GlobalResearch
Center for Research on Globalization

WikiLeaks, “Year Zero” and the CIA Hacking Files

By Dr. Binoy Kampmark
Global Research, March 10, 2017
Region: USA
Theme: Intelligence, Media Disinformation

It is now up to the device and OS manufacturers, like Apple, Google, or Samsung, to fix their volcanoes back into mountains. -Telegram Statement, Mar 8, 2017

The paradox with information releases that expose a supposedly grand internal stratagem is that they merely provide the food of confirmation otherwise lacking. Such food is potent. It blows the lid off the suggestion that a conspiracy theorist was merely a Cassandra in the wilderness chewing fingernails in fear that something hideous was afoot. It provides nutrients for those seeking greater scrutiny over the way state security, otherwise deemed the domain of closeted experts, is policed.

The entire profession (for it has now become one) of mass disclosures of secret or classified documentation has reached a point where its normality can hardly be questioned. Be it the juicy revelations of Edward Snowden in 2013, the work of WikiLeaks in this decade and the last, and the Panama Papers, whistleblowing, still punished and frowned upon, remains indispensable to the conversation about transparency and the inner operations of the Dark State and its accessories.

That Dark State was given a further lighting up on Tuesday with the release, by WikiLeaks, of its CIA Vault 7 and Year Zero series that has caused the usual flutter in the intelligence community and governments.

These comprise the machinery of hacking and cyber war tactics, an overview of methods that suggest, according to WikiLeaks, a loss of control by the agency over a good deal of its hacking arsenal (“malware, viruses, Trojans, weaponized ‘zero day’ exploits, malware remote control systems and associated documentation”).[1]

The releases reveal aspects of the internal functions of the organisation, including the works of its Engineering Development Group (EDG), dedicated to the development of software within the Center for Cyber Intelligence.

As WikiLeaks revealed, the sophisticated nature of surveillance is now such as to draw comparisons with George Orwell’s 1984 “but ‘Weeping Angel’, developed by the Embedded Devices Branch (EDB), which infests smart TVs, transforming them into covert microphones, is surely its most emblematic realization.”[2]Samsung has figured prominently in such attacks jointly conducted with Britain’s MI5/BTSS.

Even of more concern is that such methods, similar to the hoovering techniques of trawler surveillance, tend to hamper, rather than sharpen, discrimination regarding targets of value. Malware, in making its way into a range of devices (iPhones, Android, smart TVs), lingers like an innocuous, odourless smell.

This makes suggestions of ‘targeted’ surveillance, or surveillance against countries other

than those of the Five Eyes, absurd. (Vide the opinions of Australia's insipid Christopher Pyne, who assumes with school boy innocence that Washington would never have an interest in spying on Australian subjects.)

Controls over the nature of who receives or uses such devices or operating systems are less relevant than the nature of the devices, adjusted and cooked to the right level of surveillance. So called "smart" devices are hardly discerning in that regard.

The releases have also seen a rapid scramble on the part of app companies to claim that the Vault and Zero Year coverage by WikiLeaks reveals a crude reality: you simply cannot rely on the security of your messaging format.

"To put 'Year Zero' into familiar terms," the statement from Telegram instructs with confidence piercing clarity, "imagine a castle on a mountainside. That castle is a secure messaging app. The device and its OS are the mountain. Your castle can be strong, but if the mountain below is an active volcano, there's little your engineers can do."[3]

The statement by Telegram goes on to charmingly remind users that it would not matter "which messenger you use. No app can stop your keyboard from knowing what keys you press. The focus, then, is on "devices and operating systems like iOS and Android" not on the level of apps. "For this reason," the app company insists, "naming any particular app in this context is misleading."

What is not misleading is the effect of such surveillance, the insecurity it inflicts on customers, and the rampant breach of privacy. The intelligence agencies find themselves running out of breath, bloated and spread. Their outsourcing of services through less secure channels – namely contractors – has also unleased a demon they can barely control.

Defenders of such methods spring back into a default mode that assumes WikiLeaks has done something terrible, emboldening enemies of the United States as defender of the now poorly described "free world". Pundits and former members of the security coven fear that the disclosure of the CIA playbook on this is somehow tantamount to giving away the family silver to a suicide bomber in search of martyrdom. The pertinent question here, surely, is defending that world from within as a matter of course.

Even the most dyed-in-the-wool establishment type has to concede that the intelligence community, puffing and out of breath, is there for the trimming, a vigorous pruning that just might ensure its reinvigoration and relevance.

The CIA is a beast in maturation, adjusting, and flexing its muscles in accordance with circumstance. It is to be watched, accordingly cleaned and overseen by diligent groundsmen and women. Sadly, the members of Congress are not necessarily the most able, or willing, to do that watching. An external impetus, miraculously supplied, might well do the trick.

Dr. Binoy Kampmark *was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. Email: bkampmark@gmail.com*

Notes

[1] https://wikileaks.org/ciav7p1/#ANALYSIS

[2] https://wikileaks.org/ciav7p1/#ANALYSIS

[3] http://telegra.ph/Wikileaks-Vault7-NEWS

Articles by: **Dr. Binoy Kampmark**