افغانستان آزاد – آزاد افغانستان

AA-AA

چو کشور نباشد تن من مبـــاد بدین بوم و بر زنده یک تن مـــباد
همه سر به سر تن به کشتن دهیم از آن به که کشور به دشمن دهیم

www.afgazad.com afgazad@gmail.com

European Languages	زبانهای اروپائی

By Kevin Reed
04.07.2019

Trump national security team revives demand for "backdoor" access to encryption

According to a report in the online publication *Politico*, senior Trump administration officials met on June 26 to discuss measures to prohibit tech companies from developing encryption methods that cannot be broken into by law enforcement.

Three unnamed individuals with knowledge of the meeting last Wednesday revealed that key National Security Council members—including second in command figures known as the NSC Deputies Committee—debated whether to ask Congress to pass laws that would make end-to-end encryption technologies illegal.

Politico quoted one of the individuals who said, "The two paths were to either put out a statement or a general position on encryption, and [say] that they would continue to work on a solution, or to ask Congress for legislation." According to the report, no decisions were made in the meeting and a National Security Council spokesperson declined to respond when asked to comment.

The leaked information did not include specifics about what of the two positions was taken by which agencies. However, that such a high-level meeting was dedicated to the subject of data encryption—as well as the fact that the subject of their discussion was strategically leaked to the media—shows that the topic is one that continues to preoccupy the military-intelligence apparatus of American imperialism.

The topic of individuals and organizations "going dark"—blocking state access to electronic communications and file sharing with encryption—has been intensely debated within the US government for the past six years. After former NSA intelligence officer

Edward Snowden revealed to the world in June 2013 the existence of massive surveillance of every phone call and email message of the public by the National Security Agency, millions of people have adopted encryption practices around the globe.

Several of the technologies used by billions of people around the world—such as Apple iPhones and the texting app WhatsApp—utilize encryption technologies by default, preventing law enforcement access to personal information without approval of the user. One recent survey also showed that over 40 percent of corporate enterprise systems are using consistent encryption strategies in their business practices.

According to previous reports, the Department of Justice and the FBI have consistently argued in favor of doing away with encryption technologies through implementation of law enforcement “backdoor” access, while the Commerce and State Departments have warned of the “blowback” consequences of forcing through mechanisms for breaking widely used encryption methods.

The Department of Homeland Security is also divided on the subject with agencies such as the Secret Service, Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP) demanding an end to encryption technologies. They are above all frustrated by encryption blocking surveillance efforts to crack down on immigrants and asylum seekers attempting to enter the US as well as thwarting attacks on undocumented workers already in the country.

The conflict between the big technology corporations and the state over encryption has intensified during the years since the Snowden revelations. The tech monopolies argue that opening back doors to law enforcement will undermine the competitive position of US companies in the global market for computer technology that demands these capabilities in order to be considered reliable.

For example, following the rift between the FBI and Apple over access to the iPhone of a San Bernardino terrorist in December 2015, investigators eventually figured out a way to get into the phone without Apple’s assistance. In response, the giant corporation proceeded to develop a “USB restricted mode” that blocked similar future attempts to crack iPhone security.

The special USB mode—which stops connected devices from communicating with an iPhone after it has been locked for an extended period—was designed by Apple specifically to curtail tools like GrayKey that are used by law enforcement to access personal information without authorization.

There has been consistent bipartisan support for forcing Silicon Valley to work with federal agencies on a backdoor access solution. As the *Politico* article points out, the San Bernardino events took place under the Obama administration, and FBI Director James Comey took the lead in publicly attacking Apple for “trying to create a space beyond the reach of US law.”

Politico notes, “The transition between the Obama and Trump administrations saw a hand-off of sorts between two high-profile advocates of the need to access encrypted data. After President Donald Trump fired Comey, Deputy Attorney General Rod Rosenstein succeeded him as the government’s top ‘going dark’ warrior.”

As a Deputy Attorney General, Rosenstein spoke publicly about the need for law enforcement access to encrypted information. He has persistently attacked encryption on the grounds that it is “warrant proof,” “ubiquitous” and blocks “collection of evidence” on devices by default. In a country where the state has repeatedly violated the most basic democratic right against “unreasonable searches and seizures,” Rosenstein has absolutely no qualms about asserting that encryption is a “significant detriment” to public safety.

Meanwhile, technology defenders of encryption practices have repeatedly—and effectively—warned that creating a law enforcement cryptographic “master key” has a very high likelihood of being compromised and falling into the hands of dark web hackers or other “bad actors.”

In the same way that the NSA server of cyber warfare tools was mindlessly left vulnerable and hacked in 2016 or the Stuxnet computer virus was unleashed by US intelligence on Iran in 2010 and subsequently infected Windows computers around the globe over the next five years, plans to hide encryption keys “under the doormat” for law enforcement will lead inevitably to a calamity, the consequences of which are impossible to predict.

3 July 2019