افغانستان آزاد – آزاد افغانستان

AA-AA

چو کشور نباشد تن من مبـــــاد بدین بوم وبر زنده یک تن مــــباد
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://thediplomat.com/2015/04/chinas-growing-cyberwar-capabilities/

China's Growing Cyberwar Capabilities

A recent attack on GitHub highlights China's growing expertise – and aggression – in cyberspace.

By Marcel A. Green
April 13, 2015

With recent news suggesting that the recent massive denial-of-service attacks against online hosting and code-sharing site GitHub was either sponsored or encouraged by Chinese authorities, the spotlight has once again been turned on China's intentions in cyberspace and whether or not its activities pose a threat to worldwide, and especially U.S. cybersecurity.

China is one of the most active nations in cyberspace. Moreover, China has made no secret that President Xi Jinping's "new model of great power relations" policy means that it will not be afraid to challenge the U.S. and the rest of the world in areas it considers a core interest, such as cyberspace.

Much like the U.S., China has devoted substantial money, manpower and resources to developing its cyber capabilities. Chinese cyber capabilities include a mix of dedicated personnel, advanced equipment, and cyberattack methodologies. According to the cybersecurity firm Mandiant, since as early as 2006, the People's Liberation Army (PLA) has been using an elite cyberwarfare unit based in Shanghai to launch hundreds of cyberattacks targeting American interest. The unit, officially known as Unit 61398, operates under the PLA's Second Bureau of the General Staff Department's (GSD) Third Department, which is focused on cyber surveillance and monitoring of foreign electronic communications. Unit 61398 has a staff of "hundreds if not

thousands" of people, trained in advanced network security, digital signal processing, and covert communications who have access extensive "infrastructure of computer systems around the world." Recently the *Taipei Times* reported that Taiwan's National security Bureau (NSB) has identified another unit of the GSD's Third Department that is involved in cyber-activities. This unit has been revealed to be Third Department's Sixth Bureau based out of Wuhan University in Hubei Province. According to the NSB, the Sixth Bureau is "engaged in technical aspects of surveillance and intelligence gathering on the Taiwanese agencies, intercepting telecommunications signals, hacking computers and mobile phone service networks and satellite imagery reconnaissance."

In addition to its official cyberwarfare units, China is believed to also have "reached out" to people with the necessary cyber skills in the IT sector and academic community to help fill any gaps in state expertise and personnel when needed. As the GitHub attacks illustrate, there is also ample evidence that China uses hackers and other cybercriminals to accomplish operations that it is officially unwilling or unable to commit. To be sure, cybercrime is often intimately tied to state-sponsored threats to cybersecurity. The use of affiliated hackers is based on the idea that cybercriminals can be used to escape the attribution that may otherwise provide the necessary legal, military or diplomatic links that other countries can use to prove China's official participation in cyberattacks. Consequently, in October 2014, the FBI issued a warning that a Chinese hacking collective known as Axiom has been engaged in a well-resourced, sophisticated campaign to steal valuable data from U.S. government agencies. According to the warning, Axiom, and other state-sponsored Chinese hacking groups like them, are "exceedingly stealthy and agile by comparison" to Unit 61398. Later in 2014, the U.S. Department of Justice indicted five Chinese citizens, affiliated with Unit 61398 on charges of theft of business information and unauthorized access to the computers of a number of U.S. companies.

China's cyber capabilities are organized by a strategy that calls for the early application of its cyberwarfare units against an adversary "to establish information dominance." Information dominance refers to: (1) taking and maintaining control of an adversary's access to its own information, and (2) disrupting the flow of information necessary for "decision-making or combat operations." Information dominance, moreover, requires that Chinese cyber capabilities are deployed pre-emptively or as early as necessary to support more traditional combat actions. Moreover, establishing information dominance requires China to have a fairly extensive and ongoing knowledge of an adversary's capabilities.

Lastly, in order to achieve its cyber strategic goals and effectively make use of its cyberwarfare units, China has employed a wide range of advanced cyberattack methodologies. For instance, The PLA's Unit 61398 is known for its use of zero-day exploits. A zero-day exploit refers to vulnerability in software that the software maker itself does not know exists. Discovering zero-day exploits require broad access to a software developer's internal routines and procedures. It also requires a better understanding of the software then the developer. This is often achieved by employing a technique known as advanced persistent threat (APT). APT refers to a hacking process that involves a long-term campaign to break into a computer network, avoid detection, and harvest valuable information over days, months and even years. According to Mandiant, Unit 61398's informal name was APT1 due to their skill at successfully carrying out advanced persistent threats.

Understanding China's cyber capabilities will play a large role in resolving the challenge of determining the appropriate response that the U.S. and other nations can make to cyberattacks that can be attributed to China. Where the attack can be traced to an official Chinese organ, perhaps a diplomatic or military response will be suitable. Where the attack is traced to non-official organs, non-conventional responses such as economic sanctions or criminal penalties will prove more effective.