CHINESE SURVEILLANCE AND ESPIONAGE CAPABILITIES
• U.S. Cyber security firm FireEye published a report on 2016
• From 2013 to 2016, there were a total of 262 cyber attacks that were identified as China-originated.
  • 182 attacks were targeted towards the U.S.
  • 80 were targeted to France, UK, Korea, Japan etc
• Another security firm Crowdstrike published a report that Chinese has been increasing again.
3PLA

- 3rd department of People’s Liberation Army
- started as an underground unit in the 1930s helped Mao win in 1949
- 100,000 people (linguists, hackers, analysts, etc) in 12 different bureau
- Mission: Surveillance and espionage of foreign intelligence communications, corporate emails and terrorist networks
UNIT 61398

- Address: 50 Datong Rd., Pudong New Area, Shanghai, China
- Alleged to be source of Chinese computer hacking attacks

“From 2006 to at least 2014, members of the PLA conspired together to hack into computers of U.S. businesses … to maintain unauthorized access … and to steal information for those entities that would be useful to their competitors in China”
# PAST ATTACKS

<table>
<thead>
<tr>
<th>Date</th>
<th>Operation</th>
<th>Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>Titan Rain</td>
<td>DoD, NASA, Lockheed Martin</td>
</tr>
<tr>
<td>2009</td>
<td>Ghost Net</td>
<td>Dalai Lama support network, different embassies</td>
</tr>
<tr>
<td>2010</td>
<td>Aurora</td>
<td>Google, Northrop Grumman etc</td>
</tr>
<tr>
<td>2011</td>
<td>Shady Rat</td>
<td>Defense contractors, UN, IOC</td>
</tr>
<tr>
<td>2015</td>
<td>OPM</td>
<td>Personnel files of U.S. Citizens</td>
</tr>
</tbody>
</table>
• Taiwan government warns employees not to use it
• Two functions of Beidou: one aimed at the public sector being the navigation system, and a restricted Chinese and Pakistan’s internal military communication and location data.