COVERT CYBER CAPABILITIES OF THE US

DILIPRAJ E

INTRODUCTION

Though declared as the global common by the world, it is an undeniable fact that internet technology was conceived, developed, and nurtured in the US during the second half of the 20th century. In other words, the US was the cradle for cyber technology, especially the internet, which is currently the backbone of the global communication network. In fact, the internet is still indirectly governed by US laws which are secretly amended at times to be in tune with its national interests. Therefore, by default, the US has an edge over rest of the world in the cyber field, with advanced technological skills, institutional mechanisms, policy initiatives, skilled workforce and advanced implementation strategies. Such vital factors play an important role in making the US a leading, vibrant player in the complex domain of cyber space.

However, being widely acclaimed as the superpower of the world, the US has more responsibilities and accountabilities than any other country in securing and streamlining the conduct of activities in cyber space. Moreover, being the global hub for internet traffic because of the location of a larger cyber infrastructure, the responsibility increases manifold. The fact that there are more Internet Service Providers (IPSs) in the US than

Dilipraj E is Research Associate at the Centre for Air Power Studies, New Delhi.

in any other country and with the presence of the Internet Corporation for Assigned Names and Numbers (ICANN), the privately owned internet regulatory organisation, guided by the laws of the US, the bar of responsibility is raised further. In short, it can be said that in the present chaotic scenario of governance in the cyber world, internet functioning is primarily dependent on the laws, policies, infrastructure and security agencies of the US.

While many countries of the world have some overt cyber capabilities, these by themselves do not pose any threat to others as these capabilities are to be employed only during a time of conflict.

In this context, it is imperative for the US to have a robust security mechanism in order to safeguard cyber space from various threats across the domain. The defensive and offensive capabilities of the US should be efficient enough to not only protect its own national interest in cyber space but also be able to defend the global communication network. The defensive capabilities of the US are claimed to be the best in the world, but it remains an unproven fact as the country has not faced an actual threat of all out cyber warfare yet. Nevertheless, the effectiveness of US offensive capabilities in the cyber realm has been tested in various instances in the recent past and its abilities are growing day by day. A study of the US offensive capabilities in cyber space will reveal a few startling facts, not about its overt cyber capabilities but regarding its covert cyber capabilities.

While many countries of the world have some overt cyber capabilities, these by themselves do not pose any threat to others as these capabilities are to be employed only during a time of conflict. On the other hand, the very concept of covert cyber capabilities itself poses a serious threat to other players of the world, as these comprise an invisible weapon which can deflate the target's abilities without warning. Therefore, the revelations on the US' covert cyber capabilities through various sources since mid-2013 have created serious turbulence in the global cyber world which has led to a tectonic shift on all aspects from governance, regulations, ownership, legality, safety and security. It is this shift that will determine the fate of the internet and the future of cyber space.

However, while the US is trying its best to remain a superpower of the world in a multipolar environment, its covert cyber capabilities play an important role by virtually penetrating inaccessible corners of the world, which otherwise would not be possible through the traditional means in the real world, to keep the authorities posted/informed about issues pertaining to their national interest.

This paper deals with a study of the various covert cyber capabilities of the US which has taken aback the cyber community of the world. However, the paper will not cover the infamous National Security Agency's (NSA's) PRISM programme as it has gained enough limelight from the media—instead, the paper will concentrate on other covert cyber operations of the US which have more precise targeting capabilities and serious impacts.

The US is trying its best to remain a superpower of the world in a multipolar environment, its covert cyber capabilities play an important role by virtually penetrating inaccessible corners of the world, which otherwise would not be possible through the traditional means in the real world, to keep the authorities posted/informed about issues pertaining to their national interest.

US COVERT CYBER CAPABILITIES

X-Keyscore

According to the NSA of the US, X-Keyscore is a part of the agency's lawful foreign signals intelligence collection system. The NSA also claims that only a limited number of personnel in the agency can get access to X-Keyscore in order to complete their assigned tasks. Moreover, there are multiple technical, manual and supervisory checks and balances within the system in X-Keyscore to prevent deliberate misuse by anybody, along with a full audit on every search made by an NSA analyst to ensure that it is proper and within the law. The agency argues that such programmes allow it to collect the information that enables it to perform its missions successfully – to defend the nation and to protect US and allied troops abroad.[1]

While that seems to be a legitimate claim by the NSA, the real purpose of X-Keyscore was revealed when Edward Snowden exposed it through the *Sydney Morning Herald* and *O Globo* newspapers in July 2013. The exposed documents included 32 slides of a power point presentation meant for explaining the functions of the X-Keyscore programme to its trainees. This exposed classified power point document which was supposed to be declassified on August 1, 2032, reveals a number of shocking facts about the programme. An entry in the Special Source Operations (SSO) Directorate inside the NSA dated September 21, 2012, announced that X-Keyscore is operational.[2] It was also revealed that a large portion of the 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 an active role to play in this programme as contributors and partners of information sharing. Also, according to Edward Snowden, Germany also has access to X-Keyscore which he revealed in a TV interview.

X-Keyscore Location and Function

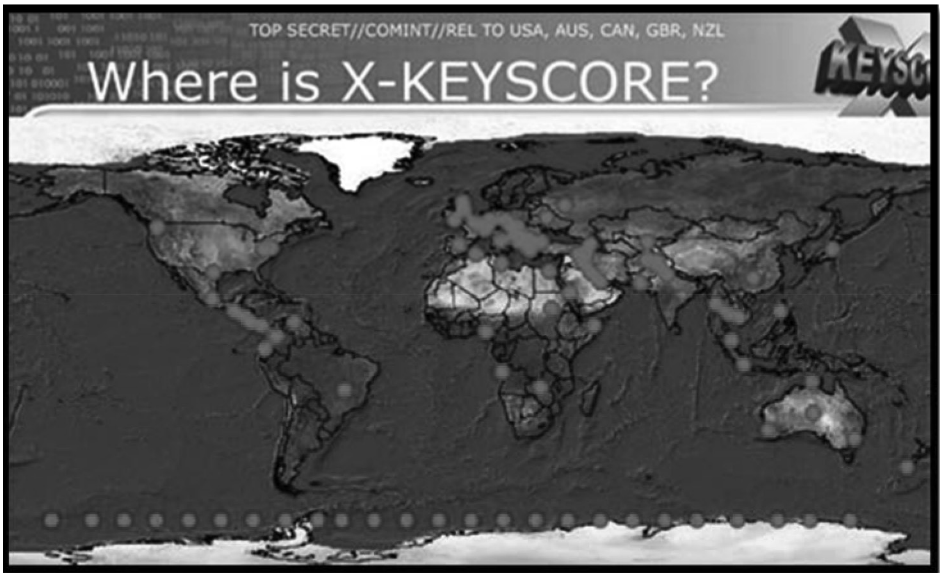
According to the exposed slides, X-Keyscore is a software tool which acts as a Digital Network Intelligence (DNI) exploitation system/ analytical framework that performs strong (e.g. e-mail) and soft (e.g. content) selection of data and metadata and provides real-time target activity surveillance. The programme stores all the data in the collection site indexed by metadata and can even provide a series of viewers for common data types. This programme has a very small but focussed team which works closely with the analysts and the support staff is integrated with the developers. The whole team's actions

[1] "X-Keyscore: 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.

[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.

in the programme are based on mission requirements. The programme is based on more than 700 servers situated in approximately 150 sites around the world and the network is a massively distributed Linux cluster.[3]

Fig 1: Location of X-Keyscore Sites



Source: NSA X-Keyscore exposed slides.

Virtually anything can be stored in this programme by indexing the data with a metadata. The programme 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, the deep method, with a strong selection pointer, is used to gather intelligence. Extraction of information from X-Keyscore is based on a "strong selection" pointer. When there are strong selection pointers, the results are precise and if not, a huge volume of data would be extracted which has to be browsed repeatedly 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.

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

The data for analysis is pooled in from all sources, including allied countries, data collected through other surveillance programmes, other departments of the NSA, and also data acquired through aerial surveillance using drones.

During a TV interview, when asked about the usefulness of X-Keyscore to its users, Snowden's reply was:

> 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 'X-Keyscore'. 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…"[4]

This statement of Snowden clearly reveals that anybody can become a target of the NSA and the NSA can track that person anywhere in the world with the help of X-Keyscore 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 programmes, other departments of the NSA, and also data acquired through aerial surveillance using drones.

In short, X-Keyscore is the processing and analysis phase of intelligence in the NSA, using which the agency claims to have captured over 300

[4] Edward Snowden, personal interview to *Norddeutscher Rundfunk*, January 26, 2014.

terrorists. But a few reports denote that X-Keyscore brands any user of the TOR network as an 'extremist' and the user is listed in the NSA's target list.[5] This raises questions regarding the terrorists arrested by using X-Keyscore as to whether they are really involved in terrorist organisations or are just frequent visitors of TOR networks and other encrypted methods in cyber space; and regarding their activities in the physical world that have branded them as terrorists. Although answers to such questions will never be given, the fact which can be understood is that X-Keyscore is the first step in digital intelligence in the internet world and more such software is to follow in cyber space as this domain is the Pandora's Box of intelligence, according to intelligence agencies around the world.

The TAO Department in the NSA is responsible for developing and employing technologies for endpoint operations. Endpoint operations involve the process of actively subverting systems that create, store or manage information like computers, peripherals and telephone switches, in order to directly retrieve data of intelligence value or achieve other operational ends.

TAILORED ACCESS OPERATIONS (TAO)

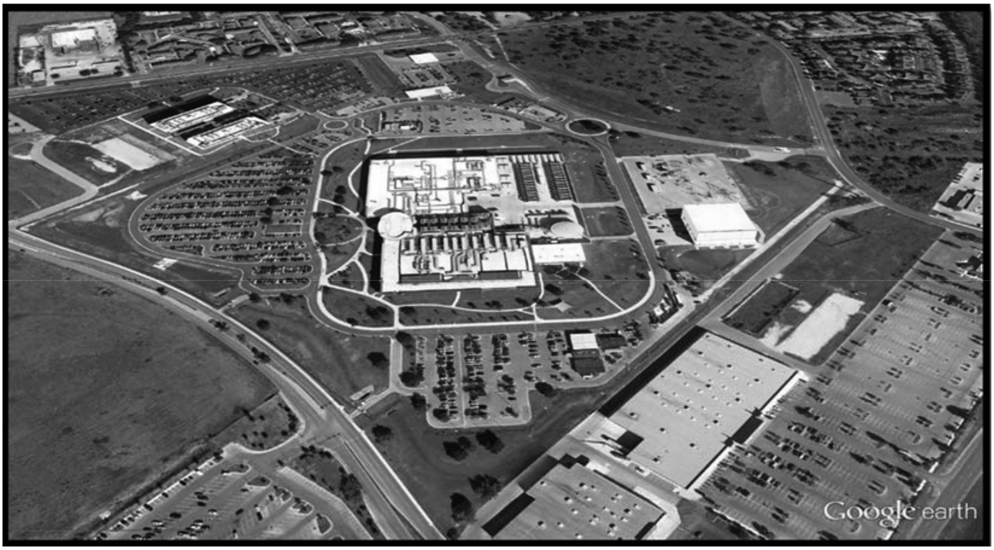
The TAO Department in the NSA is responsible for developing and employing technologies for endpoint operations. Endpoint operations involve the process of actively subverting systems that create, store or manage information like computers, peripherals and telephone switches, in order to directly retrieve data of intelligence value or achieve other operational ends. According to another revealed document titled "Expanding Endpoint Operations", which was written by an unknown colonel of the US Army as early as September 17, 2004, the TAO Department was increasing endpoint operations in terms of numbers and diversity of targets, and building a more scalable and robust endpoint operations infrastructure. The expansion

[5] "X-Keyscore Exposed: How NSA Tracks all German TOR Users as 'Extremists'", *RT*, July 3, 2013, in http://rt.com/news/170208-nsa-spies-tor-users/. Accessed on April 5, 2014.

process included the acquisition of a new endpoint access Remote Operations Centre (ROC) which would enable dramatic expansion of the operations of the TAO Department to be available for both its internal and external customers. While the internal customers are the NSA, Central Intelligence Agency (CIA) and Joint Special Operations Command (JSOC), the list of external customers include various intelligence agencies of countries like Australia, Canada, Great Britain and New Zealand.[6]

One part of the TAO Department of the NSA is believed to be operating from a base in Texas, which was earlier a Sony Chip Company and was later converted into the NSA's operative location in 2005.

Fig 2: The Location of NSA's TAO Department



Source: Google Earth.

According to revealed documents[7] from the Texas Cryptologic Centre, as of March 11, 2008, the break-up of employees of the TAO Department housed in the Texas-based centre is as follows:

[6] "Expanding Endpoint Operations", *SIDtoday*, NSANet, September 17, 2004.

[7] "Secret Documents: The Special Department TAO NSA Introduces Itself", *Der Spiegel*, December 30, 2013, in http://www.spiegel.de/fotostrecke/nsa-dokumente-die-abteilung-tao-der-nsa-fotostrecke-105355-3.html. Accessed on April 6, 2014.

Table 1: Sector-Wise Employees' Break-up of TAO based in Texas

Sector	Numbers	Breakdown
Civilians	30	Includes 1 AIA, 1 Intern
Military	30	US Air Force- 10 US Army - 8 US Navy - 10 US Marine Corp - 2
Total	**60**	
Civilian	Unknown	7 Selectees 9 Nominees Unknown No. of External Hires which include 3 CJO'd, 7 preliminary
Military	Unknown	Unknown No. Chiefs, etc 5 x USA Great Skills Billets 2 (additional) FIOCers not included (R&T)
Contractor	1	TAO/ ANT Contract

Source: "Sectret Documents: The Special Department TAO NSA Introduces Itself", *Der Spiegel*, December 30, 2013, in http://www.spiegel.de/fotostrecke/nsa-dokumente-die-abteilung-tao-der-nsa-fotostrecke-105355-3.html. Accessed on April 6, 2014.

Until 2008, TAO operations were conducted on targets in countries including Cuba, Venezuela, Iraq, Afghanistan, Mexico and Colombia. There were many kinds of operations conducted by the TAO Department involving different malwares/spywares and using different tactics for network penetration and installation of these spywares into the target's system. This includes spyware operations like Olympus Tickets, SHARPFOCUS (SF2), PARCHDUSK (PD and FOXACID messages. Initially e-mails were used to spam the target with FOXACID messages; later, the NSA QUANTUM method was started and became the method used to insert the FOXACID malware.[8] The operations of TAO are based on its motto *"Your data is our data, your equipment is our equipment – any time, any place, by any legal means"*.[9] This statement exhibits the overall intent of these clandestine organisations and covert cyber missions of the US, and their arrogance due to their possession of this supreme technology.

[8] Ibid.

[9] "The ROC: NSA's Epicentre for Computer Network Operations", *SIDtoday*, NSANet, September 6, 2006.

NSA QUANTUM

QUANTUM is one of the covert programmes of the NSA's TAO Department, targeting individuals' computers to implant specially built Trojans which enable surveillance on web-based accounts of the user in various platforms. Details about the QUANTUM programme were revealed in the German weekly *Der Spiegel* on December 30, 2013. This programme works on a concept called "man-on-the-side capability". The QUANTUM method of implant into a target is possible if the chosen target has a selector that is vulnerable to the QUANTUM technique and has been active for the last 14 days, and if detected by the single-sign on site which has QUANTUM capabilities. When a target qualifies with all these conditions, it is possible to detect the communication between the target's computer and the server in real-time and send the Trojan piggy-backing the requested content, and implant the host.[10]

The revealed documents on QUANTUM disclose the involvement of one of America's largest management consulting firms, Booz Allen Hamilton, in the programme along with the NSA's TAO Department. Going by the way the company's name appears in the document, alongside the TAO Department, it can be inferred that QUANTUM was developed by a team comprising personnel from both the NSA's TAO Department and Booz Allen Hamilton Company. The documents further reveal that apart from the US, QUANTUM also benefits the interests of Australia, Canada, Great Britain and New Zealand. In fact, it can be understood from the documents that if a partnering agreement form is set up with the General Communication Headquarters (GCHQ) of the UK, then the research and technology analysts of the TAO Department can utilise GCHQ resources in include additional capabilities to their QUANTUMTHEORY.[11]

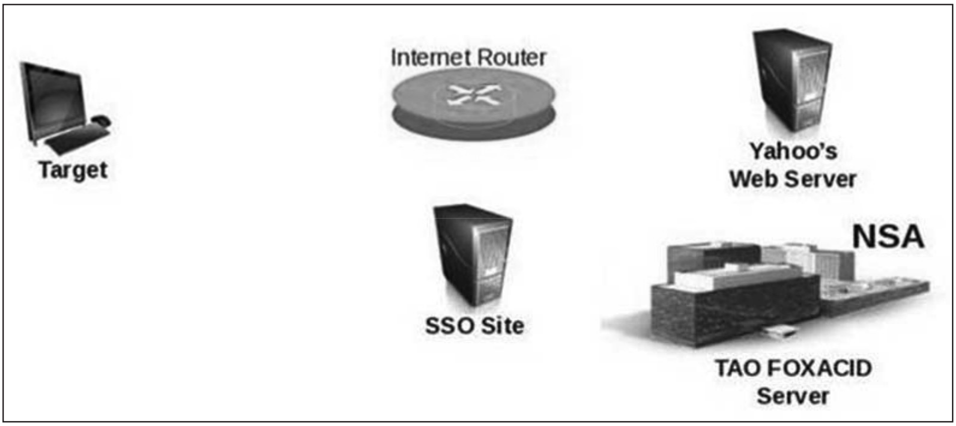
Functioning

The QUANTUM programme involves several nodes for its functioning. They are the target, internet router, Web application server, SSO site and the NSA's TAO FOXACID server.

[10] "(TS) NSA Quantum Tasking Techniques for the R & T Analyst", *Der Spiegel*, December 30, 2013.

[11] Ibid.

Fig 3: Various Nodes Involved in the Functioning of QUANTUM



Source: "(TS) NSA Quantum Tasking Techniques for the R&T Analyst," *Der Spiegel*, December 30, 2013.

The FOXACID server is an exploit server that is operated by the NSA's TAO Department for the QUANTUM programme to install the Trojans into the targets. The functioning of QUANTUM is clearly mentioned in the exposed documents and this revelation delineates the sophistication of the technology and the amount of effort that is required for this covert method of bugging. It is also mentioned that QUANTUM has been effective and successful against Yahoo, Facebook and other static Internet Protocol (IP) addresses. The functioning of QUANTUM as mentioned in the documents is as follows:

- Target logs into his/ her Yahoo account.
- SSO site connected with the internet router sees the QUANTUM tasked Yahoo selector's packet and forwards it to the TAO's FOXACID server.
- FOXACID server injects a FOXACID URL into the packet and sends it back to the target's computer.
- Simultaneously, the Yahoo server receives the packet from the target's computer through the internet router requesting e-mail content.
- Before the Yahoo packet reaches the target's computer, the FOXACID packet intervenes and beats it back to the endpoint.
- Though the target's Yahoo page is loaded, in the background, the FOXACID URL also loads which redirects to the FOXACID exploit server in the NSA's TAO.

- Now based on the exploitability of the browser, the FOXACID server deploys a stage 1 implant back to the target, thus, implanting the target with a Trojan.

It is claimed in the documents that QUANTUM is capable of targeting a wide range of realms like IPv4_public, alibabaForumUser, doubleclickID, emailAddr, rocketmail, hi5Uid, hotmailCID, linkedin, mail, mailruMrcu, msnMailToken64, qq, facebook, simbarUuid, twitter, yahoo, yahooBcookie, ymail, youtube and watcherID.

Also, the QUANTUM tasking can be done in two different ways. The Research and Technology (R&T) analysts can submit the QUANTUMTHEORY tasking upon which a stage 1 implant called VALIDATOR would be implanted on the target. Secondly, TOPI analysts can submit QUANTUMNATION tasking upon which a stage 0 implant called SEASONEDMOTH (SMOTH) is implanted on the target. A SMOTH dies within 30 days time of deployment unless there is a request to extend its life. The VALIDATOR is a small Trojan implant used as a backdoor access service against personal computers of targets of national interest, including, but not limited to, terrorist targets.[12]

Therefore, it is clear from the NSA's QUANTUM that anybody in this world can become a target for VALIDATOR or any other espionage and surveillance tool of the NSA if the person is perceived to be of some importance to the national interest of the US. Moreover, the NSA has the technological expertise to single out its target in this crowded virtual space and it can also pursue its covert methods of espionage by camouflaging its virtual communications within the trusted communications between the user and the web applications server. Another inference that can be arrived at is that the US has a free hand in tapping the internet router and is able to intervene in the communications between the user and the web applications servers because of the fact that most of the cyber infrastructure is available well within its legal and technical control jurisdictions. A feasible solution can be achieved on this front only with an effective internet governance model which involves participation from a truly global community.

[12] Ibid.

NSA ANT Catalogue

In December 2013, *Der Spiegel*, the German weekly newsmagazine revealed another of the NSA's sophisticated programmes, consisting of a digital toolbox called the "NSA ANT Catalogue". This article was co-authored by Jacob Appelbaum, Judith Horchert and Christian Stöcker. Unlike the PRISM programme which was exposed by Edward Snowden to the *Washington Post* and *The Guardian*, the exposure/whistleblower of this project is unknown. But the exposed catalogue reveals the magnitude and variety of digital weapons being used by the US intelligence agency to spy on its targets. The operations of the Advanced/Access Network Technology (ANT) division in the NSA's TAO Department range from penetrating networks, monitoring mobile phones and computers, to diverting, modifying and even deleting data. The network web created by the implants of these sophisticated tools is so big that it has succeeded in establishing a covert network for the NSA that operates parallel to the internet.

The leaked NSA ANT Catalogue is a 50-page document created in 2008. Its list is like a mail-order catalogue of digital tools, from which the employees of the NSA can order technologies from the ANT division for use against its targets. The ANT division is part of the NSA's TAO Department and they are specialised in covert data-mining and data-skimming operations, especially on specific difficult targets. ANT tools are like elite forces which are moved in only when the TAO's other hacking and data-skimming methods are not sufficient to gather the required information from their target systems.[13] While the ANT division develops both hardware and software required for these digital tools, the catalogue of these tools not only defines the operations of the tools but also gives the cost for every tool which ranges from free to $250,000.[14]

Every tool that has been developed by ANT has its own special purpose and the operating devices include almost all areas of the digital world from monitors, cables, USBs, routers, servers, mobile phones and

[13] Jacob Appelbaum, et al. , "Die Klempner aus San Antonio", *Der Spiegel*, January 2014.

[14] "Inside TAO: Documents Reveal Top NSA Hacking Unit", *Spiegel Online International*, December 29, 2013, at http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html. Accessed on April 6, 2014.

chips, at both hardware and software levels. Most of the NSA ANT tools that have been exposed belong to a family of clandestine tools called "ANGRYNEIGHBOR".

Analysis of NSA ANT Catalogue

A study on understanding the functions and operational capabilities of 50 NSA ANT tools helped to arrive at the following inferences:

- These tools are meant for special operations which are highly covert in nature for the purpose of information gathering, sabotage, espionage and surveillance.
- The functionality of the tools can be mainly associated with military operations, but not necessarily confined to the military only, as a few tools like COTTONMOUTH (USB-based) can also be used for non-military operations.
- A few tools belong to a family of tools called ANGRYNEIGHBOR, which denotes that there are more families of tools either under operation or development.
- All the disclosed documents related to the NSA ANT catalogue are dated in the year 2007. Therefore, there are high chances that these tools have become obsolete, and new versions and models would have replaced them by now.
- There are passing references to many new technologies whose functionalities do not appear in any of the exposed documents. This means that there are many more undisclosed tools developed by the ANT Department whose capabilities are unknown.
- Revelation of these tools would create a compulsion for the agency to either abandon them on the whole or switch to more covert methods of espionage and surveillance.
- In the case of abandoning, the agency would have to abandon many units of these tools which were operational in the field somewhere across the globe. If any other country's agencies were to lay their hands on these tools, identifying and investigating them could reveal more precise capabilities about them.

- Both hardware and software are implanted on devices manufactured by most widely used brands like Samsung, Cisco, Juniper, etc. Therefore, this results in distrust about US brands which, in turn, creates more hassles for any country's procurement body in terms of rigorous audit during procurement of any such devices from the US, especially for national security purposes.
- It is also revealed from the documents that the NSA implants a few of its tools by a method called interdiction, in which the agency would intervene during the supply chain process and place its implant on the devices before they get delivered to their intended recipient. This emphasises the need for enhancing the safety for any supply chain process, especially for defence equipment, irrespective of its size or function.
- The fact that many implants can be installed, controlled, operated and executed remotely emphasises the need for enhanced network security and also acts as a point of realisation for disintegrating and isolating a few sensitive networks from other national grids.

Since the cyber world is a trove of information, with the ability to virtually connect anything and everybody, this medium is utilised ably by all players for their covert operations in order to achieve their desired supremacy. Hence, the cyber domain has become the battleground of the future.

WHAT LIES AHEAD?

A futuristic look into cyber space, beyond capabilities and vulnerabilities, and by mapping the scattered dots, reveals the bigger picture of a game played by many players to achieve 'supremacy'. The US refers to this supremacy in the cyber domain as "global network supremacy".[15] As we live in the age of information, the ability to control and manipulate any given information gives a player the upper hand in this game. Since the cyber world is a trove of information, with the ability to virtually

[15] n. 9.

The use of covert capabilities helps the players to unveil the hidden plans of others by silently intruding into their networks, which helps them not only to orchestrate their immediate move but also to frame long-term policies and strategies.

connect anything and everybody, this medium is utilised ably by all players for their covert operations in order to achieve their desired supremacy. Hence, the cyber domain has become the battleground of the future. The various players are none other than entities that operate in the cyber world ranging from individuals to countries. Since the cyber world is slow in penetrating the real world, there is lot more to be virtualised. Till this is achieved and even after, the covert cyber capabilities will act as sabotaging tools to stop another player, in most cases, a country, from enhancing its capabilities in both the virtual and real worlds, and to keep them engaged in tackling the threats of sabotage. Also, at present, the use of covert capabilities helps the players to unveil the hidden plans of others by silently intruding into their networks, which helps them not only to orchestrate their immediate move but also to frame long-term policies and strategies.

A suitable example to understand the extent of danger a successful covert cyber operation can cause would be the series of events which unfolded in Iran in the recent past that changed the fate of the country's ambitious nuclear programme. Iran had started its nuclear programme with aid from the US in the 1950s under the then "Atoms for Peace" policy of the US. As the years passed and due to regime change in Iran, the country which was once an ally of the US, became a foe, and ended up facing economic sanctions from the US. The drift between the two countries also affected Iran's nuclear programme which the country struggled to continue with for long, until recently. However, with help from Russia, some other countries, and the nuclear black market, Iran sustained and enhanced its nuclear programme. Later, in 2005, when Ahmedinijad, became the president of Iran, the nuclear programme gained momentum and Iran began work towards enrichment of weapons grade uranium. Due to the failure in talks between the US and Iran, in December 2006, sanctions were imposed on Iran by the United Nations, initiated by the US, to curb its nuclear programme. However, these sanctions did not succeed in giving the desired results and Iran managed to move forward in its nuclear programme.[16]

In 2008, the centrifuges in the Natanz nuclear facility in Iran began to face unprecedented crashes. These breakdowns which seemed to be like small random accidents, continued till spring 2010 and the engineers in the facility were clueless about the reason for those crashes. In spring 2010, the situation in the Natanz facility began to deteriorate further when the centrifuges started functioning in a haphazard manner followed by more frequent and high intensity breakdowns, thus, affecting the entire nuclear programme of Iran. During this period, the engineers struggled to decipher the reasons behind the disruptions in the Natanz nuclear facility; later, it was discovered by Symantec, a cyber security products manufacturing company, that a highly sophisticated computer worm had affected the controller systems or Supervisory Control and Data Acquisition (SCADA) systems in the facility. This computer worm was named STUXNET, thus, becoming the first computer programme to be used as a cyber weapon. Additionally, technical papers started coming out related to its functioning.[17]

Later, Stuxnet started getting media attention and slowly media reports emerged about the origin of this computer worm. It was generally reported across all media that Stuxnet was the result of a joint effort by the US and Israeli intelligence agencies, the NSA and Unit 8200 respectively. It was reported that way back in 2006, after the negotiations between Iran and the West floundered, the US, during the Bush Administration, started a covert cyber programme codenamed

[16] "Timeline on Iran's Nuclear Programme", *New York Times*, November 24, 2014, in http://www.nytimes.com/interactive/2014/11/20/world/middleeast/Iran-nuclear-timeline.html?_r=2#/#time243_7215. Accessed on December 10, 2014.

[17] "How a Secret Cyber War Program Worked", *New York Times*, June 1, 2012, in http://www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-program-worked.html?ref=middleeast. Accessed on December 11, 2014.

Olympic Games in order to sabotage Iran's nuclear programme. The engineers at the NSA and Israeli Unit 8600 initially wrote a 'beacon' programme that could map the functioning of the Natanz facility and introduced it into the facility, possibly with the aid of an unsuspecting insider. The 'beacon' programme collected and transmitted information related to the facility's computer configurations and other such sensitive information to the agencies. Using the collected data, the engineers again wrote another complex 'worm' programme with the ability to disrupt the facility and, thus, introduced this programme into the computers of the facility through various unknown methods. The worm programme took control of many centrifuges in the facility which made them run either too fast or too slow and, at times, the centrifuges even exploded, whereby the worm succeeded in disrupting the nuclear programme of Iran. Surprisingly, in summer 2010, due to some programming error, the worm programme copied itself into the laptop of an Iranian scientist who worked in the facility. When the scientist connected his laptop to the internet, the worm spread to other parts of the world through the internet and that was when the malicious programme came to the notice of the world community. It was later revealed by the cyber research community that the Stuxnet programme that had spread through the internet was only one version of the various programmes written under the Olympic Games project, and many such variants were utilised on the Iranian facility in order to disrupt and sabotage the nuclear programme. Stuxnet had ably used some 'Zero-day' vulnerability in the Siemans Step 7 software which was widely used in the facility, to cause disruption. It was also reported that when Obama became US president in 2009, his predecessor President Bush successfully persuaded him to continue with the Olympic Games project by highlighting its importance.[18]

In 2013, Symantec came up with a research paper exclusively on Stuxnet, describing its evolution and different variants. This report ascertained that Stuxnet 0.5 was the oldest known Stuxnet version which was in the process of development as early as 2005 and it was in the wild since November 2007.

[18] Ibid.

Stuxnet 0.5 was less aggressive than its later versions, especially Stuxnet 1.x.[19] Some highlighting dates and the relevance of different versions of Stuxnet are mentioned in Table 2.

Table 2: Evolution of Stuxnet Versions

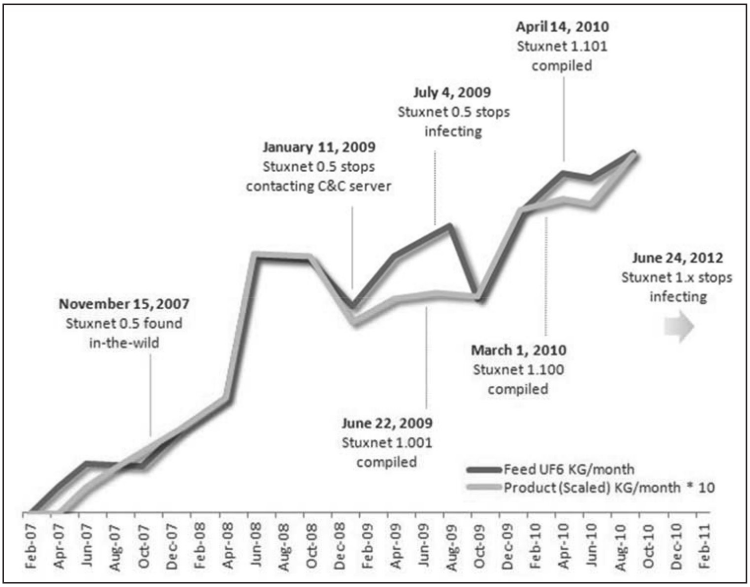
Version	Date	Description
0.500	November 3, 2005	C&C server registration
0.500	November 15, 2007	Submit date to a public scanning service
0.500	July 4, 2009	Infection stop date
1.001	June 22, 2009	Main binary compile timestamp
1.100	March 1, 2010	Main binary compile timestamp
1.101	April 14, 2010	Main binary compile timestamp
1.x	June 24, 2012	Infection stop date

Source: Geoff Mcdonald, Liam O Murchu, Stephen Doherty & Eric Chien. "Stuxnet 0.5 – The Missing Link", Symantec, version 1.0, February 26, 2013.

Fig 4 below shows the uranium enrichment production at Natanz with reference to key milestones of Stuxnet's development. Interestingly the highlighting dates in Stuxnet's life-cycle coincide with the dips in feed or production amounts and lower levels of production given the same or greater feed amounts (shown as gaps between the two lines).

[19] Geoff Mcdonald, Liam O Murchu, Stephen Doherty & Eric Chien. "Stuxnet 0.5 – The Missing Link", Symantec, version 1.0, February 26, 2013.

Fig 4: Low Enriched Uranium Production and Milestones in Stuxnet Coincidences



Source: Geoff Mcdonald, Liam O Murchu, Stephen Doherty & Eric Chien. "Stuxnet 0.5 – The Missing Link", Symantec, version 1.0, February 26, 2013.

Although the operational success of different variants of the Stuxnet worm remains unclear, it has succeeded in achieving various other aspects/ goals. These are:

One, this computer programme has succeeded in making the cyber weapon a reality.

Two, different variants of Stuxnet together succeeded in delaying Iran's nuclear programme by one and a half to two years time.

Three, the whole Stuxnet episode that disrupted Iran's nuclear programme has instilled fear about the prospective danger of cyber weapons in the mindset/ psyche of the world community.

Four, and most important, the Stuxnet episode may have been one of the main reasons for the Iranian political circle to have a rethink and return to the diplomatic table to discuss the nuclear programme with the West.

The Iranian nuclear episode is a clear example of what covert cyber operations are capable of: disturbing and disrupting a state's national security and even leading to a change of balance in international politics.

As mentioned earlier, where global cyber security is concerned, these covert cyber capabilities pose a serious threat, due to their nature being "covertness". While it is claimed by the US and other countries that these covert cyber capabilities are used to conduct network operations like tracking, detecting and identifying prospective terrorists and their activities in the cyber world, the possibility of these invisible and 'capability-disabling' weapons targeting an individual or a particular group of people or even a state, cannot be denied. Such capability poses a grave danger to cyber freedom and virtual existence for any individual in the domain as well a serious threat to the national security of any targeted nation. This fear is a compelling factor for the common users to lean towards more secretive and clandestine means of operations in the cyber domain, like using TOR networks for everyday browsing in order to hide their location and identity, fearing the consequence of being targeted. Also, many states desire to acquire such covert cyber capabilities so as to be able to participate in the ongoing game of 'supremacy' and have the ability to take revenge, if need be, on another state. If this situation continues, the deep web would go deeper and the cyber 'under' world would expand more rapidly which would only increase the complexities that already exist in this highly technical realm. This complexity in the virtual world will not only have a spillover effect into the physical world but also have its own negative repercussions on the political, economic, social and other activities of the real world.