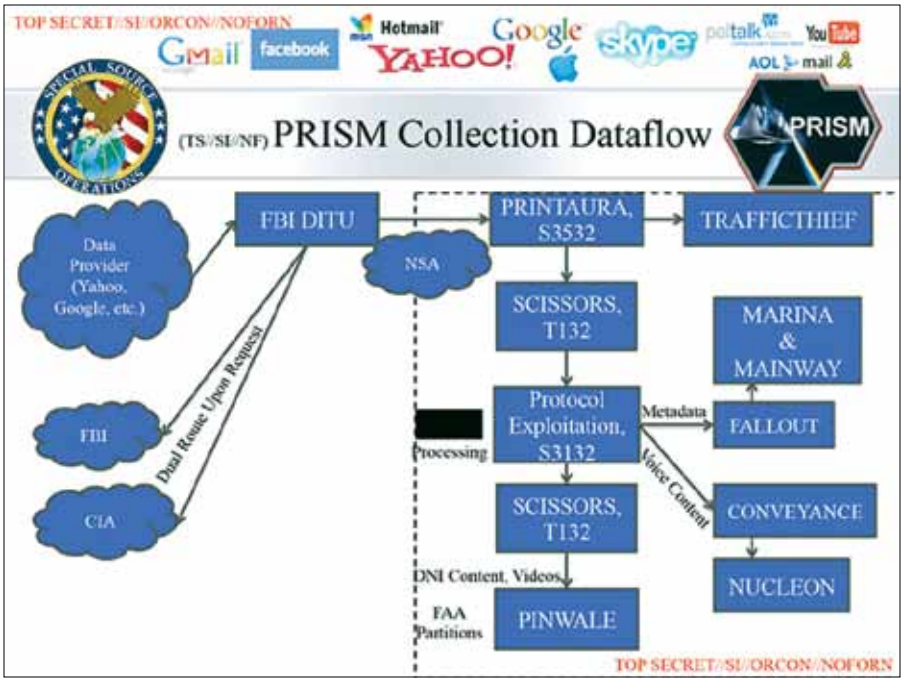
The Spying Apparatus

And that's what the FBI does, and that's how they get into this data. You see in the "ICREACH ARCHITECTURE" (**Fig. 2**), the CIA, FBI, DIA (Defense Intelligence Agency), DEA (Drug Enforcement Agency), and the Five Eyes (British, U.S.A., Canada, Australia, and New Zealand intelligence cooperation). This slide is from 2007, I believe. What they do is stamp the date for the first classification review, which is 25 years. So it's 2032, Jan. 8, I think. So if you subtract 25 from that, that means the slide was constructed on Jan. 8 of 2007, and the first review is 25 years later. This was the status in 2007, ten years ago. But of course, it's expanded since then; they've now got nine other countries participating with them in this program, but they access this data through a separate program called XKeyscore. And that one restricts access. In other words, these different programs have different access rules, called

"rules tables," of what you're allowed to look at or interrogate or search. That's how you limit what people can do in your data base.

There are limits to some of this even in ICREACH [The NSA's top-secret surveillance-related search engine], but they can simply modify their "rules table" and they can get into everything. So that's the Five Eyes [British, U.S.A., Canadian, Australian and New Zealand intelligence], looking at all the data that the NSA has on everybody, including us and including British citizens, as well as all the others around the world. Each can spy on the other, and cooperate that way, too. It's easy; the mechanisms already exist for that; that's the easy way to do it.

FIGURE 3



This all feeds into the internal NSA programs. This was where I came in. This was my design for NSA (**Fig. 3**), the whole thing: picking out, right up front, the "Traffic thief," picking out the selected targets that you knew about, and then passing it through a process where metadata gets graphed and relationships are built. We were preparing to do "two-degree separation" of selection of data from that, as a part of the process of automatically analyzing and figuring out who the new targets were, and then adding them automatically, basically taking people out of the loop. Because they did a very bad job—I mean, they were very inconsistent and variable. It's unfortunate, but that's the way the analysts were.

Then it's all indexed down to the databases—Pinwale and Nucleon—which are the Internet database in Pinwale and the phone database in Nucleon. The phone network wasn't too much of a problem—the public switched telephone network—because it was basically run by the telephone companies for NSA. The NSA wanted these selections, and the telephone companies would provide it to the NSA, including the audio. The tap points that the NSA had would also pick up all the VOIP (Voice Over Internet Protocol) audio. That was one of the main targets. The NSA felt people were using VOIP to do criminal activity. It was cheaper, too, so they didn't have to pay as much.

That was the entire design we left them, and they haven't changed a damned thing for 16 years. It's all been the same; there's nothing new here. This is what we left them. *Except we had several programs running that would not enable them to do what they're doing today*. Like right up front, we had programs that filtered out all data that wasn't relevant. We never took it in, so they never had the chance to abuse it. We never had to store it anywhere, because it wasn't kept there. So if you can make that decision right up front, your management of content is much easier.

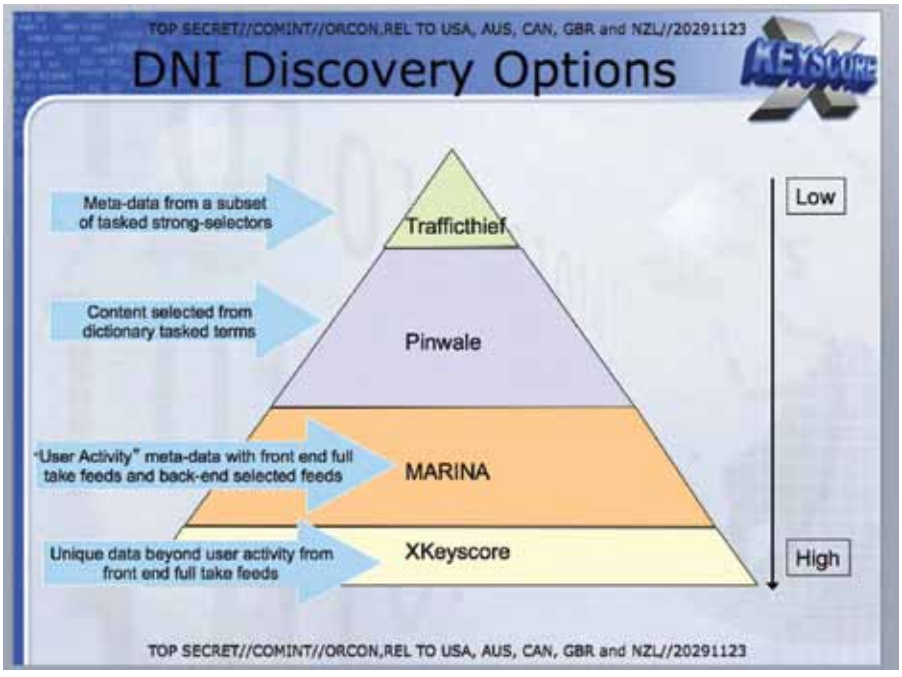
That was the approach we took. But see, then Vice President Dick Cheney wanted to know—he grew up under Nixon—he wanted to know what his enemies were doing and planning, and he wanted to know what all the politicians, all his political opponents were all about. You need to know what everybody's doing to control them. So, the policy was: let's collect it all. That's really what it's all about, controlling the American population.

You can see it with the use of data against the author and reporter Jim Risen, and also against former New York Governor Eliot Spitzer—he was going after the bankers for defrauding people, fraudulent solicitations, causing the 2007-2008 crisis; he was going to go after them criminally. In order to get rid of him, they had to

use the FBI, going directly in through the FBI technology center in Quantico, Virginia, directly into the NSA databases. There's no oversight of that, at all! There's no reporting of any of that, no auditing of any of it, and there's no oversight by the courts, or the Congress!

So this is what I've been telling people. They don't believe this crap? They should start asking questions about the Fairview program and all these accesses that are going on that they don't even know about, or they don't follow—or they don't *want* to know about, because if they *did* know about them, they couldn't claim plausible deniability! That's really what their action is; they can claim plausible deniability: "Oh, it didn't happen on my watch, I didn't know about that." This is the game they're playing; this is the lie they're perpetuating with us, the people. And the mainstream media are going along—*and they're worthless here!* They're basically worthless. They're all going along with this charade.

FIGURE 4



Tracing the Packets

When it came to looking at the data supposedly showing that the Russians "hacked" the DNC, here's the background: You *know* that *the NSA knows who took those packets and where they went*. All they had to do was have one packet and look internally at the TCP/IP format. They know the originator and terminating IP address, so you know where the system, the World Wide system, sent the packets. Because *they're machines*, you have to tell them exactly what to do, or it won't happen. So it's *in the format as to where the things go,* so the NSA should know who exactly got that, where that IP is.

I mean, they did it a few years ago with the Chinese. The NSA said, it came from a military building in Shanghai. So they should be able to do the same thing with any hack. And they should have packets on every hack, if they've got them. We used to see this stuff all the time. We had no problem at all finding out about it, recognizing it—*and that was 25 years ago!* So where are they now?

That was the main reason I opposed the idea the Russians "hacked," because NSA is not saying where the packets went, *and they would know*, because they've got trace route programs in hundreds of switches all over the world, in the U.S.A. and around the world, and those switches would tell them where those packets went. They'd have captured those packets and mapped them.

All you have to do is go on the Web and do a Google search for "trace route," and it'll give you an idea of what the capability is of the commercially available versions. They also have another program called TraceWatch, which allows you to see coming into your computer, and who's in your computer. There are various versions of that for different operating systems. So if you go on the Web and Google that, you can download it. The software is free, by the way, last time I looked. You can trace-route anybody sending you any email, you can watch who's in your computer and what they're doing.

More Intelligence Incompetence

This is the main area where all the collection accesses that NSA has, and all the data that people are

feeding them to store for them. The query goes into these programs, and the indexing by the graphs of the metadata is how they pull that data out of the storage of content. Once you pick that metadata up and say, "give me all the content on this piece of metadata," the program looks at the graph and goes in and pulls out all that data. That's how they're doing retroactive research on stored data.

That's how they're doing it. And, this is the fundamental principle (**Fig. 4**), and this is why I say these people have totally lost it, they're totally incompetent. They start at the top; it says, a low possibility of discovery of new options (at the top with the Traffic thief). That's where you're working with something that's known, and even if those known things communicate with other unknowns, they ignore that because that has a really low probability of discovery. That was really our main approach, targeted, focused approach.

And then they go down to the next one, they're going into the Pinwale system. Now, going into the Pinwale system, they use the XKeyscore and ICREACH programs, which basically do dictionary select—meaning that you feed them a bunch of words or phrases, and it pulls all the data out that has any of those words or phrases in it. Which is really a dump, it's like a Google dump. So you get 50,000, up to a million, returns, and if your input is a few billion items every day, and you do a Google search through it, like that, you'll get a couple million outputs every day. Each analyst with their Google output is trying to go through this tens of thousands or millions, or hundreds of thousands of items, and they never get through. That's why they fail.

So they can't see anything coming. Then all the terrorist attacks happen, people die—"go clean up the blood in the street"—and then you find out who did it, and then you go into the database and you say, "give me all the data on this person; I know who did it, and I can do a good forensic job for the police." Which means that the intelligence community that we have—and the GCHQ and all of them—have lost the ability to do the function of intelligence, which is to predict intentions and capabilities of potential adversaries—*in advance!* So you could do something to stop it!

That was the whole idea: We wanted to stop terrorist attacks. That's why we wanted to go to 18 sites that produced information on terrorists in January 2001, and they refused to do that. So we couldn't put it against the terrorist problem, which we put as the main problem.

At any rate, this whole pyramid says the further down you go, into Marina, which is the voice side of it, and then you use XKeyscore against all the databases, so now you're going into this massive database, your data polls, based on dictionary selection, phrase selects like that, is coming out—it's getting larger and larger, and they call it "high discovery." I call that "low."

The entire thing is reversed: low is high, and high is low, but these idiots don't know what is high and low! That's why they're failing: They don't even know they're failing. I'm just a country boy from Pennsylvania, I'm from the farmlands and the mines and so on. We used to say out there, if you're failing and continuously failing, you must be doing something wrong. And if you're doing something wrong, you need to look at your whole process and figure out what you're doing wrong and fix it!

They can't even admit they have something wrong. Because it means they have a wart on their record, and so, we can't admit a wart. That's why, if there's any whistleblower, we have to step on them. That's the way they're operating: They're like alcoholics—but they can't admit they're alcoholics, so they'll never fix their problems. So all these problems continue with U.S. intelligence.

Until we step up to this, people are going to continue to die to keep this entire stupid process going. That's the problem I see. That's why I'm calling them idiots and fools for doing what they're doing. And they're doing it at the expense of the lives of people in countries around the world—not just here. They're all buying into this crap. And the British also, and they're even going overboard with video. But we're catching up, just like we're trying to catch up with the British in invading countries: They've still invaded more countries than we have.

The Non-Existent Russian Hack

And then, when we at the Veterans Intelligence Professionals for Sanity (VIPS) looked at the raw data that was produced by Guccifer 2.0, that said this was the evidence that the "hack" on the DNC was by the Russians. We went through that data. Every time there's a file transfer or something that's transferred off a computer, a file comes out like an email, and you have a timestamp at the end of the email, when it's sent; the next email, a timestamp; the next email, a timestamp; a file, a timestamp and so on. So you get a timestamp at the end of the data transfer for each component of data.

That means you can line it all up, look at the timestamps and the difference between timestamps, and calculate the number of bits and then calculate the transfer rate.

That's exactly what we did, and when we looked at the Guccifer 2.0 data, we found the highest transfer rate was 49.1 megabytes/second. We tested data transfer rates around the world to try to see how fast we could do that; can we really do it at that rate? We said we couldn't, and we alleged that, and people took issue with that. So we said, "OK we'll test it, and see." I got some hackers in Europe to try to download a file we set up here in the U.S.A., download it across the Atlantic and into the European network; and we got some from a personal computer at 100 megabits, we got 0.8 megabytes/second, instead of 49.1 megabytes/second. And then on a DSL 200 megabit commercial line, we got 1.6 megabytes/second. And then on a data center to data center transfer from the New Jersey data center to a data center in the U.K., we got 12 megabytes/second. And we had some people try it in Belgrade, and also in Albania, and they just threw up their hands, it didn't even work—it was like running off a dial-up process. You just never get it across in time, so it was pointless to even try. The best transfer output across the network we got, was 12 megabytes/second—bytes, not bits.

That meant that even with the data, it was one-fourth the speed that was necessary. But if you pass something into the network, it adds all this housekeeping data to it, like the TCP/IP transfer format and other formats, and also data showing the transfer between segments of the line and so on, and timing and all of that. So you can do a trace route. If you re-trace the route, you see that that data goes with the packets, too. That meant that it's really close to doubling that data they have to transfer, so it means really that the transfer rate was only one-fourth to one-eighth the necessary speed of the network to transfer and make that happen.

So it was impossible. We just couldn't do it. We said, we're open to anybody that can show that that can be done, and then we'll replicate it just to be sure. That's the scientific method.

We failed to transfer it, and *there was a greater implication beyond that*. That argued, by the way, that it was a local download—wherever local was—where they did it, but it did match the thumb drive transfer rate from a computer. That did match. So it could be done on a thumb drive.

But we also looked at the data.

There were two batches of data that came out of Guccifer 2.0. One was dated the 5th of July, on the 5th of July transfer; and another was dated the 1st of September. So after we looked at that, some things looked a little suspicious. I was doing this with Duncan Campbell. He and I were looking at this the month before last. If you ignored the date and the hour, and looked only at the minute, second and millisecond, *the two files merged*. They interleaved with one another, so that it could form *one continuous file*. In other words, Guccifer 2.0 was playing with the data, and then he did a ripple change, a one-sided edit, on the hour and the date.

Fraud & Fakery

What that meant was, *all of this is a fake*. It's a fabrication! All the data that they pushed to say this was evidence of a hack, is a fake! We looked at that and said, "Hmm, who's faking this? Well, the timing of it looks like it might be somebody internally here in the U.S.A., who might have also used something like the NSA's Marble Framework program, to fake things. Which is where they go in—and I think Ray wants to say more about the Marble programs so I won't go into that too much.

You have to think about this. It's funny—this is really a poor, sloppy technical job, trying to fake a hack. *Period!* That's it. This is a fabrication from the beginning, and they're all building off this fabrication, and they have nothing else to produce in terms of evidence. The mainstream media say I'm a conspiracy theorist. The only thing they can do is throw labels at me! They have no evidence whatsoever to point to, *none!* And the stuff they point to, we've already shown is a clear fabrication and a fake!

And so, they're all, what we would call in the country, "sucking a hind tit." [laughter]—If you know what that term means. If you've ever raised cows, and a calf gets on the hind tit, they get kicked! That's the whole idea of that one. It's a good country saying.

But, we also look at them as being "chip pitchers," if you know what that is from the country. [laughter] Do I have to explain that one? Cow chips. They fall, and flatten, they dry out; they get really light, and round in shape for frisbee type throwing: So they're pitching chips. It's something that's done quite frequently in Washington, D.C., OK? And it fits right into the character of what they're doing here. This is the whole thing: This is just a fake! And it's an obvious one at that.

That's all I have to say. [applause]