Centre for Air Power Studies

# X-KEYSCORE – NSA's DIGITAL INTELLIGENCE CLUSTER

***Dilipraj. E***
***Research Associate, CAPS***

*"You could read anyone's email in the world. Anybody you've got email address for, any website you can watch traffic to and from it, any computer that an individual sits at you can watch it, any laptop that you're tracking you can follow it as it moves from place to place throughout the world. It's a one stop shop for access to the NSA's information. And what's more you can tag individuals using 'XKeyscore'. Let's say I saw you once and I thought what you were doing was interesting or you just have access that's interesting to me, let's say you work at a major German corporation and I want access to that network, I can track your username on a website on a form somewhere, I can track your real name, I can track associations with your friends and I can build what's called a fingerprint which is network activity unique to you which means anywhere you go in the world anywhere you try to sort of hide your online presence hide your identity, the NSA can find you and anyone who's allowed to use this or who the NSA shares their software with can do the same thing…"*[1]

- Edward Snowden

The above statement was made by Edward Snowden during a TV interview when questioned about the utility of XKeyscore to its users.

Edward Snowden exposed the functionality of Xkeyscore in "The Sydney Morning Herald" newspaper and "O Globo" newspaper in July 2013. The exposed document also

includes a 32 slide power point presentation which was used as training material for explaining the functions of the XKeyscore program to its new trainees. The uncovered classified documents revealed a number of scandalous facts about the Xkeyscore program which was scheduled to be declassified on 01 August 2032. Few exposed entries in the Special Source Operations (SSO) directorate inside the NSA dated 21 September 2012 announced that XKeyscore was operational.[2] It also revealed that a large portion of NSA's information collection in the internet comes from its allies across the globe. Based on the exposed slides and documents, it can be assumed that countries like Australia, Canada, Great Britain and New Zealand have had an active role to play in this program as contributors and partners of information sharing in this program. Also, according to Edward Snowden, Germany also has access to XKeyscore which he revealed during the TV interview.

When these documents were made known and were seriously discussed among the cyber community around the world, the NSA gave their justification for the program on their part. According to NSA, XKeyscore is part of the agency's lawful foreign signals intelligence collection system. NSA also claimed that only limited personnel in the agency could get access to XKeyscore in order to complete their assigned tasks. Moreover, there are multiple technical, manual and supervisory checks and balances within the system in XKeyscore to prevent deliberate misuse by anybody along with full audit on every search made by an NSA analyst to ensure that they are appropriate and within the perimeters of law. The agency argues that this type of program allows them to collect the information that enables them to perform their missions successfully – to defend the nation and to protect US and its allied troops abroad.[3]

While it seems to be a legitimate claim by the NSA, a deep study about the program reveals the real purpose of such clandestine programs by NSA.

***X-Keyscore Location and Function***

According to the exposed slides, XKeyscore is a Software tool which acts as a Digital Network Intelligence (DNI) Exploitation System/ Analytical Framework that performs strong (e.g. e-mail) and soft (e.g. content) selection of data and metadata and provides real

time target activity surveillance. The program stores all the data in the collection site indexed by metadata and can even provide a series of viewers for common data types. This program has a very few but focused team which works closely with the analysts and the support staff are integrated with developers. The whole teams' action in the program is based on mission requirements. The program is based on more than 700 servers situated in approximately 150 sites around the world and the network is a massively distributed Linux cluster.[4]


Fig 1: Location of XKeyscore sites.
Source: NSA X-Keyscore exposed slides

In this program virtually anything can be stored by indexing the data with a metadata. This program has the capability to analyse data at two levels – shallow and deep. While the shallow method would help to look into more data for identification of possible intelligence, a deep method with strong selection pointer is used to gather intelligence. A careful study of the exposed documents reveals that extraction of information from the XKeyscore is based on "Strong Selection" pointer. When there are strong selection pointers, the results are precise and if not, huge volume of data would be extracted which has to be browsed and filtered again and again in order to get the required information. This shows that the analysts have to be smart and innovative in order to extract the required information from the humongous volumes of collected data.

Therefore, according to the previously mentioned statement by Snowden, it is clear that anybody could become a potential target of NSA and NSA could track that person anywhere in the world with the help of XKeyscore and an intelligent and innovative analyst without moving from their location. The data for analysis is pooled in from all sources including allied countries, data collected through other surveillance programs, other departments of NSA and also data acquired through aerial surveillance using drones.

In short, XKeyscore is the processing and analysis phase of intelligence in NSA using which the agency claims to have captured over 300 terrorists. But few reports denote that XKeyscore brands any user of the TOR network as an 'Extremist' and the user is listed in the NSA's target list.[5] This evokes few questions regarding the arrested terrorists using XKeyscore as to whether they were really involved in terrorist organizations or are they just frequent visitors of TOR networks and other encrypted methods in the cyber space; in connection to their activities in the physical world that branded them a terrorist. Although answers to such questions will never be given by the agency, the fact is that, XKeyscore is only the first step in digital intelligence in the internet world and more such methods will come into effect in the cyber space as this domain is a Pandora's Box of intelligence according to many intelligence agencies around the world.

**ARTICLES BY SAME AUTHOR**

***ENHANCING INDIA'S CYBER HUMAN RESOURCE***

***"ACCESSING THE INACCESSIBLE" PART I: NSA's DIGITAL TOOLS OF ESPIONAGE***

***PART II: KEYBOARDs, USBs & VGAs***

***PART III: NSA'S TOOLS OF ESPIONAGE ON COMPUTERS***

***PART IV: NSA'S TOOLS OF ESPIONAGE IN W-LAN AND ROUTER***

***PART V: NSA'S TOOLS OF ESPIONAGE IN FIREWALLS AND SERVERS***

***More Articles***

## End Notes

[1] Edward Snowden, Personal interview to Norddeutscher Rundfunk, January 26, 2014.

[2] "How the NSA is still harvesting your online data", *The Guardian",* June 27, 2014, in http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection, accessed on April 4, 2014.

[3] "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'", *The Guardian,* July 31, 2013, in http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data, accessed on April 4, 2014.

[4] "NSA X-Keyscore", Exposed document in http://www.documentcloud.org/documents/743244-xkeyscore-slidedeck.html, accessed on August 4, 2013.

[5] "XKeyscore Exposed: How NSA tracks all German TOR Users as 'extremists'", *RT,* July 03, 2013, in http://rt.com/news/170208-nsa-spies-tor-users/, accessed on April 5, 2014.