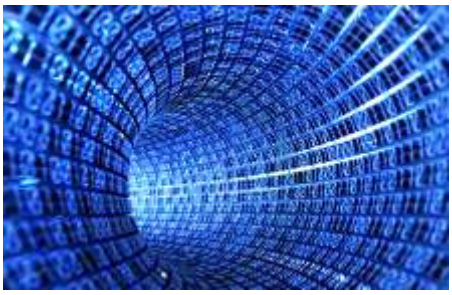
“Asymmetric Cyber Warfare”: Superpowers Accuse Each Other

by zed - wsws *Thursday, May 9 2013, 1:00pm*
international / prose / post

> "*The greatest victory is had by creating the circumstances which induce the opponent to defeat itself*" -- *Anon hacker.*
>
> It should be understood from the outset that the activities of Uber or elite hackers are untraceable -- "Uber," used in a cyber context actually means untraceable or invisible. Furthermore, it is child's play to camouflage an attack by directing its source to another party.



It makes naught of recent US accusations that China is responsible for numerous cyber attacks that occur on the net.

Consider for a moment an elite group of hackers from say Eastern Europe that are right royally pissed off that the US has violently intervened in their nations and in some cases overtly occupies (bases) sovereign States. Consider also that China pledged allegiance to some of these States but did nothing when the US and NATO conducted overt conventional military attacks. It places the US and China in the same treacherous category as far as these elite groups are concerned.

In order to balance the situation elite groups would create circumstances that would pitch these two nations against each other, as seems to be occurring as I write.

If we mention that representatives of these elite groups warned both nations that they would pay for their treachery, a foggy scenario becomes clear.

Indeed, no-one knows the identities or location of these Uber hackers, least of all me; but I do know what I was told would happen some years past and now I witness it happening today. I refer to a seminal paper written by 'nano' which basically outlined the new warfare of the 21st century and ridiculed the conventional warfare the civilian killing US brutishly specialises in.

A recent article highlights the digital incompetence of the US and the security specialists that have 'traced' attacks to China, 'spoofing' (as its known) or camouflaging attacks has been a REALITY for over 20 years and the level of sophistication reached today virtually ensures that elite attacks are invisible/untraceable or attacks are blamed on others.

Before leaving you to read the article I would mention that I have reason to believe that elite hackers are pitching superpowers against each other for reasons of retribution, specifically for their crimes

against humanity and sovereign States -- both China and the US have appalling records in that regard.

The article makes reference to something that has been kept hidden for some time and that is that satellites of major superpowers have been under massive attack for over a decade; indeed, it is considered the holy grail of hacking to compromise these systems and some claim to have done exactly that but have not yet gained complete control over these systems. However, one could imagine what Uber hackers would be capable of when they do. In the meantime continue accusing each other of attacks, you dumb lame fucks!

> **US Accuses China of Cyber Attacks and Espionage**
> by John Chan
>
> In a marked escalation of Washington's propaganda against China, the US Defence Department has the first time named the Chinese government and the People's Liberation Army (PLA) as being responsible for major cyber attacks on Western corporations and the US government.
>
> The 2013 annual Pentagon report on the Chinese military depicts China as an aggressor threatening global cyber security and regional stability in the Asia-Pacific. The purpose is to justify the ongoing American buildup of naval, air, space and cyberspace warfare capacities against China—all part of the Obama administration's "pivot" to Asia.
>
> The report declared: "The US government continued to be targeted for (cyber) instructions, some of which appear to be attributable directly to the Chinese government and military." The paper claimed that China was using the information it gathered for the purposes of "building a picture of US defence networks, logistics, and related military capabilities that could be exploited during a crisis."
>
> The Pentagon further alleged that the Chinese government was engaged in massive espionage operations to obtain advanced US technology in order to support China's military modernisation.
>
> These accusations provoked angry reactions from Beijing. Chinese foreign ministry spokeswoman Hua Chungying said the Pentagon report "made irresponsible comments about China's normal and justified defence buildup and hyped up the so-called China military threat." She described the accusations of Chinese hacking activity as "groundless criticism and hype" that would "harm bilateral efforts at cooperation and dialogue."
>
> A People's Daily commentary yesterday by Zhong Sheng—a pen name used by the Beijing leadership—said the real "hacking empire" was the United States, which was engaged in "espionage against not only against enemies but allies." It said the US had a "cyber army" of 50,000 personnel, with 2,000 types of "cyber weapons." Moreover, in 2011 Russia and China had proposed an "International Code of Conduct for Information Security" to the UN to prevent a "cyber arms race and war," but the US alone had consistently opposed and blocked it.
>
> A Global Times editorial yesterday advocated that China should respond in kind to the Pentagon accusations. "For instance, if the United States announced the formation of cyber war units, with stopping Chinese cyber attacks as the main justification, then

China should pick a time to announce her own cyber war forces. The Americans should be let known that, it is they who had driven China to build a cyber army."

The issue emerged three months ago, when the New York Times highlighted a study by a US computer security firm Mandiant, which named the PLA's Unit 61398 as the largest source of theft of data from major US corporations and government departments in recent years. As it turned out, the firm provided no concrete evidence to support its claims. (See: "US uses hacking allegations to escalate threats against China")

Nevertheless, President Barack Obama provocatively phoned Chinese President Xi Jinping immediately after Xi was officially inaugurated in March to demand that Beijing stop hacking. Obama's national security adviser, Thomas Donilon, delivered a speech in the same month declaring that American companies were facing "cyber intrusions emanating from China on an unprecedented scale" and that "the international community cannot tolerate such activity from any country."

While making unsubstantiated allegations against China, the Pentagon report passed over Washington's cyber warfare preparations that will be aimed especially against China. In 2010, the White House inaugurated a separate Cyber Command. Obama allocated $13 billion for cyber warfare in fiscal 2014, even as his administration imposed savage cuts on essential social spending.

As in every military field, the US is seeking to maintain or achieve unrivalled supremacy. It is the US that has actually conducted cyber warfare, including during the 1999 bombing of Serbia, when it hacked into and disrupted Serbian air defence systems. In 2010, in a joint operation with Israel, the US implanted a Stuxnet virus to attack the industrial controllers inside gas centrifuges at Iran's Natanz uranium enrichment plant.

Cyber warfare now occupies a central position in the US military doctrine. The Pentagon report pointed to the PLA's increasing dependence on computer networks. It said China saw electronic warfare as a key to countering the US, including via jamming and anti-jamming, using radio, radar, optical, infrared and microwave frequencies, to "suppress or deceive enemy electronic equipment." At the same time, the PLA command structure was now able to share real-time information, meaning it "no longer requires meetings for command decision-making." Without directly spelling it out, the report implied that these military computer networks and electronic systems must be US cyber warfare targets.

Since the 1990s, Chinese military thinkers have written extensively about the centrality of cyber warfare as computer networks became essential economic and military infrastructure. However, China has developed such capacity primarily as part of an "asymmetrical" doctrine to disrupt any military action against China by a superior military force. As the Pentagon paper stated, China had placed an emphasis on "destroying, damaging and interfering with the enemy's reconnaissance and communications satellites" as a component of China's "information blockade" tactics.

The Pentagon report points to the stepping up of US preparations to attack a potential rival that could otherwise challenge aspects of US military supremacy in Asia-Pacific by the end of this decade. The report drew particular attention to new Chinese stealth fighters and nuclear submarines that could provide deterrents against nuclear attack.

A New York Times article in February revealed that a secret legal review drawn up by the Obama administration had concluded that the president “has the broad power to order a pre-emptive [cyber] strike if the United States detects credible evidence of a major digital attack looming from abroad.” In other words, in this sphere of warfare as in every other, the US imperialism is prepared to carry out criminal acts of aggressive to prosecute its interests. China is undoubtedly at the top of the list of targets.

These developments pose grave risks of war. As the Pentagon calculates that its military superiority over China could be eroded in the foreseeable future, the danger is that US imperialism will increasingly consider using its current overwhelming military advantage to confront Beijing. US propaganda that China represents a serious cyber threat forms part of the ideological justification for the war drive.

http://wsws.org/en/articles/2013/05/09/pent-m09.html
