---

15 June 2013. Matthew Aid, Inside the NSA: Peeling Back the Curtain:

http://www.independent.co.uk/news/world/americas/inside-the-nsa-peeling-back-the-curtain-on-americas-intelligence-agency-8658016.html

12 June 2013

NSA Office of Tailored Access Operations

Matthew Aid Website: http://www.matthewaid.com/

Source: Foreign Policy via South China Post
http://www.scmp.com/news/china/article/1259175/inside-nsas-ultra-secret-china-hacking-group

Inside the NSA's ultra-secret China hacking group

Wednesday, 12 June, 2013, 4:19pm

Mathew M. Aid

Last weekend, US President Barack Obama sat down for a series of meetings with China's newly appointed leader, Xi Jinping. We know that the two leaders spoke at length about the topic du jour – cyber-espionage – a subject that has long frustrated officials in Washington and is now front and centre with the revelations of sweeping US data mining. The media has focused at length on China's aggressive attempts to electronically steal US military and commercial secrets, but Xi pushed back at the "shirt-sleeves" summit, noting that China, too, was the recipient of cyber-espionage. But what Obama probably neglected to mention is that he has his own hacker army, and it has burrowed its way deep, deep into China's networks.

When the agenda for the meeting at the Sunnylands estate outside Palm Springs, California, was agreed to several months ago, both parties agreed that it would be a nice opportunity for President Xi, who assumed his post in March, to discuss a wide range of security and economic issues of concern to both countries. According to diplomatic sources, the issue of cyber-security was not one of the key topics to be discussed at the summit. Sino-American economic relations, climate change, and the growing threat posed by North Korea were supposed to dominate the discussions.

Then, two weeks ago, White House officials leaked to the press that Obama intended to raise privately with Xi the highly contentious issue of China's widespread use of computer hacking to steal US government, military, and commercial secrets. According to a Chinese diplomat in Washington who spoke in confidence, Beijing was furious about the sudden elevation of cyber-security and Chinese espionage on the meeting's agenda. According to a diplomatic source in Washington, the Chinese government was even angrier that the White House leaked the new agenda item to the press before Washington bothered to tell Beijing about it.

Last week's revelations about the National Security Agency's Prism and Verizon metadata collection only add fuel to Beijing's position.

So the Chinese began to hit back. Senior Chinese officials have publicly accused the US government of hypocrisy and have alleged that Washington is also actively engaged in cyber-espionage. When the latest allegation of Chinese cyber-espionage was levelled in late May in a front-page Washington

Post article, which alleged that hackers employed by the Chinese military had stolen the blueprints of over three dozen American weapons systems, the Chinese government's top internet official, Huang Chengqing, shot back that Beijing possessed "mountains of data" showing that the United States has engaged in widespread hacking designed to steal Chinese government secrets. Last week's revelations about the National Security Agency's Prism and Verizon metadata collection from a 29-year-old former CIA undercover operative named Edward J. Snowden, who is now living in Hong Kong, only add fuel to Beijing's position.

But Washington never publicly responded to Huang's allegation, and nobody in the US media seems to have bothered to ask the White House if there is a modicum of truth to the Chinese charges.

It turns out that the Chinese government's allegations are essentially correct. According to a number of confidential sources, a highly secretive unit of the National Security Agency (NSA), the US government's huge electronic eavesdropping organisation, called the Office of Tailored Access Operations (TAO) has successfully penetrated Chinese computer and telecommunications systems for almost 15 years, generating some of the best and most reliable intelligence information about what is going on inside the People's Republic of China.

Hidden away inside the massive NSA headquarters complex at Fort Meade, Maryland, in a large suite of offices segregated from the rest of the agency, TAO is a mystery to many NSA employees. Relatively few NSA officials have complete access to information about TAO because of the extraordinary sensitivity of its operations, and it requires a special security clearance to gain access to the unit's work spaces inside the NSA operations complex. The door leading to its ultramodern operations centre is protected by armed guards, an imposing steel door that can only be

entered by entering the correct six-digit code into a keypad, and a retinal scanner to ensure that only those individuals specially cleared for access get through the door.

According to former NSA officials interviewed for this article, TAO's mission is simple. It collects intelligence information on foreign targets by surreptitiously hacking into their computers and telecommunications systems, cracking passwords, compromising the computer security systems protecting the targeted computer, stealing the data stored on computer hard drives, and then copying all the messages and data traffic passing within the targeted e-mail and text-messaging systems. The technical term of art used by NSA to describe these operations is computer network exploitation (CNE).

TAO has successfully penetrated Chinese computer and telecom systems for almost 15 years

TAO is also responsible for developing the information that would allow the United States to destroy or damage foreign computer and telecommunications systems with a cyberattack if so directed by the president. The organisation responsible for conducting such a cyberattack is US Cyber Command (Cybercom), whose headquarters is located at Fort Meade and whose chief is the director of the NSA, Gen. Keith Alexander.

Commanded since April of this year by Robert Joyce, who formerly was the deputy director of the NSA's Information Assurance Directorate (responsible for protecting the US government's communications and computer systems), TAO, sources say, is now the largest and arguably the most important component of the NSA's huge Signal Intelligence (SIGINT) Directorate, consisting of over 1,000 military and civilian computer hackers, intelligence analysts, targeting specialists, computer hardware and software designers, and electrical engineers.

The sanctum sanctorum of TAO is its ultra-modern operations centre at Fort Meade called the Remote Operations Center (ROC), which is where the unit's 600 or so military and civilian computer hackers (they themselves CNE operators) work in rotating shifts 24 hours a day, seven days a week.

These operators spend their days (or nights) searching the ether for computers systems and supporting telecommunications networks being used by, for example, foreign terrorists to pass messages to their members or sympathisers. Once these computers have been identified and located, the computer hackers working in the ROC break into the targeted computer systems electronically using special software designed by TAO's own corps of software designers and engineers specifically for this purpose, download the contents of the computers' hard drives, and place software implants or other devices called "buggies" inside the computers' operating systems, which allows TAO intercept operators at Fort Meade to continuously monitor the e-mail and/or text-messaging traffic coming in and out of the computers or hand-held devices.

TAO's work would not be possible without the team of gifted computer scientists and software engineers belonging to the Data Network Technologies Branch, who develop the sophisticated computer software that allows the unit's operators to perform their intelligence collection mission. A separate unit within TAO called the Telecommunications Network Technologies Branch (TNT) develops the techniques that allow TAO's hackers to covertly gain access to targeted computer systems and telecommunications networks without being detected. Meanwhile, TAO's Mission Infrastructure Technologies Branch develops and builds the sensitive computer and telecommunications monitoring hardware and support infrastructure that keeps the effort up and running.

TAO even has its own small clandestine intelligence-gathering unit called the Access Technologies Operations Branch, which includes personnel seconded by the CIA and the FBI, who perform what are described as "off-net operations", which is a polite way of saying that they arrange for CIA agents to surreptitiously plant eavesdropping devices on computers and/or telecommunications systems overseas so that TAO's hackers can remotely access them from Fort Meade.

It is important to note that TAO is not supposed to work against domestic targets in the United States or its possessions. This is the responsibility of the FBI, which is the sole US intelligence agency chartered for domestic telecommunications surveillance. But in light of information about wider NSA snooping, one has to prudently be concerned about whether TAO is able to perform its mission of collecting foreign intelligence without accessing communications originating in or transiting through the United States.

Since its creation in 1997, TAO has garnered a reputation for producing some of the best intelligence available to the US intelligence community not only about China, but also on foreign terrorist groups, espionage activities being conducted against the United States by foreign governments, ballistic missile and weapons of mass destruction developments around the globe, and the latest political, military, and economic developments around the globe.

TAO's operators [are] tapping into thousands of foreign computer systems and accessing password-protected computer hard drives and e-mails of targets around the world.

According to a former NSA official, by 2007 TAO's 600 intercept operators were secretly tapping into thousands of foreign computer systems and accessing password-protected computer hard drives and e-mails of targets around the world. As detailed in my 2009 history of NSA, The Secret Sentry, this highly classified intercept programme, known at the time as Stumpcursor, proved to be critically important during the US Army's 2007 "surge" in Iraq, where it was credited with single-handedly identifying and locating over 100 Iraqi and al Qaeda insurgent cells in and around Baghdad. That same year, sources report that TAO was given an award for producing particularly important intelligence information about whether Iran was trying to build an atomic bomb.

By the time Obama became president of the United States in January 2009, TAO had become something akin to the wunderkind of the US intelligence community. "It's become an industry unto itself," a former NSA official said of TAO at the time. "They go places and get things that nobody else in the IC [intelligence community] can."

Given the nature and extraordinary political sensitivity of its work, it will come as no surprise that TAO has always been, and remains, extraordinarily publicity shy. Everything about TAO is classified top secret codeword, even within the hyper-secretive NSA. Its name has appeared in print only a few times over the past decade, and the handful of reporters who have dared inquire about it have been politely but very firmly warned by senior US

intelligence officials not to describe its work for fear that it might compromise its ongoing efforts. According to a senior US defence official who is familiar with TAO's work, "The agency believes that the less people know about them [TAO] the better."

The word among NSA officials is that if you want to get promoted or recognised, get a transfer to TAO as soon as you can. The current head of the NSA's SIGINT Directorate, Teresa Shea, 54, got her current job in large part because of the work she did as chief of TAO in the years after the 9/11 terrorist attacks, when the unit earned plaudits for its ability to collect extremely hard-to-come-by information during the latter part of George W. Bush's administration. We do not know what the information was, but sources suggest that it must have been pretty important to propel Shea to her position today. But according to a recently retired NSA official, TAO "is the place to be right now".

There's no question that TAO has continued to grow in size and importance since Obama took office in 2009, which is indicative of its outsized role. In recent years, TAO's collection operations have expanded from Fort Meade to some of the agency's most important listening posts in the United States. There are now mini-TAO units operating at the huge NSA SIGINT intercept and processing centres at NSA Hawaii at Wahiawa on the island of Oahu; NSA Georgia at Fort Gordon, Georgia; and NSA Texas at the Medina Annex outside San Antonio, Texas; and within the huge NSA listening post at Buckley Air Force Base outside Denver.

The problem is that TAO has become so large and produces so much valuable intelligence information that it has become virtually impossible to hide it anymore. The Chinese government is certainly aware of TAO's activities. The "mountains of data" statement by China's top internet official, Huang Chengqing, is clearly an implied threat by Beijing to release this data. Thus it is unlikely that President Obama pressed President Xi too hard at the Sunnydale summit on the question of China's cyber-espionage activities. As any high-stakes poker player knows, you can only press your luck so far when the guy on the other side of the table knows what cards you have in your hand.

Mathew M. Aid is the author of Intel Wars: The Secret History of the Fight Against Terror and The Secret Sentry: The Untold History of the National Security Agency, and is co-editor with Cees Wiebes of Secrets of Signals Intelligence During the Cold War and Beyond.