Watching online space

Nighat Dad[*]

[*] Nighat Dad, a lawyer and human rights activists, is the Executive Director of Digital Rights Foundation, Pakistan. She has been recently included in Next Generation Leaders List by TIME's magazine for her work on helping women fight online harassment.

Needless to say, militants exploit online space for their narrow agenda. Internet proliferate their messages, spreading it to distant areas and unknown people. Jihadist groups, for instance, run websites which freely offers videos and magazines espousing their thinking; anyone can read that material and watch video. This way, online medium serves as yet another recruitment and propaganda platform to the militants.

With this mind, probably, the government inserted a point, in NAP, of regulating social media and internet.

Surely, checking internet is one important step in eliminating terrorist. But several factors raise doubts if the effort will ever be effective in catching terrorists.

First of all, how much of online space has in reality been exploited for recruitment in Pakistan is unknown. Yes, the failed Times Square bomber drew inspiration from YouTube videos of an Al-Qaeda ideologue in Yemen, but that was in the United States, not Pakistan. Pakistani militancy has largely made inroads in those areas where the accessibility of internet is low, like FATA or south Punjab.

This is not to say that urban terrorists don't rely on internet. They do. But they are steps ahead of the monitoring measures our officials have been thinking of. Militants reportedly send each other messages in encrypted language or by leaving messages at public forums.

Squeezing open space

Post-NAP, the suggested remedy by the government is not in synch with the digital bits on ground. Reportedly, the government has been planning to roll out cybercrime bill, in response to the militant threat. That bill will encompass activities beyond the domain of terrorism.

Modern-day terrorism that confronts Pakistan is a temporary phenomenon. It has come to haunt us after the 9/11 attacks mostly. Since then, there has been urges to fight militants at home. Much of the failure in driving militancy out has to do with our inaction and confusion. Once the state decides to face militants head-on, as it claims so, terrorist won't stay for long.

What is need is a time-bound response, not something that is ever lasting. Military courts are a case in point, to which political parties agreed only when the government ensured that the courts will stay for two years only.

The cybercrime bill will stay forever. Once enacted, it will stay as law.

The said bill is draconian, simply. With no protections, the bill slaps strict punishments: several years of punishment, and hefty fine. People can be grilled for mere suspicion; their devices could be confiscated. Likewise, the definition of "anti-Pakistan" is too vague. The law can also punish someone accused of supporting crime.[1]

Surely, no country should compromise on is national security, but having a law that strips off rights for ever, in the name of security, is not a reasonable way out. The law declares terrorist anyone who commits crime online. The two need not be connected.

Currently, the bill is sitting with the standing committee of the National Assembly. A working group has also been constituted to 'fine tune' the bill. But the whole process is kept secret. Little is known about the group's members, meeting minutes, and other details.

To be sure, the exercise on drafting a cybercrime bill starter much earlier. And it includes a broad range of issues including electronic theft. But, it was after NAP that more urgency was expressed to re-draft the bill that caters to the militant problem and pass it immediately. To some, the substance of the cybercrime bill is based on countering the militant threat.

Anusha Rehman, minister for I.T., readily admits that the need for new bill is contingent upon the militant threat. On one occasion, she counted security agencies and IT stakeholders (ministry of IT, IT professionals) as the only two stakeholders to the bill. When asked if civil society can be counted, she dismissed the calls.

Clearly, what she and her party ignores is that should political landscape change a bit, they might find their own colleagues dragged under the cybercrime bill.

Surely, abuse or hate speech populates online space. Lately, there has been a tendency among some section to out rightly degrade, curse, and harass others. They should be checked, as demanded passionately by human rights activists. But such hate speak is often traced to the corridors of the rightwing speakers, who quickly jump at questioning the faith or loyalty of their rivals. Such people squeeze whatever little space there is for those desiring a pluralistic voice. And they go unchecked.

As of now, the suggested remedy by Pakistani government aims at further squeezing those voices, to the advantage of those who flout an

[1] For details of the amended bill, see: Waseem Abbasi, "Law to punish cyber-crimes on the cards," *The News*, September 7, 2015.

exclusive agenda aimed at stifling voices of other people.

This despite that there are already laws through which the government can keep an eye on terrorism activities online; being one of them; Anti-Terrorism Act 1997 deals with terrorism, Section 509 of the PPC deals with crimes against women and the 1887 Telegraph Act. Then, there is Pakistan Protection Act, with a breakout time of two years. And so forth.

Ironically, the goal-oriented terrorists find their way out. They are tech-savvy, too. It would not be an exaggeration to say that they operate beyond the capacity of the government.

What is, therefore, worrisome is that while the terrorists might get away with their acts, the common citizens will come in the crosshairs.

A committee was also formed to monitor the progress on this point of NAP. Nine months later, there is no information available about the committee meetings and decisions made.

Black and white approach

The government has limited technical capacity of handling cyber-related issues, as if there is little understanding of the issue.

Generally, when it comes to data collection, the agencies have to get a warrant for that, under Fair Trial Act. However, on what the government has been doing, the approach is in black and white, comprising of two key elements: monitoring and censorship.

The government has already been monitoring web and suspending websites it accused of being anti-Pakistan. As of now, internet in Pakistan is regulated by Pakistan Telecommunication Authority, a regulatory body. According to a report by Privacy International, as of June 2013, Pakistani intelligence agency "sought to develop a mass surveillance system" to monitor Pakistani internet users on a massive scale following American National Security Agency model.[2]

The government's approach is buying software worth millions of dollars. Fin Fisher costing 57 million Pakistani rupees is an example; rather ironically, this surveillance software, costing millions of dollars, monitored on a handful of people.[3]

[2] "Tipping the scales: Security & surveillance in Pakistan," Privacy Intelligence, https://www.privacyinternational.org/sites/default/files/PAKISTAN%20REPORT%20HIGH%20RES%2020150721.pdf

[3]"Pakistan is a Fin Fisher customer, leak confirms," DRF, August 22, 2014,

Then, there were reports that Pakistani IT companies, on behalf of security agencies, have approached notorious international firms, like Hacking Team, to buy surveillance technologies worth of million dollars. A recent Privacy International is an eye-opener in this regards.

For late, the government has been planning to lay a mass surveillance system; even a tender has been floated.

Rather strikingly, the government has blocked websites that have nothing to do with terrorism. On the other hand, the websites of terrorism are freely accessible. Part of suspicion owes to government's selective regulation of internet: while the government has eagerly clamped down on Baloch websites, websites luring youth on religious grounds stay open.

There are also several codes invoked to clamp down on internet users: Anti-Terrorism Act, Pakistan Protection Ordinance, blasphemy law, exceptions of article 19 of the constitution. These legislations empower different security bodies to do the job. ATA gives power to police, proposed cyber bill to the agencies, and PPA to the military. There are stark disagreements among them, yet the same power is diffused to different authorities.

With new law, government's surveillance will be further unregulated and massive, although it is mentioned that the Fair Trial Act 2013 will be followed to acquire the warrants from High Court to conduct surveillance however there is still an accountability question about the implementation of such FTA provisions aim to regulate surveillance powers by agencies. From the outset it is still too arbitrary and collected data end up to exploit political gains.

One of the provisions of the proposed bill deals with seized data. Under the law, the government will retain the data for one year, whereas the ISPs are asked to keep it for long. There is fear that the government cannot protect the data it intends to retain, and that the data might get 'leaked' to exploit political goals.

We, demanding a change in this provision, are asking to remove the requirement for blanket retention of metadata by service providers. Mandatory blanket retention of metadata is inherently disproportionate and therefore a violation of the right to privacy. Instead, service providers may be required, upon a judicially-authorized warrant, to provide the

http://digitalrightsfoundation.pk/pakistan-is-a-finfisher-customer-leak-confirms.

relevant authorities with metadata that the service providers collect for the purposes of delivering their services on specified individuals

There should be a comprehensive legislation on personal data protection. Pakistan has none. There is no way that victims of privacy violations can get legal remedy. Also a privacy commission should be established which should work as a watch dog and not only entertain peoples complaint s but keep an eye on upcoming legislations against violation of privacy rights.