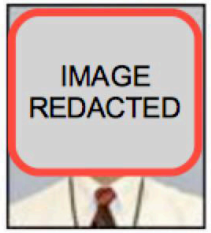
TOP SECRET//COMINT//NOFORN

June 2010

(U) Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets

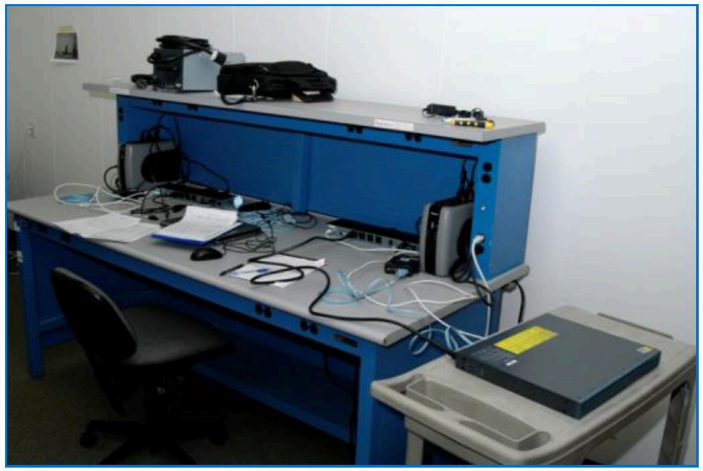
By: (U//FOUO) NAME REDACTED, Chief, Access and Target Development (S3261)



(TS//SI//NF) Not all SIGINT tradecraft involves accessing signals and networks from thousands of miles away… In fact, sometimes it is very hands-on (literally!). Here's how it works: shipments of computer network devices (servers, routers, etc.) being delivered to our targets throughout the world are ***intercepted***. Next, they are ***redirected to a secret location*** where Tailored Access Operations/Access Operations (AO – S326) employees, with the support of the Remote Operations Center (S321), enable the ***installation of beacon implants*** directly into our targets' electronic devices. These devices are then re-packaged and ***placed back into transit*** to the original destination. All of this happens with the support of Intelligence Community partners and the technical wizards in TAO.

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.





(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

(TS//SI//NF) In one recent case, after several months a beacon implanted through supply-chain interdiction called back to the NSA covert infrastructure. This call back provided us access to further exploit the device and survey the network.