# Google Cloud is Busted by Russians and Chinese and Revealed To Be Security-Proof

By Stephen Bryen

Perhaps it is a good thing that Google employees convinced their management not to do business with the Pentagon, thereby pulling out of participating in a $10 billion cloud computing contract called JEDI (Joint Enterprise Defense Infrastructure).

On November 12th, Google's services were hit by a massive hack allegedly carried out by Russians, Chinese, and Nigerians. The hack redirected all of Google's search, business, and cloud computing operations through servers run in these countries using a hack called the Border Gateway Protocol (BGP). This gave the hackers unprecedented access to extremely sensitive information on users and direct access to any data that was not independently encrypted (one presumes that the typical computer network security protocols were automatically compromised by being run through servers that did not belong to Google). Even more critically, it gave the three countries complete control over all of Google's operations and data. While the hack only lasted about an hour and a half, it demonstrated in clear terms just how vulnerable computer networks are and showed that the critical infrastructure could have been taken down, had the hackers wanted to do so.

For the record, the Google Cloud and Google's G-Suite business services have good security practices, and the Google Cloud in particular has some security features that are quite advanced. But that did not stop the BGP

hack, because BGP hacks exploit the IP addresses and information routing addresses that are built into the modern internet. Worse yet, computer experts say that current technology can't stop a BGP hack.

The Pentagon with its JEDI contract wants to migrate its computer networks to the cloud, and just not any old cloud but a cloud system run by private enterprise that is shared with the public. While the Pentagon doubtlessly will use some form of encryption for its cloud operations, it cannot protect the exploitation of its networks if exposed on a public network. Moreover, the Pentagon has yet to explain how it will back up the system if it fails for any reason.

The Pentagon points out that the CIA already is on the cloud using Amazon's cloud services. In fact, the Pentagon wanted to use the same vendor, but ran into a buzzsaw of complaints about the lack of competition. While the Pentagon closed the bids for the JEDI contract on October 12th, the complaints are still rolling in and two major vendors, Oracle and IBM, are protesting the JEDI contract through the Government Accountability Office. Where this will end up is still anyone's guess.

But the hack of Google should be sobering enough that deciding to go with the cloud approach really needs a serious security scrub. Beyond that, the entire computer network environment used by DOD should be assessed because it is dangerous and highly failure prone and is costing billions in lost technology and compromised information. The Pentagon has set up a special Task Force to try and address technology losses.

The core issue is what the networks are made of today. Most of the computer equipment including network routers and ancillary devices such as printers and web cameras, are made in China. All of them are inherently non-secure because of where they come from and because the U.S. government, including the Pentagon and the military services, buy equioment without any security vetting. No equipment is tested for security and, for the most part the buying process is based on published specifications provided by the manufacturing company or distributor. Even equipment that looks American is usually stuffed with parts that come from abroad. No one can tell you what's inside the box.

China has been known to plant hardware, firmware, and software in devices such as computer motherboards or smart phones. Given that more than 70 percent of all computer hardware either is Chinese in origin or contains Chinese origin components, no one can trust present-day networks. Harvesting information is, therefore quite easy for Chinese spies and China has used what it has stolen to build everything from stealth fighter planes to modern missiles.

If the existing network is not trustworthy, the new cloud computing environment just expands the problem from a specific target to the broader network itself, meaning that command and control systems and communications become instantly vulnerable. Even if there are backup systems, the sheer volume of a cloud computing crash means that recovery could be very difficult, perhaps not even possible.

One can add to the risk profile the question of backup systems. Pentagon networks have grown up over many years, have been modified as new technology and new demands require more data handling and better information management, and because they are complex often are a mix of old and new equipment, compounding vulnerabilities and the challenge of keeping them in good operating shape. When the cloud becomes a

replacement, keeping the old system as a backup is a major challenge, if it can be done at all. More likely is that the old system will progressively get scrapped in favor of the "cheaper" cloud, replacing a largely distributed system with a centralized target for foreign adversaries.

The Pentagon buys a lot of military hardware based on a process of writing specifications and measuring performance, with milestones and requirements needing to be met to move onto the next acquisition stage. While the current system is expensive and burdensome, generally it produces good results (although there are still failures). But when it comes to electronics and computers, mostly the acquisition process is replaced by buying equipment "off the shelf." This is called COTS (commercial off the shelf) hardware and software. COTS has got the Pentagon, the military, and its many contractors into a lot of trouble because of the ease of foreign hacking of data. When you transfer most of these vulnerabilities to the cloud you centralize the security vulnerability and expose the entire system to potential compromise or collapse.

Google will recover from the Chinese, Russian, and Nigerian redirect of their services. Probably they won't even be able to do much of an assessment of what was compromised or lost, so they will plow ahead and put the redirect of their system on the back burner. When the Pentagon is up on the cloud, the outcome will be a lot worse.