افغانستان آزاد ـ آزاد افغانستان

AA-AA

چو کشور نباشد تن من مبـــاد   بدین بوم وبر زنده یک تن مــباد
همه سر به سر تن به کشتن دهیم   از آن به که کشور به دشمن دهیم

www.afgazad.com	afgazad@gmail.com
European Languages	زبان های اروپائی

http://www.strategic-culture.org/news/2014/05/18/washington-spies-on-nato-other-allies.html

Washington Spies on NATO; Other Allies

Wayne MADSEN

5/18/2014

As the United States marshals its eastern European NATO allies to confront Russia and the independence governments and movements in the Donbass and Odessa regions of Ukraine, the latest revelations of National Security Agency whistleblower Edward Snowden confirm that the then-U.S. ambassador to the United Nations Susan Rice ordered NSA to spy on the Washington embassies and New York UN delegations of a number of U.S. allies, including NATO members…

Although Bulgaria and Slovakia are NATO members, their embassies and UN delegations came under massive NSA surveillance.

Bugging devices were placed by NSA in the computer systems of the Bulgarian embassy in Washington, DC. Computer «implants» are inserted in a classified program known as HIGHLANDS. The cover name for the NSA operation against Bulgaria and its diplomats was known as MERCED. Similarly, HIGHLANDS bugs transmitted computer data from computers of the Slovak embassy in Washington, in addition to the transmission of computer screen images by an operation codenamed VAGRANT. The Slovak bugging operation was codenamed FLEMING.

One aspirant NATO member, Georgia, saw its Washington embassy bugged by both

HIGHLANDS and VAGRANT operations. The project targeting the Georgian embassy was codenamed NAVARRO.

Ambassador Rice, who is now President Obama's National Security Adviser, is quoted in a TOP SECRET/Not Releasable to Foreign Nationals (NOFORN) document as saying the bugging of the UN Security Council members' diplomatic offices, as well as the office of UN Secretary General Ban Ki-moon, «helped me to know when other Permreps [Permanent Representatives] were telling the truth... gave us an upper hand in negotiations [on a UN resolution on UN sanctions on Iran]... and provided us information on various countries' 'red lines.'»

Essentially, the Obama administration, while publicly lauding U.S. allies, in secret decided to second-guess them by spying on their ambassadors and senior diplomats.

Other NSA programs are used to collect different types of signals from the targeted computers and data networks within embassies and UN missions. These include MAGNETIC, the collection of magnetic emanations from data equipment; MINERALIZE, the collection of data from local area network (LAN) equipment; OCEAN, an acronym for Optical Collection System for Raster-Based Computer Screens; LIFESAVER, the imaging of computer hard drives; GENIE, a multi-stage collection operation involving the «jumping» of the airgap between physically unconnected systems; BLACKHEART, the collection of data from a Federal Bureau of Investigation implant; DROPMIRE, the passive collection of emanations from an antenna and laser printer collection; CUSTOMS, the collection of computer data by Customs agents at border crossings; DEWSWEEPER, the collection of data from a Universal Serial Bus connected to a wireless bridge; and RADON, the use of Ethernet taps to inject packets to enable bi-directional sniffing of «denied», meaning secured, networks.

Implants are inserted by NSA into targeted computer systems and network devices through what the NSA calls «supply-chain interdiction». Equipment is intercepted between the manufacturer and the end-user. At a secret facility called a «load station», devices called «beacons» are inserted clandestinely into a device's hardware. These pre-positioned access points permit later access by NSA into «hard target» networks around the world.

NSA names its strategic partners in its «collect-it-all», codenamed ASPHALT operations, around the world. These are AT&T, EDS, Qwest, H-P, Motorola, Cisco, Qualcomm, Oracle, Intel, IBM, Microsoft, and Verizon. In all, over 80 «major global corporations» support NSA's worldwide collection efforts. With corporate cooperation, NSA captures Internet data from seven «international choke point» access sites in the continental United States. Their cover names are Breckenridge, Tahoe, and Sun Valley on the U.S. West Coast; Whistler in the South; and Killington, Coppermountain, and Maverick on the East Coast.

Targeted network beacon implants have their own codenames. They include HOMEMAKER, DOGHUT, QUARTERPOUNDER, QUEENSLAND, SCALLION, SPORTCOAST, CLEVERDEVICE, TITAN POINTE, BIRCHWOOD, MAYTAG, EAGLE, EDEN, and SUBSTRATUM.

NSA deputized Poland as an official «Third Party» signals intelligence (SIGINT) partner of the so-called FIVE EYES intelligence alliance of the United States, United Kingdom, Canada, Australia, and New Zealand. According to one NSA memorandum, Poland has forwarded to NSA since May 2009 commercial dial number recognition (DNR) metadata collected within Poland by the SIGINT department of the Polish government. The SIGINT is processed by an intelligence system code named ORANGECRUSH, which is part of a larger foreign SIGINT collection system called OAKSTAR. However, according to the NSA memorandum, Poland was not to be told about ORANGECRUSH. For the Poles, NSA determined that the system would only be known by the code name BUFFALOGREEN. The cloak-and-dagger code name game with Poland indicates that the NSA does not fully trust Poland as a Third Party SIGINT partner.

However, when it comes to supporting NATO's operations directed against Russia over Ukraine, Moldova, and Kaliningrad, the United States demands full Polish cooperation and support. ORANGECRUSH operations, although involving Poland, was only to include intelligence authorized to be shared with Poland under the BUFFALOGREEN program within the NSA's Special Source Operations division. Cooperating in the Polish SIGINT program are the NSA Commercial Solutions Center (NCSC), the NSA's Foreign Affairs Division, an a commercial telecommunications partner. The Polish SIGINT efforts conducted jointly with NSA involve the targeting of the «Afghan National Army, Middle East, limited African continent, and European communications».

Polish SIGINT products are sent to NSA's Second Parties of the United Kingdom, Canada, Australia, and New Zealand via a system code named TICKETWINDOW. The authorization for the NSA-Polish intelligence sharing is posted on a notification system called STINGRAY.

Computer Network Exploitation (CNE) operations directed against the Internet are conducted from U.S. diplomatic compounds in Prague, Budapest, Sofia, Zagreb, Tirana, Sarajevo, and Pristina. In addition to Poland, Hungary, and the Czech Republic, newly revealed NSA documents name Croatia, Macedonia, and Romania as official Third Party partners of the NSA.

NSA's eastern European partners are also supporting new methods for NSA and its partners, including Britain's Government Communications Headquarters (GCHQ) to intercept and store communications from GSM (Global System for Mobile Communications) and GPRS (General packet radio service (GPRS) from networks installed on commercial aircraft. For example, one new classified NSA slide released in Glenn Greenwald's new book, «No Place to Hide», details Russian Aeroflot airlines as an NSA target of surveillance. The NSA/GCHQ airline surveillance system is codenamed THIEVING MAGPIE. Another slide identifies a classified system known as SOUTHWINDS that has the capability to track airline passenger communications globally. Initially, THIEVING MAGPIE was able to track the personal identification numbers (PINs) and email addresses of Blackberry devices. A parallel phone tracking system targeting airlines is codenamed HOMING PIGEON.

One NSA slide is amazingly honest in what it describes as America's gambit to control the Internet through the immense powers being amassed by NSA and its allies. The slide states: «Let's be blunt. The Western world (especially the U.S.) gained influence and made a lot of money via the drafting of earlier standards. The U.S. was the major player in shaping today's Internet. This resulted in pervasive exportation of American culture as well as technology. It also resulted in a lot of money being made by U.S. entities».

And there, in a nutshell, is the reason for America’s steady expansion of its military and political presence deep into central and eastern Europe via NATO, the World Bank, and the International Monetary Fund. NSA’s deputizing of eastern European NATO nations as NSA Third Party surveillance partners has nothing to do with U.S. or European «national security». It has everything to do with maintaining America’s control of the Internet to push its cultural and economic influence around the world. As the most recent NSA disclosures reveal, NSA is more than happy to embrace and, at the same time, spy on its new European allies to protect the almighty American dollar and those who obscenely profit from it.