Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)
06/16

THE ENCRYPTION DILEMMA: COMBATING THE *SCOURGE OF TERRORISM WHILST BALANCING CIVIL RIGHTS AND NATIONAL SECURITY*

Gp Capt Ashish Gupta
Senior Fellow, CAPS

The year 2015 was the annus horribilis for the way the terrorism plagued the world without remission and with unabated violence and heinous aggravations. The Charlie Hebdo shooting, suicide bombings at the mosques in the city of in the city of Sana'a Yemen, the beach resort shooting in Tunisian town of Sousse, Khan Bani Saad bombing in Iraq during the Eid al-Fitr celebrations, Ankara bombings near Ankara central station in Turkey, Russian Metro jet airliner crash over Egypt's Sinai desert, November Paris attacks, San Bernardino shooting in California USA – these are the grim reminders that the scourge of terrorism is on the increase and the scope and destructiveness of the terrorist attacks are unprecedented in recent times. The advent of 2016 does not bring any respite from terrorist violence. The Pathankot terror attack, terrorist attack in Jakarta Indonesia, attacks in the Ouagadougou, the capital of Burkina Faso firms up the resolve of international community to work together to eradicate the scourge of terrorism.

Some of the terrorist attacks were scrupulously planned and remained below the radar of law-enforcement and security agencies till their culminations. It has been reported that the Islamic State of Iraq and Syria (ISIS) operatives use encryption communication for exchange of information. Besides, ISIS uses the power of social media as a key instrument of coercion, enticement, indoctrination, pro-selytization and propaganda for waging its own version of modern jihad. Its operatives have switched to more sophisticated form of encryption to evade detection. The messaging apps like WhatsApp, Viber and Telegram are increasing being used by ISIS and other militant

organizations. As these messaging apps use sophisticated and end-to-end encryption, the shared messages- despite of their dark and insidious contents- cannot be decrypted even by app's creators, owners and developers.

After the San Bernardino shooting, on December 09, 2015the FBI Director James B. Comey, while making a statement before Senate Judiciary Committee brought out that ISIS is increasingly using encrypted private messaging platforms. He said that, " This real and growing gap, which the FBI refers to as "Going Dark"; we believe it must be addressed, since the resulting risks are grave both in both traditional criminal matters as well as in national security matters." He further commented that the US government is trying to ensure that the private players who own and operate these platforms - with end-to-end encryption - understand the national security risks that results from the use of their encrypted products and services by malicious actors. Though there is no legislating obligation upon these companies, the companies are being asked to cooperate constructively with the US government. [1] France, the country that rates value of privacy much higher than other countries is now considering outlawing the 'encryption' in the wake of the Paris massacre. The British Prime Minister, David Cameron has made similar demands.

Encryption is the bedrock of digital economy, high digital trust-quotient and privacy protector. It is the underpinning of the internet ensuring the privacy of mail, secured e-commerce transactions and protection from cyber espionage. End-to-end encryption ensures that the data in any conceivable form are encrypted in transit and in storage and the key to decrypt this available only with those mutually communicating. In effect, the US government is trying to force the tech companies to provide 'back doors' within the encryption schemes to facilitate privileged access to law enforcement and secret services.Some of the top US top brass and intelligence officials including FBI Director Comey met with the executives from Apple, Facebook, Twitter and Google in Silicon Valley on January 8, 2016. [2] The CEOs of top tech companies including Apple CEO Tim Cook were extremely firm on their stand of doing nothing which could dilute the privileges and protection of their customers. In one of his speech, Tim Cook made his stand very clear by saying that, "we at Apple reject the idea that our customers should have to make tradeoffs between privacy and security. We can, and we must provide both in equal measure. We believe that people have a fundamental right to privacy. The American people demand it, the constitution demands it, morality demands it." [3] The law enforcement officials, on the other hand insisted that surveillance on suspected terrorists would help them to prevent horrific acts of violence, like those in Paris and San Bernardino, Calif.

The issue has now acquired emotional and political overtones and in the run-up for US Presidential election 2016, has become a hotly debated issue. Most of the2016 Republican candidates have rallied behind the issue, arguing that government agencies ought to be given the same access to text messages and data on cell phones that they can get by wire tapping a landline. Democratic candidates have been more circumspect, calling for a balance between civil rights and national security.[4]

The similar issue had cropped up in the past when Philip R. Zimmermann, the creator of Pretty Good Privacy (PGP) - an email encryption software package which was published for free on the Internet in 1991 - was subjected to a three-year criminal investigation.[5] At that time, the US government felt that the publishing of PGP on internet tantamount to export of cryptographic software, which could harm national security. In fact, the cryptographic software and related technical data are specifically enumerated on the 'Munitions List' and require a license for exporting.[6] In response, Zimmermann published his source code as a book and invoked his right to free speech provided by the First Amendment to the U.S. Constitution which states that "Congress shall make no law ... abridging the freedom of speech."[7] The US Supreme Court ruled that Zimmermann's public distribution of PGP was a protected form of speech under the First Amendment and the case was dropped in 1996.

Melvin Kranzberg once famously commented: "Technology is neither good nor bad; nor is it neutral."[8] It is not possible to outlaw encryption technology. Once the technology genie is out of the bottle, it is difficult to put it back in. If, for argument's sake, we concede that every device is stripped of protection provided by encryption or is fitted with back door, these will leave them much more vulnerable for exploitation from hackers cyber criminals and possibly from terrorists. The back door, designed for law enforcement agencies can also be exploited by the terrorists. Besides, writing a new encrypted app is not exactly rocket science and switching over to apps made in other countries without restrictive regulations will be child's play. On the other hands, law enforcement and security agencies - mandated and entrusted with the responsibility to combat scourge of terrorism and to protect innocent people from heinous terrorist attacks and unimaginable atrocities – want to identify even subtle and fleeting signatures to determine magnitude, timing and place of immediate response by way of continuous and unhindered monitoring of activities and communication of the suspected terrorists. The debate is not going to die down anytime soon and it looks like both the parties have valid and compelling points in support of their respective arguments. Nevertheless, how valid the arguments may be there is no denying of the fact that the global scourge of terrorism can only be exterminated

through the collaborative and integrated efforts - of global political leadership, military law-enforcement, intelligence and security agencies, financial institutes and public and private companies- even if it require giving up of parochial concerns, financial considerations and sense of misplaced morality.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

Notes

[1] The US Federal Bureu of Investigation, *Oversight of the Federal Bureau of Investigation*,James B. Comey, Director, Federal Bureau of Investigation, Statement Before the Senate Judiciary Committee, Washington, D.CDecember 09, 2015, https://www.fbi.gov/news/testimony/oversight-of-the-federal-bureau-of-investigation-8, accessed on January 20, 2016.

[2] Haley Sweetland Edwards, "Why we can't unscramblethe fight overencryption,"*Time*, January 25 , 2016, p.25.

[3] Matthew Panzarino,"Apple's Tim Cook Delivers Blistering Speech On Encryption, Privacy" , *The Techcrunch* , June 2, 2015, http://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy/#.oero2hn:kVGu, accessed on January 20, 2016.

[4] Edwards, n. 3, p.26.

[5] Philip Zimmermann, Creator of PGP and Co-founder of Silent Circle, https://www.philzimmermann.com/EN/ background/ index.html,

[6] Stay, Ronald J., "Cryptic Controversy: U.S. Government Restrictions on Cryptography Exports and the Plight of Philip Zimmermann," Georgia State University Law Review: Vol. 13: Iss. 2, Article 14

[7] The Constitution of the United States of America, Amendment I

[8] James W. Fraser, *Reading, Writing, and Justice: School Reform as if Democracy Matters*, (Albany: State University of New York Press, 1997), p.142.