Outline of Program Prism and its Effects on Cyber Security of Pakistan

Myra Asghar Abbasi
Department of Management Sciences, Centre of Advance Studies in Engineering, Centre of Advance Studies in Engineering, Islamabad, Pakistan

Abstract
The basic objective of this research paper is to explore in detail the salient features of the project PRISM – a clandestine NSA initiated endeavour aimed at launching extensive internet surveillance activities as a new anti-terrorism front – and its impacts on the cyber security of Pakistan.

Courtesy the revelations made by Wikileaks and the now the well-famed whistleblower, Edward Snowden, who was a former NSA contractor; the lid has been blown off the size and scope of America’s extensive surveillance activities across the globe.

Pakistan, which has been at the forefront of America’s war in Afghanistan, has been a major victim of the PRISM project. According to some figures unearthed, the bulk of NSA’s cyber surveillance missions have been conducted in Iran and Pakistan.

Hence, this research aims to uncover the extent to which the PRISM program has carried out its operations in Pakistan, what potential threats and challenges it poses to the country’s national security and what steps need to be taken to counter this issue.

Methodology
The methodology adopted was twofold. First, a detailed secondary research on the subject was carried out so as to underscore the major underlying reasons contributing towards this problem. For this purpose, relevant studies, data, stats and information already processed was carefully inspected and an understanding of the extent, magnitude and the degree of the effects of different reasons causing this problem was evolved.

Secondly, interviews were conducted of the individuals or organizations which have been a victim of this project.

Multiple initiatives undertaken by the current government were also screened citing data and facts collected during the research, the degree of their effectiveness was gauged and a judgment on whether they will yield the desired results has been made keeping in view the ever increasing need of privacy legislation of the country.

Based on the information gathered from the above stated methods, a comprehensive dissection of the problem was conducted and solutions suggested which, according to the understanding of the author, presents guidelines as to how to go about this dilemma in the coming days.

Nature and Size of the Problem
Youth is nowadays nearly living and breathing in social media. Every other person is actively using social networks and users hardly know they are being spied upon at all times. Their activities, conversations and personal profile, everything is under surveillance. U.S kept on spying every nation they wanted to with impunity from 2007 till 2013 when one NSA’s private contractor, Edward Snowden, oozed a few documents allied to the program.
After the devastating incident of 9/11, U.S government became more circumspect on matters related to its national security. They surreptitiously started a small program called “Prism”. Prism is a U.S surveillance program which started in 2007 featuring sizeable representation from NSA, CIA and FBI. Under its umbrella U.S is collecting enormous amount of data from social websites like Facebook, yahoo, google etc. along with millions of GB’s of data from the mobile companies like AT&T and Verizon [7].

The Prism programme composed of cyber assault against myriad governments, including members of the European Union. According to the information leaked by Snowden, NSA had even tapped phone calls of Germany’s chancellor Angela Merkel and also many embassies fell victim to its activities. This resulted in a diplomatic standoff between Europe and America, with the former being visibly perturbed over the latter’s disregard of its sovereignty and matters related to privacy of its citizens. European Union even demanded a probe into the matter and those punitive measures be taken against the culprits.

More than 90% of current web applications have some kind of development flaw in them that if anyone has any idea of hacking, then these faults help the cyber criminals and intelligence agencies to get any user’s online data. [10]

Historically, major legal problems arose from the difference between the laws of two countries pertaining to the matter, especially when one act is legal in one country and illegal in the other. The issue of territorial integrity and legal jurisdiction also emerged when the victim (A) and accused (B) were hailing from different geographical locations. In such cases when the accused is claimed for trial by the authorities of victim’s nation, (B) should possess dual criminality i.e. the act he executed should be considered illegal in the legislation of both the countries [3]

Data Collection by NSA for Prism

Under this program and with the help of email service providers, NSA has almost completely got its hands on all e-mails and they could even collect all kinds of encrypted data being transported on internet. [1]. This encrypted data is kept indefinitely for decryption and extraction of more information.

![Diagram of what does NSA collect](image)

**Figure 1- what does NSA collect**

As shown in figure-1, NSA is collecting two kinds of data. Members categorize the collection of emails in the collection of raw data, now-a-days major personal/official
communications are going on using internet. An e-mail sent and received has a lot of information on it other than the content e.g. internet protocol (ip), using which geographical location can be extracted. A sent and received e-mail is kept indefinitely in the servers even if it is removed from the client system [1]. Also, users of Facebook and other social networks carry this idea that if profiles and information is made private it is not accessible to anyone which is completely wrong. All the information about an account, public or private, is accessible on servers too [2]. So, technically there is no privacy as anyone who can access servers can extract all kinds of information about an individual by eyeing his e-mail inbox since the day it was made to the present time.

NSA has forced many telecom companies to give away their users data including Verizon [7], after the British colonial period when the British government searched personal properties a lot, at that time anger rose in public and they started reacting. At that time, the fourth amendment rose, according to which “the right of the people to be secure, in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supports by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” [7]

Data Processing for Prism

According to [5], the initial data collection and operation is performed by FBI “Data Interception Unit” (aka DITU).

The DITU then forwards the processed information to NSA program “PRINTAURA” which is used to control the traffic flow. NSA reviews the data and passes it on to next unit “SCISSORS” and “PROTOCOL EXPLOITATION S3132” where this data is filtered on the basis of their type’s i.e. audio, video, and other internet records. This data is further passed to another unit using specific paths (NUCLEON, PINWALE, MAINWAY, or MARINA) for the analysis. This data is saved in NSA’s servers in the end based on the date, source and type of data. This data is kept indefinitely and new information related to these tags keep on stacking in the servers.

Wiretapping was also one way to collect data. Spiers now-a-days collect data using handy devices, modern gadget and sometimes with the help of very good looking people e.g. James bond. [9]

Cyber Security and Laws in Pakistan

Since the division of sub-continent and inception of Pakistan’s police system in 1947-48, little has changed in the nature of the predictable crimes. Practically all conventional crimes have shared the characteristic of neighbourhood. The criminal and victim belong to same geographical site. However, the cyber domain now makes it possible to commit a crime from anywhere in the world with geographical constraints no longer serving as impediments. This new advancement has amplified global criminal doings. While criminals have been swift to embrace new technologies, law enforcing agencies have struggled to keep pace. There are a number of reasons for this, the primary one being limited funding and competing priorities [3]. Impacts of any surveillance program within the country are only measured effortlessly when the country has a legislation about cyber data-privacy. Unfortunately there is no such
law in Pakistan which impedes cyber-crime practices.

According to the local newspaper in Pakistan, and a British national daily newspaper “The Guardian” Pakistan is the second most spied upon nation. Snapshots of 2013 revealed that NSA collected 13.5 billion intelligence reports as shown in Table 2.

The Guardian mentioned in June 2013 that foreign intelligence surveillance court forced huge Verizon to provide the CDRs (All call Detail Records) for communications (I)between U.S and abroad (II)completely within U.S, and no one from NSA should disclose this information to any other person that NSA has sought perceptible information under this order [4]

As this monitoring law is not applicable outside U.S [5], NSA is not allowed to gather any information of any country legislatively that is why the national security agency approached the outer world by exploiting the privacy of their own citizens. Pakistan is being spied on easily using all the social networks (esp. FB, M.S, Apple, google, AOL, yahoo, skype, and yahoo) but telephonic data is received by gathering up the information of American citizens who connect with Pakistani’s using telephone.

Table 2: Most Spied on Nations by NSA

<table>
<thead>
<tr>
<th>Country</th>
<th>Amount of data NSA collects/ month</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Iran</td>
<td>14 billion</td>
</tr>
<tr>
<td>2 Pakistan</td>
<td>13.5 billion</td>
</tr>
<tr>
<td>3 Jordan</td>
<td>12.7 billion</td>
</tr>
</tbody>
</table>

Cyber trespass is a very common way of peeking in to anyone’s computer, network, that too without altering or misusing any kind of data from the system. Such kind of trespassing usually extract personal information from the systems and leave the user unaware of the whole process. [10]

**How to Counter Prism**

As it is evident from Table 2, Pakistan has borne the brunt of America’s surveillance operations carried out under the Prism project. That is mainly due to the fact that Pakistan is currently an important player and ally in America’s war in Afghanistan.

Though the Taliban militia against whom this war was waged is centred in Afghanistan, a sizeable amount of fighters and tribal people from Pakistan’s restive Federally Administered

Tribal Areas cross the porous Durand Line to fight against America who they see as a foreign occupier. Besides, there are a lot of other militant groups based in Pakistan who view America as the enemy and have remained active participants of this war.
Hence, to effectively dismantle its enemy in the region and to consolidate the gains which she made after overthrowing the Taliban regime, America has launched a vast surveillance programme within Pakistan also. Its size and scope has already been discussed thanks to the revelations made by Edward Snowden.

The issue of the presence of this intensive surveillance network inside the country poses several questions for the government and its strong military establishment. It is not just a matter of an aggressive American foreign policy towards Pakistan but an issue of national security.

Protecting the privacy and rights of its citizens is the responsibility of any government. Thus, it becomes pertinent that appropriate steps be undertaken to neutralize this cyber onslaught from America.

Firstly, a political consensus needs to be evolved in the country taking all the stakeholders on board demanding an end and curtailment of the Prism operations in the country. An effective and audacious resolution should be passed in the parliament voicing Pakistan’s resentment to this programme and sending out a strong message to America that such endeavours will not be tolerated. For that purpose, the government can link Pakistan’s support to America’s war with an immediate and complete end to her surveillance activities inside the country. Secondly, given the magnitude of the problem, Pakistan should emulate the European Union by turning to the United Nations, pressing for an expansion of Article 17 of the UN’s International Covenant on Civil and Political Rights. It should be demanded that an additional protocol be added to the law safeguarding the privacy of individuals in this digital and technological era.

Then, it is also crucial that efficient and effective cyber security mechanisms be prepared to repel any such incursions. The current state of cyber security in place at different mobile companies needs to assessed and upgraded. For this purpose, the government should provide necessary capital and resources to put a strong protective network firewall, purchase the essential infrastructure, arrange trainings of personnel and even hire proficient skilled individuals well-versed in the trade of cyber activities.

However, to undertake all these measures, willingness and a strong intention on the part of those concerned is a prerequisite. Given Pakistan’s pro-American foreign policy since its inception coupled with the fact that she draws an annual sum of 1 billion dollar from America’s coalition support fund, the chances of the government taking any measures which could affect its relationship with America remain to be bleak.

References
(21CW), 2014 IEEE Conference on , vol., no., pp.1,4, 24-26 June 2014-------


