Chinese Information Warfare Capabilities 2002-2009

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The Annual Report to Congress on the Military Power of the People’s Republic of China from the US Department of Defense has been issued every year since 2002:

The FY2000 National Defense Authorization Act (Section 1202) directs the Secretary of Defense to submit a report “…on the current and future military strategy of the People’s Republic of China [PRC]. The report shall address the current and probable future course of military-technological development on the People’s Liberation Army [PLA] and the tenets and probable development of Chinese grand strategy, security strategy, and military strategy, and of the military organizations and operational concepts, through the next 20 years.”

This report, submitted in response to the FY2000 National Defense Authorization Act, addresses (1) China’s grand strategy, security strategy, and military strategy; (2) developments in China’s military doctrine and force structure, to include developments in advanced technologies which would enhance China’s military capabilities; and, (3) the security situation in the Taiwan Strait.<http://www.defenselink.mil/pubs/china.html>

Reading through all the reports from 2002 through 2009 (the latter, not yet listed on the index page mentioned above, is available separately <http://www.defenselink.mil/pubs/pdfs/China_Military_Power_Report_2009.pdf>) provides valuable perspective on the DoD view of Chinese information warfare capabilities.

I have compiled extracts from the Annual Reports bearing on information warfare capabilities and commitment of the PRC and the PLA, including specific commentary about industrial espionage sponsored by agencies in the PRC.

The summary of extracts, “US DoD Annual Estimates of Information Warfare Capabilities and Commitment of the PRC 2002-2009,” is freely available online <http://www.mekabay.com/overviews/dod_prc_iw.pdf>. China’s propensity for gaining significant short-cuts in its industrial and military development processes through industrial espionage are well documented in this compilation and elsewhere. Interestingly, the same information warfare techniques seem to be applied to political espionage in the persecution of Tibetan nationalists.

The recently published report by researcher Dr Shishir Nagaraja <http://www.cl.cam.ac.uk/~sn275/> of the University of Illinois at Urbana-Champaign and Professor Ross Anderson <http://www.cl.cam.ac.uk/~rja14/> of Cambridge University on “malware-based electronic surveillance of a political organisation by the agents of a nation state” is entitled “The snooping dragon: social-malware surveillance of the Tibetan movement.” [Technical Report Number 746 from the University of Cambridge Computer Laboratory (UCAM-CL-TR-746, ISSN 1476-2986) <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf>] The scientists’ research reveals systematic espionage carried out through malware. The authors write in their abstract,

“While malware attacks are not new, two aspects of this case make it worth serious study. First, it was a targeted surveillance attack designed to collect actionable intelligence for use
by the police and security services of a repressive state, with potentially fatal consequences for those exposed. Second, the modus operandi combined social phishing with high-grade malware. This combination of well-written malware with well-designed email lures, which we call social malware, is devastatingly effective. Few organizations outside the defence and intelligence sector could withstand such an attack, and although this particular case involved the agents of a major power, the attack could in fact have been mounted by a capable motivated individual. This report is therefore of importance not just to companies who may attract the attention of government agencies, but to all organisations. As social-malware attacks spread, they are bound to target people such as accounts-payable and payroll staff who use computers to make payments. Prevention will be hard. The traditional defence against social malware in government agencies involves expensive and intrusive measures that range from mandatory access controls to tiresome operational security procedures. These will not be sustainable in the economy as a whole. Evolving practical low-cost defences against social-malware attacks will be a real challenge.”

As world economic conditions continue to worsen, I expect to see growing use of industrial espionage techniques by current actors and by new ones. Threats against proprietary information and perhaps even risks from sabotage may well increase over the next months and perhaps years.

Despite the reflex tendency for retrenchment as revenues fall, now is not the time to be reducing the information security workforce.

Semper vigilans.

***

M. E. Kabay, PhD, CISSP-ISSMP <mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online. <http://www.mekabay.com/cv/>

Copyright © 2009 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.