GlobalResearch
Center for Research on Globalization

"Angst" Against Encryption: National Security and the Surveillance State. The Global Crackdown

By Dr. Binoy Kampmark
Global Research, December 07, 2015

State bureaucracy has a universal operating rationale: if an error occurred because of a flaw in the system, an oversight perhaps, or because of ill-planning, the solution shall relate to something else. It should be termed the iron law of non-resolution. It is one that holds resolutely in intelligence and security circles.

For the vast sums being put into defence and security, states across the globe find themselves numerous steps behind anticipating attacks. The starkest illustration of this was the November 13 attacks on Paris, a cruel unmasking of the national security state's inability to do what it was meant to. All that surveillance, all that eye-gazing and accumulation – to what end?

A notable point in all of this is that it took human indifference, an arrogant callousness that refused to accept intelligence from another agency. The excuse: security agencies get that all the time. Shrug the shoulders and go back to bed. Not that it was the sole cause – far from it – but it was fundamental. Errors are ultimately traceable to human agency.

The one system that remains a perceived friend and foe of government and state authorities in general is the Internet and the labyrinthine channels of communication it offers. It could not be anything else, being itself a child of the military. It was initially built to facilitate survival and secrecy, rather than its anti-twin, transparency. Unsurprisingly, it has become a rather vigorous battleground over encryption technologies.

Political representatives, feeling the pinch about the need to do something – anything – after a dramatic attack, have found the subject nearest to their loathing: encryption. Ranking intelligence committee chair Senator Dianne Feinstein from California has gone so far as to call encryption the Internet's "Achilles' heel" when it is, in fact, its invaluable, strengthened torso.[1]

Feinstein's Jekyll-Hyde reasoning here is that privacy will be protected by the surveillance state because the State is not particularly interested in the frivolities of the ordinary citizen. It is the greatest canard of all: data collection programs, and the means to access communications data, actual serve a broader public good. We are the eyes in the background overseeing that good is done. But repeatedly, Feinstein's assertions that such programs target "foreign governments, terrorist groups and overseas criminal syndicates" have been shown to be a product of either a deceptive mind, or at least an overly convinced one.

What a tease and annoyance encryption has become for intelligence and security personnel who struggle to fulfil their briefs. Chatter between terrorist cells, it was said, took place discretely and secretly. Yet even French authorities admit that the November 13 attacks

were not facilitated by encrypted communications.

Many such attacks tend to be preceded by boisterousness, a screech promising martyrdom plastered across social media postings. A notable feature of ISIS recruits and others who have joined the jihadi fruit salad of brutal converts is their distinct inability to shut up. Gabble before you die. If you want to find them, just scroll down the lists, scour the search engines, and sip your coffee.

In France, a heated effort is underway to target systems that ensure strong encryption protections. While these are still at a planning stage, the fact that they have made it to the memorandum continues to show the jittery nature of responses to November 13. According to *Le Monde*, it has obtained an internal document from the Ministry of Interior authored by the French Department of Civil Liberties and Legal Affairs outlining two key proposals to be brought before France's parliament.

One proposed bill involves looking at ways to ban Tor (the onion router), a service that is attractive in anonymising Internet users.[2] The document suggests that efforts could be made "to block or forbid communications of the Tor network" that would go beyond that of a state of emergency. This would be a tall order, but not impossible, if authorities can arm-wrestle internet service providers to do their bidding.

"Shared or open" Wi-Fi networks during a state of emergency are also on the table, and would be the subject of a second bill, ostensibly as a counter-terrorist measure. Again, the rationale here is that suspects can engage in clandestine communications using publically available Wi-Fi networks beyond tracking.

The markedly daft suggestion? Shut down the hotspots; close down the access points. Never mind the basic fact that many such suspects use open communications on unencrypted technologies.

Much of this is also state sloth, the imperative of the failed; officials simply uninterested in making efforts to, for instance, crack Tor communications. Researchers at Carnegie Mellon's Computer Emergency Response Team staged an attack on the service last year between February and July that demonstrated that deanonymizing could also be initiated.[3] Bad for Tor, but surely a point that should have been jotted down by the sleuths.

Other efforts have also been made to limit Tor's use in China, whose authorities work around the clock to limit various services available through the Internet in what has been called the Great Firewall of China. Blocking sites is a regular feature, and VPN services have become a subject of particular interest.[4]

That will not come as surprising to the tech watchers and liberty lovers who insist that the PRC is prone to such measures. But when the President of the United States does more than hint at weakening encryption to defeat a foe, all take notice. In his Oval Office address on Sunday, Barack Obama revealed he would "urge high-tech and law enforcement leaders to make it harder to use technology to escape from justice." It should, however, be said that the White House rejected a proposal in October that would have permitted authorities the means to weaken encryption technologies.[5]

FBI director James Comey, undeterred, will keep up the pressure to do so, having badgered

Apple and Google for some time to render their products more readily accessible to law enforcement authorities. (Call it Comey's "back-door" rationale to encryption, if you will.)

The disease that misrelates the actual cause to the hypothetical extends into coverage of terrorist attacks as well, with media outlets running blind with the official line of speculation that the terrorists involved in Paris just might have used encrypted services.

Trevor Timm in the *Columbia Journal Review* noted the trend all too well: "Why were officials saying it was 'likely'? Not because they had actual evidence, but because they assumed that if authorities *didn't* know about the plot in advance, the terrorists *must have* used encryption."[6]

Timm rounds off with the obvious point that encryption had become "an important tool for journalists of all stripes," protecting computers, phones, daily conversations with sources via text message or email that might be snared in the surveillance dragnet. And not just journalists. Undermining end-to-end encryption services may make accessing information by state authorities easier; but it will not make them more competent. What diminishes online security for some invariably diminishes it for all.

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

Notes:

[1] http://www.cbsnews.com/videos/feinstein-the-achilles-heel-in-the-internet-is-encryption/

[2] http://www.lemonde.fr/attaques-a-paris/article/2015/12/05/la-liste-musclee-des-envies-des-policiers_4825245_4809495.html

[3] http://gizmodo.com/attack-on-tor-has-likely-stripped-users-of-anonymity-1613247621

[4] http://techcrunch.com/2015/09/07/china-continues-its-crackdown-on-vpn-services/

[5] http://www.dailydot.com/politics/obama-encryption-backdoors-debate-status-quo/

[6]http://www.cjr.org/first_person/misinformation_and_misconceptions_how_not_to_report_on_the_encryption_debate.php

---