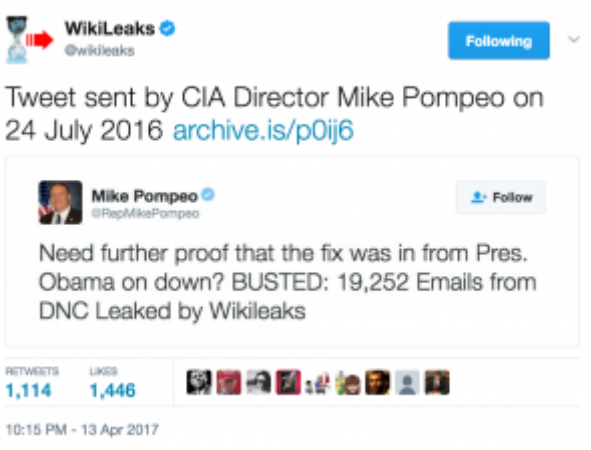
POMPEO LIKENS WIKILEAKS' RELEASE OF CIA'S HACKING TOOLS TO PHILIP AGEE



In a speech designed to generate headlines, CIA Director Mike Pompeo just attacked WikiLeaks as a "a non-state hostile intelligence service often abetted by state actors like Russia." The speech was explicitly a response to an op-ed Julian Assange had in the WaPo a few days ago.

> Now, for those of you who read the editorial page of the Washington Post—and I have a feeling that many of you in this room do—yesterday you would have seen a piece of sophistry penned by Mr. Assange. You would have read a convoluted mass of words wherein Assange compared himself to Thomas Jefferson, Dwight Eisenhower, and the Pulitzer Prize-winning work of legitimate news organizations such as the New York Times and the Washington Post. One can only imagine the absurd comparisons that the original draft contained.

But the speech deserves closer analysis for several reasons.

CIA Directors hoping to build trust should fact and hypocrisy check better

First, it had the predictable CIA Director errors. As an example, it pretends to be rebutting "false narratives" purportedly spread by WikiLeaks, but uses as an example "the fanciful nation that they spy on their fellow citizens via microwave ovens," a suggestion first spread by KellyAnne Conway, not WikiLeaks (though WikiLeaks responded by pointing to ways to spy with microwaves, though not ovens). It suggests Assange "directed Chelsea Manning in her theft of specific secret information;" had Assange's direction been that clear cut, he would have been indicted. Perhaps most hilariously, a guy who — nine months ago — was applauding a WikiLeaks release today had this to say:

> First, it is high time we called out those who grant a platform to these leakers and so-called transparency activists. We know the danger that Assange and his not-so-merry band of brothers pose to democracies around the world. Ignorance or misplaced idealism is no longer an acceptable excuse for lionizing these demons.

Yes. By all means, we should call out those who grant a platform to WikiLeaks. Like Mike Pompeo.

The never-ending defense of all spying overseas

The speech is also worth reviewing because of something that has become tiresome in recent years.

To rebut that false narrative Pompeo rebuts a claim that's beside the point to WikiLeaks' presentation of the CIA Vault 7 files (though it is one WikiLeaks has suggested on Twitter): that CIA spies on Americans.

> [W]e are an intelligence organization that engages in foreign espionage. We steal secrets from foreign adversaries, hostile entities, and terrorist organizations. We analyze this intelligence so that our government can better understand the adversaries we face in a challenging and dangerous world.
>
> [snip]
>
> So I'd now like to make clear what CIA doesn't do. We are a foreign intelligence agency. We focus on collecting information about foreign governments, foreign terrorist organizations, and the like—not Americans. A number of specific rules keep us centered on that mission and protect the privacy of our fellow Americans. To take just one important example, CIA is legally prohibited from spying on people through electronic surveillance in the United States. We're not tapping anyone's phone in Wichita.

Assange has focused primarily not on domestic spying, but on how incompetent CIA was for losing its hacking tools and for the proliferation risk it poses. Here's what Assange said in his op-ed.

> Our most recent disclosures describe the CIA's multibillion-dollar cyberwarfare program, in which the agency created dangerous cyberweapons, targeted private companies' consumer products and then lost control of its cyber-arsenal. Our source(s) said they hoped to initiate a principled public debate about the

> “security, creation, use, proliferation and democratic control of cyberweapons.”

Pompeo admits aggressive use of tools, and promises better security

That’s not a point that Pompeo really debates, though he does say,

> CIA is aggressive in our pursuit of the information we need to help safeguard our country. We utilize the whole toolkit at our disposal, fully employing the authorities and capabilities that Congress,

As for losing the cyber toolkit (Pompeo does not, of course, confirm that that is what WikiLeaks has been releasing), Pompeo does promise these changes to improve CIA’s own security.

> Second, there are steps that we have to take at home—in fact, this is a process we’ve already started. We’ve got to strengthen our own systems; we’ve got to improve internal mechanisms that help us in our counterintelligence mission. All of us in the Intelligence Community had a wake-up call after Snowden’s treachery. Unfortunately, the threat has not abated.
>
> I can’t go into great detail, but the steps we take can’t be static. Our approach to security has to be constantly evolving. We need to be as clever and innovative as the enemies we face. They won’t relent, and neither will we.
>
> We can never truly eliminate the threat

> but we can mitigate and manage it. This relies on agility and on dynamic "defense in depth." It depends on a fundamental change in how we address digital problems, understanding that best practices have to evolve in real time. It is a long-term project but the strides we have taken—particularly the rapid and tireless response of our Directorate of Digital Innovation—give us grounds for optimism.

If these changes go beyond finally ensuring all devices require multi-factor authentication (something a Mike Pompeo overseen CIA did not have this time last year), then it will be a good thing.

The Philip Agee comparison

But I'm perhaps most interested in the implicit comparison Pompeo makes to start his speech. He suggests a comparison between Philip Agee (and the murder of Chief of Station Richard Welch ~~after being outed by Agee~~) and WikiLeaks (or perhaps Assange personally).

> That man was Philip Agee, one of the founding members of the magazine *Counterspy*, which in its first issue in 1973 called for the exposure of CIA undercover operatives overseas. In its September 1974 issue, *Counterspy* publicly identified Richard Welch as the CIA Chief of Station in Athens. Later, Richard's home address and phone number were outed in the press in Greece.
>
> In December 1975, Richard and his wife were returning home from a Christmas party in Athens. When he got out of his car to open the gate in front of his house, Richard Welch was assassinated by a Greek terrorist cell. At the time of his death, Richard was the highest-

> ranking CIA officer killed in the line of duty.

That's a pretty remarkable way to introduce this speech. Perhaps to defend it, in the section of the speech dedicated to painting WikiLeaks as a hostile actor, Pompeo notes AQAP thanked WikiLeaks for tipping it off to a way to fight the US it hadn't thought of.

> Following a recent WikiLeaks disclosure, an al Qa'ida in the Arabian Peninsula member posted a comment online thanking WikiLeaks for providing a means to fight America in a way that AQAP had not previously envisioned.

That's still a long way from posting CIA officers' identities.

Security firms begin to expose CIA's roles

All that said, I can't help but wonder whether this spat between former WikiLeaks booster Mike Pompeo and WikiLeaks stems from a development that I've been anticipating: when security firms start treating US intelligence hackers like they do Russian or Chinese ones.

In the wake of WikiLeaks' Vault 7 documents, both Symantec and Kaspersky wrote reports on Vault 7 hacks they had seen working with clients. Symantec provided a very convincing table correlating the compilation time of what they've seen with the evidence WikiLeaks presented.

Corentry sample (MD5 hash)	Date/time of sample compilation	Embedded Corentry version number	Corentry compiler	Vault 7 changelog number	Vault 7 changelog date
N/A	N/A	N/A	N/A	2.1.0 - 2.4.1	Jan 12, 2011 - Feb 28, 2013
e20d5255d8ab1ff5f157847d2f3ffb25	23/08/2013 10:20	3.0.0	GCC	3.0.0	Aug 23, 2013
5df76f1ad59e019e52862585d27f1de2	21/02/2014 11:07	3.1.0	GCC	3.1.0	Feb 20, 2014
318d8b61d642274dd0513c293e535b38	15/05/2014 09:01	3.1.1	GCC	3.1.1	May 14, 2014
N/A	N/A	N/A	N/A	3.2.0	Jul 15, 2014
511a473e26e7f10947561ded8f73ffd0	03/09/2014 00:12	3.2.1	GCC	3.2.1	Aug 18, 2014
c06d422656ca69827f63802667723932	25/02/2015 16:50	N/A	MSVC	3.3.0	Feb 25, 2015
N/A	N/A	N/A	N/A	3.3.1 -> 3.5.0	May 17, 2015 -> Nov 13, 2015

Symantec also described the victims generally (including describing what sounds like CIA detasking as soon as they realized they had accidentally attacked a US target).

> Longhorn has infiltrated governments and internationally operating organizations, in addition to targets in the financial, telecoms, energy, aerospace, information technology, education, and natural resources sectors. All of the organizations targeted would be of interest to a nation-state attacker.
>
> Longhorn has infected 40 targets in at least 16 countries across the Middle East, Europe, Asia, and Africa. On one occasion a computer in the United States was compromised but, following infection, an uninstaller was launched within hours, which may indicate this victim was infected unintentionally.

Kaspersky offered no such public detail.

Nevertheless, these reports are just one of several developments of late (which I hope to return to) that exhibit the US' hackers being treated like Russian or Chinese hackers are — as general adversaries outside of their country. If, as seems likely given Symantec's description of European victims, some of the victims are nominal US allies, that'll grow worse.

If I'm right, it's a significant development. It may not equate to a CIA officer being outed. But it may case far more problems.

Update: As a number of people have made clear, Agee was not responsible for Welch’s death. So I’ve deleted those words.