Beware Psiphon, CIA tech tool to assist, fuel global protests

by

Kit Klarenberg

on

Press TV

Ever since foreign-backed riots broke out in Iran in mid-September, Western news outlets have frequently drawn attention to the role of Psiphon, a free, open-source smartphone application and computer program that allows users to circumvent restrictions on websites and online resources in helping troublemakers organize and coordinate their activities, and send and receive messages to and from the outside world.

In the process, Psiphon has received untold amounts of highly-influential free advertising, and some Iranians - along with residents of West Asia more widely - will no doubt have been encouraged to download the software.

However, not a single mainstream source has hitherto acknowledged the spectral origins of Psiphon, let alone the malign aims it serves, and sinister purposes to which it can be put by its sponsors in the American intelligence community.

Psiphon was launched in 2009. Avowedly intended to support anti-government elements in countries

the company considers "enemies of the internet", the resource employs a combination of secure communication and obfuscation technologies, including VPNs, web proxies, and secure shell protocols (SSH), which allows users to effectively set up their own private servers that their own government cannot monitor.

Over Psiphon's lifetime, it has been funded and distributed by a variety of spook-adjacent organizations.

For example, it was for several years promoted by ASL19, which was founded by an Iranian expat Ali Bangi in 2013 to capitalize on the vast US funding flowing for "internet freedom" initiatives in the wake of the Arab Spring.

A June 2011 New York Times probe into Washington's "internet freedom" push concluded that all these endeavors serve to "deploy 'shadow' internet and mobile phone systems dissidents can use to communicate outside the reach of governments in countries like Iran, Syria and Libya."

Bangi's proximity to the US government was made abundantly clear when in 2016 he attended the White House's annual celebration of Nowruz, invariably a coming-out party for elite state-sponsored "regime change" activists.

Such high-level appearances, along with his status as a permanent fixture at tech conferences and digital rights events, cemented his place as a "rock star" figure within the Iranian diaspora community.

Bangi was nonetheless forced to resign from ASL19 in 2018, after he ended up in court in Canada on charges of sexual assault and forcible imprisonment.

A resultant profile in technology industry magazine The Verge alleged that he had fostered a culture of widespread drug use, sexism, harassment, and bullying within the organization, with female employees a particular target of his ire. On several occasions, he was aggressive and even violent towards staff.

With Bangi and ASL19 out of the picture, in 2019, Psiphon began receiving millions from the Open Technology Fund, created seven years earlier by Radio Free Asia (RFA), which in turn was founded by the US Central Intelligence Agency (CIA) in 1948 after it was officially authorized to engage in "black operations", including propaganda, economic warfare, sabotage, subversion, and "assistance to underground resistance movements."

In 2007, the CIA website ranked RFA and other "psychological warfare" initiatives such as Radio Free Europe and Voice of America among "the longest-running and most successful covert action campaigns" it ever mounted.

Today, RFA is an asset of the US Agency for Global Media, which is funded by the US Congress to the tune of hundreds of millions of dollars every year. Its CEO has acknowledged that the organization's priorities "reflect US national security interests."

OTF was one of the several initiatives that spun out of Washington's aforementioned "internet freedom" push.

Individuals intimately involved in making this desire a reality are under no illusion as to the true raison d'etre they are serving. In February 2015, Jillian York, an OTF advisory board member, stated she "fundamentally" believed "internet freedom" was "at heart an agenda of regime change."

OTF, being the brainchild of a US intelligence-created "psychological warfare" platform, illuminates a key purpose of Psiphon - ensuring citizens of countries in the crosshairs of ongoing US-led "regime change efforts" can continue to access Western state propaganda.

A November 2019 US Agency for Global Media factsheet on "tools supported by OTF" gives top-

billing to Psiphon.

"OTF provides USAGM networks with assistance to protect their content online and ensure it is resistant to censorship. For example, when USAGM news sites were abruptly blocked in Pakistan, OTF created mirror sites to ensure USAGM content remained available for key audiences...OTF provides emergency support to independent media outlets and journalists facing digital attacks to get back online and mitigate future attacks," it states.

A May 2020 OTF report on "highlights and challenges" of the year to date likewise notes that "veteran circumvention tool provider" Psiphon ensures USAGM-published content - which includes Voice of America Farsi - can reach audiences in countries where it is banned.

Similarly, a dedicated section of the BBC website, following the British state broadcaster's prohibition in Russia, in March offered an explanatory guide to how local residents can download the app via Android, Apple and Windows.

Should users "find it difficult" to access Psiphon via established app stores, they are invited to send a blank message to a listed email address to receive "a direct and safe download link."

In Iran, such utility is no doubt similarly invaluable given the fact that hostile media such as the BBC and RFA paint an utterly one-sided picture of the unfolding unrest, framing violent, incendiary actions by anti-government elements as peaceful, while wholly ignoring far larger pro-government popular demonstrations.

Another core Psiphon strength from the perspective of Western power is that it funnels all user data to and through centralized servers owned by the company itself.

While individuals' activities on the network might be shielded from the prying eyes of their own government, Psiphon can track what sites they are visiting and their communications in real-time.

This allows foreign actors to keep an unblinking eye trained on protesters and protest movements, and to respond accordingly.

Psiphon's meddling in Iran is now a long-established matter of public record. Back in 2013, the company published a blog hailing the "particularly big impact" it had made in the country, "coinciding with their (Iranian) presidential election."

While acknowledging Tehran had "always been a big challenge for us," Psiphon boasted that its software "stayed available" consistently during this time, despite repeated efforts to "severely throttle" operation.

That none of this background has emerged in any of the fawning mainstream puff pieces on Psiphon is shocking, but unsurprising.

Afterall, Western news outlets stand to materially benefit from a US-run protection racket projecting their agitprop to countless millions of people in secret.

And in becoming actively complicit in a US "regime change" operation, mainstream journalists are all less likely to acknowledge the reality of what's happening in Tehran, why and who stands to materially benefit from the government's ouster. That, however, is a far-fetched dream of Western powers.