## Economic War Room - CYBER Status Update:

Thieves are consistently using cyber technology to anonymously steal your personal identity, money, credit card, and banking accounts. **Hacking devices and tools are available to any criminal online**. Many of these devices are preprogrammed so even amateurs can use them. Even major corporations/businesses with sophisticated IT teams are at risk. Recently, GE's advanced secrets for military gas turbine helicopter engines were allegedly stolen through an employee. The Chinese-American employee allegedly sent the secret plans to China through embedded pictures online.

## Your Mission:

To understand the cyber threats in your everyday life, at retail, and in the business environment. Also, to understand precautions and technology solutions that will help you secure your information.

## There are 3 tools being used to access corporate data and your information:

1. Hardware – Designed to collect your data
2. Cyber – Online hacks
3. Physical theft of Intellectual property. Hire someone to go in, get the data, and send it out.

HARDWARE

CYBER

HUMAN

# (OSINT) – Open Sourced Intelligence Briefing

Kevin Freeman and Kevin Henson, CTO Allied Special Operations Group (ASOG), discuss cyber threats.

## 1. Another Recent China Cyber theft:

A. China is consistently using cyber, big data, and artificial intelligence to steal U.S. intellectual property.

B. There is an education agenda- PLA plan is to send Chinese students to learn and bring things back to their handlers.

C. All Chinese-national students may be required to work for the Chinese government/military. Approximately 10 percent of total Chinese-national college students in the U.S. work directly for PLA intelligence service. In computer fields 80 to 85 percent of those students enrolled in the US may be taking that data directly back to Chinese handlers.

D. As part of their assignment here, China also encourage students to get jobs in the U.S. to seek and send further information.

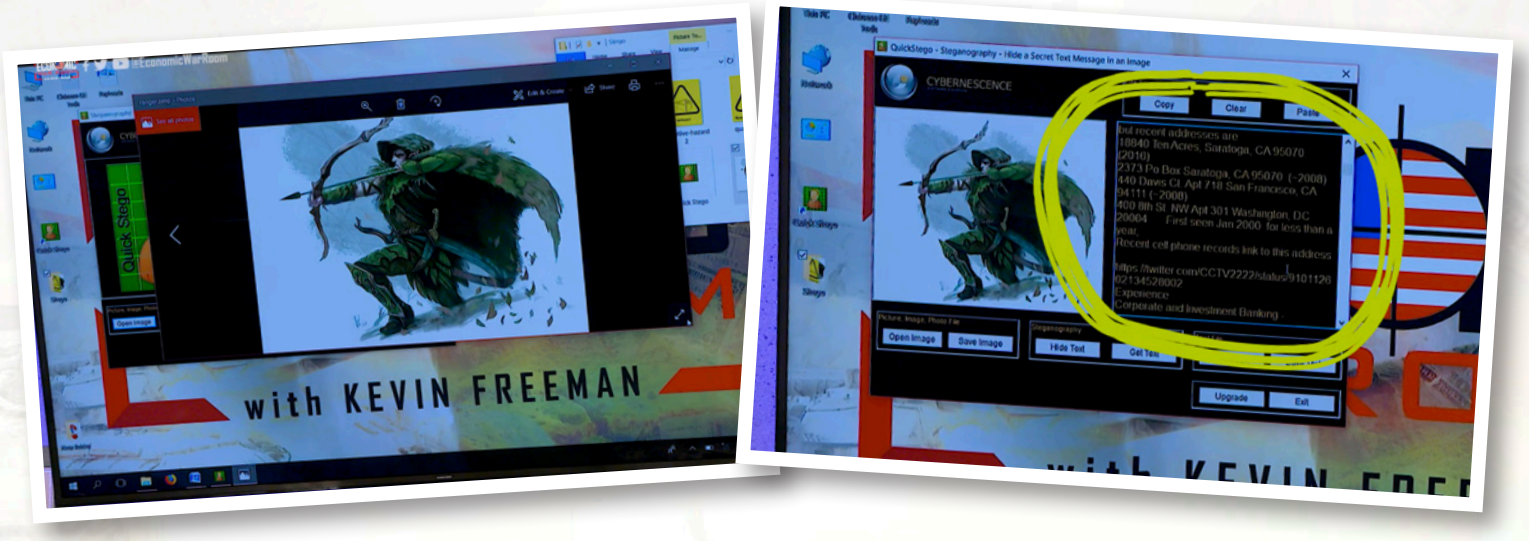
E. Recently, a Chinese American engineer employed by GE, was accused of stealing secrets from GE gas turbine technology and sending to China by hiding the data in family photos.

F. The engineer had a handbook of all the technology the Chinese want from the U.S. and allegedly has been sending data back through pictures.

G. Chinese military has stolen GE/US military technology to upgrade their helicopters so they could compete in a military engagement with us.

H. China is conducting military espionage masked as commercial espionage.

I. Steganography and a tool like QuickStego lets you hide data in pictures. In fact, you could hide a software program in a picture. Mailing a picture of your family to China or somewhere else? There might be more there than you can see! If data is encrypted and then put in pictures it will not be found.




J. The Chinese are looking for how to gain advantage in both the short term and long term. Rather than develop their own technology for 15 to 20 years they have a track record of stealing U.S. technology to build their own attack helicopters.


Look familiar?

**"One Chinese definition of peace is the extension of conflict by political and economic means."**

**2. Public Wi-Fi and other personal cyber risk?** **The following are examples of hacking gadgets available for $100 to $300. These are available to buy online, and they can cost you or your company a fortune.**


A. **LAN Turtle** - Plug it in and it can easily tie into your network. Cleaning crews might plug in a simple device and your computer is compromised. Contractors installing your servers can plug this in and access your servers from anywhere in the world. This is a commercial item that can be bought on online for $100.

B. **Regular USB device:** Plug into a computer and connect through guest account and nobody notices. Again, this is available online through hack shops.

C. **Modified USB device**: Plugs in to any computer, it launches and starts a program. Ducky tool launches and types a script with no help, grabs browser history, looks at your files, takes your passwords, and sets up a persistent reverse shell. It opens the computer so anyone can access overseas. Download the payload you want put it in these devices and it automatically gets it. Plug this in and take control of any computer.


D. **Bash Bunny**: One of the most dangerous cyber tools out there. An easy way to compromise a system. A multi-function USB attack with a multi-function attack switch. If armed works like USB, and runs script like ducky tool, but it has an entire computer inside. This is a completely programmable hacking tool with all kinds of prewritten hacks, making it easy to perform an attack or penetrate a network. It goes from plug to clone in less than 7 seconds.

E. **Pineapple NANO**: A small device that clones the identity of the nearest Wi-Fi hot spot. With this device operating, you think you are logging on to Starbucks or any other public Wi-Fi. The Nano instead routes all traffic through this device so they can take everything from you. Even going through a cell network can be vulnerable.

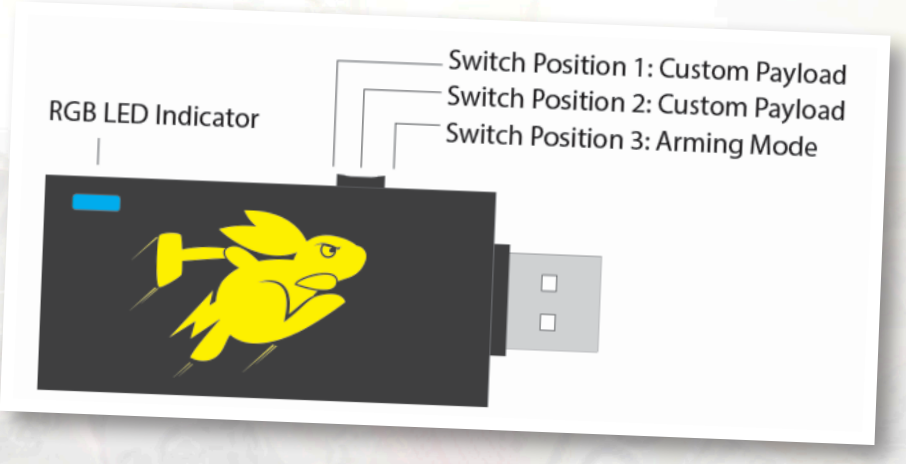
F. **A Network Tap** - Another USB device. It can hide behind a wall or a desk and you will never know it was installed. Criminals could go into the mall, plug this into a cash register under the counter, and then the hack begins. Get all customer and retailer data, transactions globally, and access financial data. This USB device can protect and encrypt your information, or flip the switch and it will steal information.

## Why You Should Care:

- **There is an economic risk to you.**
- **There is a national security and military risk.**
- **There is a lifestyle risk. Stolen identities and information can wreak havoc on your life.**
- **Stolen proprietary information could bankrupt business, hurt jobs, and destroy productivity.**

**"The USB Bash Bunny is possibly the most dangerous device in cyber hacking."**

– Kevin Henson



# Economic Patriot Action Plan

As an economic patriot, you can make a difference.

**Step 1: Take care of your personal cyber risk:**

A. Do not leave your computer or smart device lying around. Take it home or lock it in your desk.

B. Anyone plugging into your USB port can create problems. Do not share USB drives unless you are completely sure of the source.

C. Turn off plug and play options on your computer, so some of these hack devices are not as easy to run. Plug and play is convenient, but reduces the security of your computer significantly.

D. If you are part of a business or corporation, you should hire a reputable company to try and hack you, understand vulnerabilities, and develop a plan to reduce risk. Note: If you represent a major corporation, consider contacting a company like Allied Special Operations Group (ASOG) to conduct a cyber audit. https://alliedspecialops.us

E. Have a complex password on your computers (according to conventional advice—which is still good – at least 16 characters with Upper and Lower Case and special character like #$_% and so on), but understand there are easy ways to hack around that still.

F. Keep your computer software patches up to date.

G. Get CCleaner or comparable software for your Mac or PC. Look to ensure you are not running a lot of services on the background of the machine. CCleaner will allow you to look at what programs are running in the background. Consider deleting something that is running you did not install, or you are not using. Be sure, however, to not delete critical system files.

H. Check programs and if you are not sure what it is, consider getting rid of it.

I. Installing a firewall is a very good idea. Look for Firewall appliances like pfSense security gateway that can be use as a firewall between cable modem and the computer. For more information on how to install look for Eli the Computer Guy on You Tube.

J. Do not let teenage children use your work computer or home computer with sensitive financial or personal information. File share for music and movies can have a lot of malware.

**Step 2. On a National Security basis**, we need to recognize that espionage takes place on three (3) levels. We must not be blind to this truth due to political correctness. Background, security checks, and policies should be reviewed as it relates to protecting America's intellectual property, National Security and Economic Infrastructure:

**Step 3**. Websites that sell the Cyber hacking technology devices and how to use them should be carefully monitored. Until, recently the FBI was not aware they existed and sites are still going. Tutorials are also available on You Tube.

WE are in a cyber economic war.

**What we see as a MARKETPLACE**
**our enemies view as a BATTLESPACE™**

**Step 4:** Share this battle plan and get others to subscribe:

A. Get others to sign up and review our weekly Economic War Room battle plans. Each of these will address critical solutions to the threats highlighted on this briefing.

B. Subscribe to our weekly Economic War Room show on TheBlaze at EconomicWarRoom.com.

C. Follow, like, comment and share on Facebook and Twitter.

***Thank you for accepting this mission. Together, we will make a difference!***

SHAREABLE THOUGHTS: The Chinese moved forward 50 years in technology in 10 years, through the theft of technology.

The Pentagon's answer to stopping hacking was to glue shut the USB plug on their computers.

# The EWR Collection Deck From Kevin Freeman

## Allied Special Operations Group

https://alliedspecialops.us

## Hacker Tools in the Wild

How U.S. surveillance technology is propping up authoritarian regimes
https://www.washingtonpost.com/outlook/2019/01/17/how-us-surveillance-technology-is-propping-up-authoritarian-regimes/

Top Ten Tools For Cybersecurity Pros (and Black Hat Hackers)
https://www.cybersecuritymastersdegree.org/2017/11/top-ten-tools-for-cybersecurity-pros-and-black-hat-hackers/

Top 15 Ethical Hacking Tools Used by Infosec Professionals
https://securitytrails.com/blog/top-15-ethical-hacking-tools-used-by-infosec-professionals

10 Hacking Tools You Think Would be Illegal But are for Sale Online
https://www.inverse.com/article/38612-hacking-tools-legal-available

## Chinese Spying

Tampered Chinese Ethernet port used to hack 'major US telecom,' says Bloomberg report
https://www.theverge.com/2018/10/9/17955848/supermicro-telecom-server-hack-apple-amazon

Chinese spy charged with trying to steal US aviation trade secrets
https://www.cnbc.com/2018/10/10/chinese-spy-charged-with-trying-to-steal-us-aviation-trade-secrets.html

Court papers detail alleged Chinese espionage scheme
https://www.flightglobal.com/news/articles/court-papers-detail-alleged-chinese-espionage-scheme-452613/

How much has the US lost from China's IP theft?
https://money.cnn.com/2018/03/23/technology/china-us-trump-tariffs-ip-theft/index.html

How China's rampant intellectual property theft, long overlooked by US, sparked trade war
https://www.scmp.com/magazines/post-magazine/long-reads/article/2170132/how-chinas-rampant-intellectual-property-theft

## Ways to Protect Your Computer from Hackers

How to keep your computer safe from hackers and cyber attacks
https://www.mirror.co.uk/tech/computer-safe-cyber-attack-ransomware-11900249

Seven easy tips to protect your PC from hackers and malware
https://home.bt.com/tech-gadgets/computing/tips-protect-your-pc-hackers-malware-11363942012065

The risks of public Wi-Fi
https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html

Why you should never, ever connect to public WiFi
https://www.csoonline.com/article/3246984/wi-fi/why-you-should-never-ever-connect-to-public-wifi.html

How to Do a Cyber Security Audit
http://www.nccdata.com/blog/how-to-do-a-cyber-security-audit/