

ISIS Hacks U.S. Central Command While Obama Is Announcing New Cyber Security Legislation

By Melissa Dykes

Global Research, January 13, 2015

The Daily Sheeple 12 January 2015

Theme: Media Disinformation

Could it really get any more convenient than this?

The top story today (January 12) everywhere is that ISIS hackers attacked U.S. Central Command and posted sensitive info on the agency's official Twitter page.

Via The Washington Free Beacon:

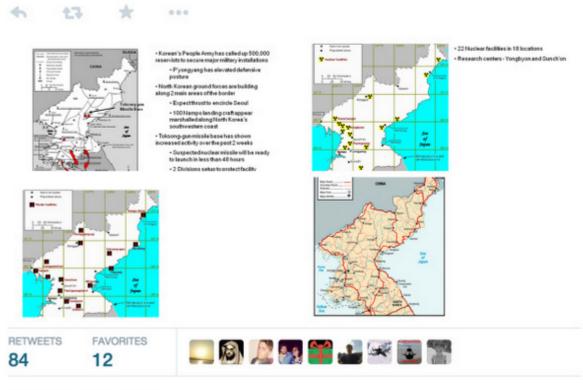
Hackers with the Islamic State, also known as ISIS or ISIL, posted links on U.S. Central Command's <u>official Twitter page</u> to what it claimed was "confidential data from your mobile devices."

"ISIS is already here, we are in your PCs, in each military base. With Allah's permission we are in CENTCOM now," said one tweet sent from CENTCOM's account.





Pentagon Networks Hacked. Korean Scenarios



12:50 PM - 12 Jan 2015

Further:

The hackers subsequently tweeted images of spreadsheets containing the home addresses, phone numbers, and email addresses of dozens of current and former senior U.S. military officers.

"AMERICAN SOLDIERS, WE ARE COMING WATCH YOUR BACK," one tweet stated.



So the hack attack *just so happened* to come JUST as President Obama was addressing the nation on, what else? <u>Cyber security</u>.

Really? How serendipitous. In fact, if you look up serendipitous in the dictionary, this situation might be in there as a textbook example.

Obama is expected to address cyber security again at the State of the Union where he is set to continue drumming up support for two new pieces of legislation on cyber security he is about to propose.

And now he's telling Americans that these attacks pose a "direct threat to the economic security of American families."

<u>Wired</u> reported, "The president cited the recent hacks at Target, Home Depot and Sony as primary reasons why Congress should pass the Personal Data Notification and Protection Act. The bill would help unify a multitude of state breach laws that currently exist. Lawmakers have tried for nearly a decade to pass a federal bill to replace the patchwork of state laws, but have repeatedly failed, in part because either the laws didn't go far enough or went too far."

So for ten years they've wanted to pass more federal laws to replace state laws, but they haven't been able to — now the Sony hack (which looks like a <u>psyop</u>) and the oh-so-timely CENTCOM hack — and *bam* — more laws?

What better way to get support for passing more cyber security laws than an ISIS CENTCOM cyber attack occurring right when the president is talking about passing more cyber security laws?

(Pray tell...what all is in those bills, anyway? Anyone read the fine print yet?)

This is classic Hegelian Dialectic problem-reaction-solution for another government power grab.

I mean, the writers of <u>Wag the Dog</u> couldn't make this stuff up. Or maybe they could, because it really seems like they did.

The president will also be talking to the Department of Homeland Security on Tuesday about even more ways the nation can defend itself against cybercrime ... Considering that everything Homeland Security does seems to take a little more of our liberties in exchange for security (theater), this ought to be good.

Also note that government officials are using the recent attack on French satirical newspaper Charlie Hebdo to justify and call for even more big brother surveillance society NSA spying on Americans.

From recent article "Sickening: Police & Surveillance State Apologists Leap At Charlie Hebdo Opportunity To Advocate For More Spying, Less Freedom," in the blog <u>Tech Dirt</u>:

...former NSA and CIA director Michael Hayden went on cable news on Thursday morning to use the Charlie Hebdo attack as an excuse for why the program was so useful. After spending about four minutes talking about how these kinds of random small attacks are likely to be the new way terrorists attack, he then defends metadata collection:

Let me add another thought here too: You know, I was talking to you guys

about 12 months ago, about these massive amounts of metadata that NSA held in storage. That metadata doesn't look all that scary this morning and I wouldn't be surprised if the French services pick up cell phones associated with the attack and ask the Americans, 'where have you seen these phones active globally?'.

Actually, no, that metadata does still seem pretty scary, because it also includes a hell of a lot more than just those responsible for the attack. And, it's not like law enforcement and the intelligence community can't go back to the operators currently responsible and ask them for that data. There's still no reason to believe that the NSA needs to just be sitting on this data all the time. And, of course, it doesn't seem like all that metadata helped prevent any attack, now did it? [emphasis added]

Exactly.

So while they are calling for *even more* surveillance state spying on Americans, even more unconstitutional collection of our data, at the same time they admit they cannot protect anyone's data ... so please give them more laws and power?

Does not compute.

Melissa Melton is a writer, researcher, and analyst for <u>The Daily Sheeple</u>, where this <u>first appeared</u>, and a co-creator of <u>Truthstream Media</u> with Aaron Dykes, a site that offers teleprompter-free, unscripted analysis of The Matrix we find ourselves living in. Melissa also co-founded <u>Nutritional Anarchy</u> with Daisy Luther of The Organic Prepper, a site focused on resistance through food self-sufficiency. Wake the flock up!

The original source of this article is <u>The Daily Sheeple</u> Copyright © <u>Melissa Dykes</u>, <u>The Daily Sheeple</u>, 2015

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Melissa Dykes

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: $\underline{publications@globalresearch.ca}$