**ROYAL UNITED SERVICES INSTITUTE**
**OF NEW SOUTH WLES**

# REPORT SYNOPSIS

## *Enter the Cyber Dragon: understanding Chinese intelligence agencies' cyber capabilities*

**by Dr Tobias Feakin**

Australian Strategic Policy Institute Special Report No. 50 (June 2013)

---

[Dr Tobias Feakin, Senior Analyst for National Security at the Australian Strategic Policy Institute, covered aspects of this report in his address to Royal United Services Institute of New South Wales on 25 June 2013.]

1. There is much informed assessment and credible speculation about the significant scale of China's collection of foreign intelligence achieved through cyber operations, but there is insufficient knowledge in the West about that country's ability and achievements in analysing and applying that intelligence.

2. There is much more to learn also about the processing of that intelligence for economic, political and military purposes and the part cyber-accessed intelligence plays in policy formulation.

3. The most recognised cyber issue these days everywhere for policymakers is not the many military applications but cyber espionage and its effect on international relationships.

4. A major obstacle to China's use of cyber intelligence concerns its integration of data into a centralised mechanism for ordering and applying data for use by government, a weakness caused by multiple cyber entities with various missions, instanced by no less than four military-orientated People's Liberation Army (PLA) units responsible separately for foreign intelligence, signals intelligence and electronic warfare, as well as two civilian agencies functioning via the Ministry of State Security and the Ministry of Public Security interested mainly, but not only, in internal dissent.

5. The PLA unit responsible for signals intelligence is reported to be one of the most sophisticated in the world and pays particular attention to the Asia–Pacific region.

6. The Chinese government has a love-hate relationship with private hackers characterised by tolerance of them and a wish to contain them; the hackers generally act to protect China from critics, but are themselves critical of the government's slow response to curtailing the activities of those identified by the hackers, particularly entities interested in democracy, the Falun Gong, Tibet autonomy, Taiwan independence and others promoting criticism of China overseas.

7. There have been many accusations of China attempting to influence business in the West in a wide range of areas, and even of bugging Western business executives to acquire intellectual property, but the extent and value of this is unknown other than for a few well-publicised events.

8. Notwithstanding the above, the United States remains by far the most advanced nation in cyber capabilities, particularly cyber espionage.

**Ian Ingleby**
30 June 2013