GlobalResearch
Center for Research on Globalization

NSA Whistleblower: Clinton Emails Damaged U.S. National Security Much More than Manning, Assange Or Any Other Whistleblower

By Washington's Blog
Global Research, July 08, 2016
Washington's Blog 7 July 2016

Region: USA
Theme: Intelligence

Clinton Revealed "Intelligence Methods" and Sources

FBI director Comey said today that Hillary Clinton running emails containing government information on an unsecured, private server was not as bad as former CIA director Petraeus sharing classified documents with his lover.

But the highest-level NSA whistleblower in history, William Binney – the NSA executive who *created* the agency's mass surveillance program for digital information, who served as the senior technical director within the agency, who managed six thousand NSA employees, the 36-year NSA veteran widely regarded as a "legend" within the agency and the NSA's best-ever analyst and code-breaker, who mapped out the Soviet command-and-control structure before anyone else knew how, and so predicted Soviet invasions before they happened ("in the 1970s, he decrypted the Soviet Union's command system, which provided the US and its allies with real-time surveillance of all Soviet troop movements and Russian atomic weapons") – explains why Comey's statement is nonsense.

By way of background, recall that – when the American press reported that U.S. intelligence services tracked Bin Laden through his satellite phone – he stopping using that type of phone … so we could no longer easily track him.

This is *exactly* what government officials mean whenever they say that someone – say Edward Snowden, Wikileaks' Julian Assange, or Chelsea (formerly Bradley) Manning – is threatening national security by "revealing confidential information-gathering methods or sources."

Also by way of background, Binney pointed us to an article from March written by former NSA analyst, counterintelligence officer and War College professor John Schindler:

> Just-released State Department documents obtained by Judicial Watch under the Freedom of Information Act [here] detail a bureaucratic showdown between Ms. Clinton and NSA at the outset of her tenure at Foggy Bottom.
>
> ***
>
> One senior NSA official, now retired, recalled the kerfuffle with Team Clinton in early 2009 about Blackberrys. "It was the usual Clinton prima donna stuff," he explained, "the whole 'rules are for other people' act that I remembered from the '90s." Why Ms. Clinton would not simply check her personal email on an office computer, like every other government employee less senior than the

president, seems a germane question, given what a major scandal email-gate turned out to be. “What did she not want put on a government system, where security people might see it?” the former NSA official asked, adding, “I wonder now, and I sure wish I’d asked about it back in 2009.”

He’s not the only NSA affiliate with pointed questions about what Hillary Clinton and her staff at Foggy Bottom were really up to—and why they went to such trouble to circumvent federal laws about the use of IT systems and the handling of classified information.

***

As I explained in this column in January, one of the most controversial of Ms. Clinton’s emails released by the State Department under judicial order was one sent on June 8, 2011, to the Secretary of State by Sidney Blumenthal, Ms. Clinton’s unsavory friend and confidant who was running a private intelligence service for Ms. Clinton. This email contains an amazingly detailed assessment of events in Sudan, specifically a coup being plotted by top generals in that war-torn country. Mr. Blumenthal’s information came from a top-ranking source with direct access to Sudan’s top military and intelligence officials, and recounted a high-level meeting that had taken place only 24 hours before.

To anybody familiar with intelligence reporting, this unmistakably signals intelligence, termed SIGINT in the trade. In other words, Mr. Blumenthal, a private citizen who had enjoyed no access to U.S. intelligence for over a decade when he sent that email, somehow got hold of SIGINT about the Sudanese leadership and managed to send it, via open, unclassified email, to his friend Ms. Clinton only one day later.

NSA officials were appalled by the State Department’s release of this email, since it bore all the hallmarks of Agency reporting. Back in early January when I reported this, I was confident that Mr. Blumenthal’s information came from highly classified NSA sources, based on my years of reading and writing such reports myself, and one veteran agency official told me it was NSA information with “at least 90 percent confidence.”

Now, over two months later, I can confirm that the contents of Sid Blumenthal’s June 8, 2011, email to Hillary Clinton, sent to her personal, unclassified account, were indeedbased on highly sensitive NSA information. The agency investigated this compromise and determined that Mr. Blumenthal’s highly detailed account of Sudanese goings-on, including the retelling of high-level conversations in that country, was indeed derived from NSA intelligence.

Specifically, this information was illegally lifted from four different NSA reports, all of them classified “Top Secret / Special Intelligence.” Worse, at least one of those reports was issued under the GAMMA compartment, which is an NSA handling caveat that is applied to extraordinarily sensitive information (for instance, decrypted conversations between top foreign leadership, as this was). GAMMA is properly viewed as a SIGINT Special Access Program, or SAP, several of which from the CIA Ms. Clinton compromised in another series of her “unclassified” emails.

Currently serving NSA officials have told me they have no doubt that Mr. Blumenthal’s information came from their reports. “It’s word-for-word, verbatim copying,” one of them explained. “In one case, an entire paragraph was lifted from an NSA report” that was classified Top Secret / Special Intelligence.

How Mr. Blumenthal got his hands on this information is the key question, and

> there's no firm answer yet. The fact that he was able to take four separate highly classified NSA reports—none of which he was supposed to have any access to—and pass the details of them to Hillary Clinton via email only hours after NSA released them in Top Secret / Special Intelligence channels indicates something highly unusual, as well as illegal, was going on.

Binney explained to Washington's Blog the serious nature of Clinton's breach of GAMMA classified information:

> The compromise of this kind of cryptology success has a number of impacts on the ability of NSA to produce accurate intelligence on foreign targets of highest interest.
>
> (1) This lets the leaders of a foreign country know that their communications have been compromised and thatwe read what they are saying, planning and intending to do.
>
> (2) It compromises the fact that a particular type of encryption is readable. Not just the leadership; but, also all the others in that country and around the world that are using that encryption.
>
> (3) It lets our potential adversaries know our technology capabilities in attacking encryption.
>
> (4) If other countries (like Russia or China or any others) know the encryption system involved, then they too will look at it for any weakness or flaws that would allow reading the system.
>
> (5) It alerts adversaries to look into that system for structural errors in encryption design also look for human error in using the system or a combination of both that would make the system vulnerable.
>
> (6) This presents the country using that system the opportunity to feed false information into the intelligence produced by NSA which means the free world.
>
> (7) For NSA, this means that they have to find other ways to validate any intelligence they get from this encryption to insure the validity of the information they get.
>
> The target country may stop using that encryption for leadership (as was the case with GAMMA GUPY) but may continue to use it at other levels of communication; but, over time, they have been alerted to this weakness and will move as fast as they can to replace it with other encryption.

GAMMA GUPY was the U.S. spy program which installed an antenna on the roof of the United States Embassy in Moscow to eavesdrop on top officials of the Soviet Union in Moscow as they chatted with each other on their car telephones. When nationally-syndicated journalist Jack Anderson reported on GAMMA GUPY in 1971, it alerted the Soviet leadership … so they immediately stopped talking in a way that could be overheard.

Binney continued:

> This [Clinton's email hijinks] is real serious, on the order of what Jack Anderson compromises in 1971 dealing with the "Gamma Gupy" source.

> This is the most sensitive intelligence, and [Clinton] and her staff took it out of classified reports and put excerpts in open source on her server.
>
> ***
>
> All in all, this is a rather devastating compromise of technical capability and a commensurate loss of high value intelligence.
>
> I know this kind of technical explanation is rather difficult for the public to understand and comprehend, but it is rather devastating to people responsible for intelligence production.
>
> In my view, this is much worse than what Julian Assange or Chelsea Manning or any of the other whistleblowers have done.
>
> Some are in prison for as many as 35 years. Others have just been ruined and kept from getting anything but menial jobs. But, those in high positions get a pass for much worse offenses.

Indeed.

Articles by: Washington's Blog