SPECIAL REPORT

ASPI

June 2013 — Issue 50

Enter the Cyber Dragon

Understanding Chinese intelligence agencies' cyber capabilities

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

by Tobias Feakin

> China's intelligence services have long been underanalyzed as major bureaucratic organizations and components of state power. This may have mattered relatively little during China's inward-looking and under-developed years. Today, its leaders are significant players on the world stage, and understanding how and what they learn about the world and how they formulate their policy choices is more important than ever.[1]

Espionage, or rather the information that it provides, is power, and cyberspace enables access to a far more geographically unrestricted information pool than do human intelligence (HUMINT) methods. The growing public attention paid to cyber-espionage throughout 2013 has been remarkable, and is marking a distinct shift to raise the issue's priority.

This has been due in large part to two elements. First, the 'Mandiant Report', a US private sector led investigation, publicly exposed, in a level of detail rarely seen, one of the Chinese People's Liberation Army (PLA) cyber-espionage units that had been hacking the *New York Times*' computer systems during 2012 and 2013. Second, the increasing rate of public announcements from the highest levels of US Government which outline their increased prioritisation of cyber issues. This reached a crescendo when the issue of cyberattacks was raised in the first conversation between President Obama and new Chinese President Xi Jinping. The cyber issue has been transformed from a low-order technical issue to one of strategic importance.

With the increased public focus on cyberattacks, it could be perceived that China is the only source of such attacks. Most reports wag the finger at ubiquitous 'Chinese' sources, but give little additional information. In fact, most developed and, indeed, many developing nations regularly use cyber capabilities for espionage. This is an extension of traditional espionage, but with fewer risks. And there's a bonus, at least for sophisticated attacks it's very difficult to identify the perpetrator. There's little discussion of the advanced state of the Russian Federation's cyber-espionage efforts, or the fact that the US is the most advanced nation, by some margin, when it comes to espionage in cyberspace.

The spotlight is currently firmly on China, but the organisations within China that use cyber-means for information, espionage and intelligence purposes remain relatively unknown. Aside from the Mandiant Report, the media have tended to refer to a generic 'Chinese' hacking source rather than a specific agency or other source. This is no doubt due to the inherent difficulties in attributing attacks and the sensitivities of such direct reporting.

This paper provides a clearer understanding of the key elements of the Chinese intelligence agencies that exploit the cyberdomain. It also shows that, while cybersecurity is a concern, much media coverage tends to oversimplify the issue and not present the public with the fuller picture.

The development of Chinese cyber capabilities

China's awakening to the value of asymmetrical technical capabilities can be traced back to the Gulf War in 1990–91. The US demonstrated not only its vast military superiority to a largely Soviet-equipped military (which in many ways mirrored China's own) but also its capacity for a new, different kind of warfare. Computers and other high-end technology provided real-time intelligence and enabled its array of smart weaponry. The Chinese military referred to the Gulf War as 'the great transformation', and this led during the rest of the 1990s to a great deal of contemplation, reflection and discussion in strategic circles about how China could adapt to this new battlespace. Various Chinese strategic thinkers such as Major General Wang Pufeng and Major General Dai Qungmin progressed thinking on how China could use the cyberdomain, leading to the concept of 'Integrated Network Electronic Warfare'. The culmination of this thinking led to the 1999 publication of *Unrestricted Warfare*, a book that laid the foundations of Chinese thinking on cyber issues. It focused on taking advantage of weaknesses created by an adversary's superior conventional capabilities, and a great deal on cyber-means for achieving this.[2]

However, the major current concern of policymakers isn't China's use of cyber capabilities in support of military operations. It's the use of cyberspace for espionage, reports of which have been so prevalent in the media in 2013, the year when cyber issues took on a heightened priority and strategic weight. Governments must now work out how to handle cyber matters as an element of their foreign policy to prevent long-term damage to international relationships.

China is determined to be a leader in information and communications technology more broadly. It's adopted a 15-year development strategy (2006–2020) that prioritises the 'informatisation' of its public services and economy and seeks to ensure its national security through cyber means.[3]

Chinese intelligence agencies

In January 2013, the PLA's Lieutenant General Qi Jianguo wrote in the official weekly newspaper of the Chinese Communist Party Central Party School:

> Cybersecurity concerns national sovereignty as well as the security of economic and social operations, and it concerns the quality of human existence. The West's so-called 'internet freedom' actually is a type of cyber-hegemony. In the information era, seizing and maintaining superiority in cyberspace is more important than seizing command of sea and command of the air were in World War II.[4]

Qi is responsible for foreign relations and intelligence in the PLA, and this was the first time he'd put his views on cyber issues in the public domain. While those views don't necessarily represent official Chinese policy, they encapsulate Chinese sentiment about cyberspace.

China's intelligence services, like those of most other countries, are split between civilian and military intelligence agencies. However, as Nigel Inkster points out, China has no formal central mechanism for assessing intelligence reports and filtering them into a common position for the government to consider.[5] In

Australia, this function would be carried out by the Office of National Assessments, which has a statutory role of advising the Prime Minister and the National Security Committee of Cabinet, as well as coordinating the activities of the collection agencies.

This means that the Chinese do not have an official way to integrate reporting into considered strategic analysis, or the ability to distil assessments into a single whole-of-government view. Chinese intelligence agencies, both military and civilian, also have components that operate at the provincial level, leading to regional differences in their analysis, performance and equipment. With multiple layers between the intelligence sources and China's leaders, it's probable that what reaches the top levels has been influenced by multiple procedures and biases, leading to a less reliable finished intelligence product.[6] It's important to remember that an authoritarian system isn't necessarily a unified and uncompetitive one.

Of the civilian agencies, the Ministry of State Security (MSS) is responsible for counterespionage, counterintelligence, foreign intelligence and domestic intelligence. The MSS's cyber capabilities are relatively unknown, but it's thought to have developed them to increase the collection of political and economic data on foreign governments, non-government organisations and those opposed to the People's Republic of China, all of which are a focus of interest for the ministry.[7]

A second civilian agency, the Ministry of Public Security (MPS), has responsibility for national policing and, to a lesser degree, domestic intelligence.[8] The MPS also actively supports information security research, the certification of commercial products for use by the Chinese Government, the control of commercial information security companies and the funding of academic grants. This has included the funding of a joint research project between Zhongxing Telecommunications Corporation and Chongqing University of Posts and Telecommunications.[9] This is but one example where Chinese military and intelligence agencies have become involved in the corporate sector, blurring the lines between the two and their separate objectives.[10]

There have been many examples of such involvement. The one with perhaps the highest profile involves Huawei, the Chinese telecommunications company. Along with Zhongxing Telecommunications Corporation, Huawei has been barred on security grounds from bidding for US contracts and acquisitions. In Australia, it's been banned from involvement in the National Broadband Network.[11] In a media release, the Attorney-General's Department stated that the decision to exclude Huawei was:

> ... consistent with the government's practice for ensuring the security and resilience of Australia's critical infrastructure ... We have a responsibility to do our utmost to protect its integrity and that of the information carried on it.[12]

According to a 2012 *Economist* report, these decisions have been made because Huawei's critics believe that:

> it has stolen vast amounts of intellectual property and that it has been heavily subsidised in its expansion by the Chinese government, eager to use it as a Trojan horse with which to infiltrate itself into more and more foreign networks.[13]

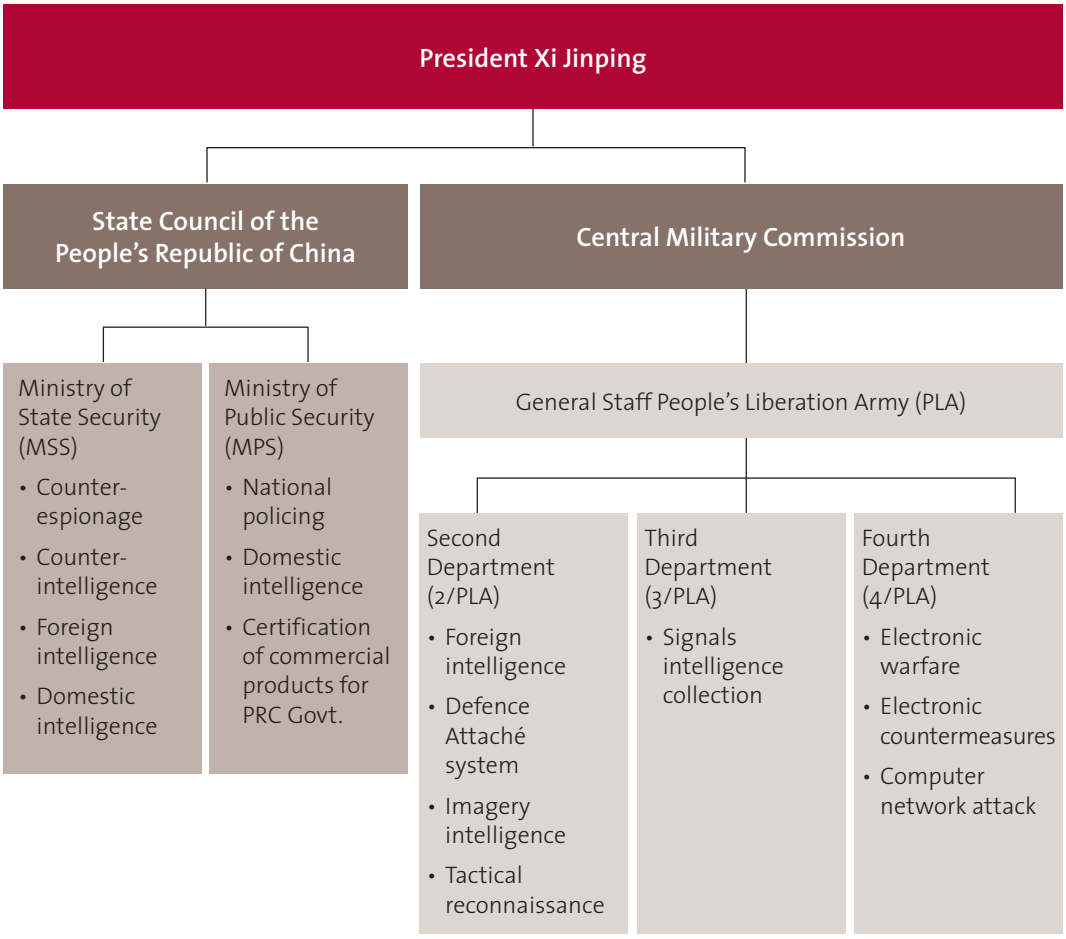
Military intelligence is the job of the PLA. The Second Department of the PLA General Staff Department (2PLA) is responsible for foreign intelligence gathering, the Defence Attaché system, imagery intelligence and tactical reconnaissance. The Third Department (3PLA) is the primary signals

intelligence (SIGINT) collection and analysis agency. 3PLA oversees one of the world's largest and most sophisticated SIGINT and cybercollection infrastructures, and certainly the largest indigenous operation in the Asia–Pacific region.[14] It manages approximately 12 operational bureaus and three research institutes and recovers huge volumes of data.[15] The Fourth Department (4PLA) is responsible for electronic warfare, countermeasures and computer network attack. The key differentiator between 4PLA and 3PLA is 4PLA's offensive mission.

While these divisions of labour appear quite straightforward, they're not. Many of the agencies have overlapping responsibilities and capabilities. For example, the MSS and the MPS are both concerned to some degree with internal dissent. Both the MSS and the military intelligence agencies are concerned with foreign influences and entities in China.

By no means are all cyber-activities conducted from China the work of the intelligence agencies.[16] Many attacks are rudimentary, and China's large community of patriotic 'netizens'—Chinese citizens who take it upon themselves to attack targets that question the Chinese state and its ideals—could well be responsible. One such organisation is the Red Hacker Alliance, which comprises some 300,000 people. There's no direct PLA control over the daily operations of the organisation, but rather an overlap of views and ideology. The group is tolerated because its activities allow plausible deniability and because of the benefits of the vast volume of information that the state can reap from its members.

Figure 1: Organisational chart



Yet this relationship can sometimes backfire. The group has shown an increasing willingness to demonstrate its dissatisfaction with what it perceives to be slow government responses to events by defacing government websites. The Chinese Government has had to develop ways to communicate with these hackers, to influence and attempt to stop their activities in these situations, but with limited success. The balancing act is highly complex. The Red Hacker Alliance fears a potential government crackdown on what it does, and the government fears a hack-instigated rebellion.[17]

Types of operations and motivations

What types of malicious network operations does China conduct, and to what end? While presenting evidence to the US Committee on Foreign Affairs in 2010, Larry Wortzel, a Commissioner of the US–China Economic and Security Review Commission, suggested that three key operation types predominate. Two are relevant to this discussion: those for exerting domestic control and those for intelligence gathering.

Operations to strengthen political and economic control in China

This type of information gathering is used to understand what key political dissidents are saying, how they use the web, and who they communicate with. Another aim is to understand who in China is providing what's seen as inflammatory information to international media outlets. This was exemplified by the *New York Times* hacking incident. The paper was subject to sustained hacking for four months, beginning after it published a story in October 2012 about Wen Jiabao's relatives accumulating several billion dollars through various business dealings during his time in power. It was suspected that hackers searched for information on who the sources of the stories within China were.[18]

Traditionally, the key targets for such attacks have been Chinese democracy activists, Tibetans, the Uighur community, Falun Gong practitioners and supporters of Taiwanese independence, as well as others who may paint a negative picture of China both at home and abroad. Essentially, the cyberdomain has meant that political dissidents of any persuasion, who in the past were too far away to be reached, can now be tracked clandestinely.

Operations to gather economic, political, military or technology intelligence and information

The aim of these operations is to gather information that could accelerate the development of the Chinese economy, to allow stronger economic negotiating positions and market access, to develop and field weapons systems, and to save time in technology research and development.[19]

In addition, a great deal of attention is paid to gathering information on foreign governments and those who comprise them. Indeed, it's been claimed that much information is being gathered to create a clearer picture of current and future leaders:

> They want to arm their diplomats and businessmen with the inside scoop to be able to expand their political and economic allies to help foster ruling elites that will never challenge the legitimacy of the Chinese Communist regime.[20]

However, it would be naive to imagine that most governments with a foreign intelligence collection capability do not accumulate information about political elites to understand the current and future direction of particular countries and how best to influence them.

Table 1: International cyberattacks reported in the media			
Date	**Target**	**Industry**	**Type of attack**
Attributed to: Third Department PLA 2nd Bureau			
March 2009	Coca-Cola takeover of China Huiyuan Juice Group	Food	Spear phishing attack
March 2011	RSA	Security firm	Spear phishing attack
April 2011	L-3 Communications	Defence contractor	Compromised SecurIDs
May 2011	Lockheed Martin	Defence contractor	Compromised SecurIDs
May 2011	Northrop Grumman	Defence contractor	Compromised SecurIDs
September 2012	Ongoing – US / Indian Government, defence & areospace industries	Government/Defence	Backdoor Trojan
January 2013	The New York Times	Media	Advanced Pesistent Threat (APT)
Attributed to: Chinese Government/ intelligence			
June 2007	Pentagon	Government	No details
March 2009	BAE Systems	Defence contractor	APT
Atttibuted to: China			
May 2010	U.S. Chamber of Commerce	Lobbying	APT
June 2011	Google	Internet	Phishing
August 2011	Mitsubishi Heavy Industries	Defence contractor	APT
October 2011	Japanese diplomatic missions (10 countries)	Government	APT
January 2012	European Aeronautic Defence and Space Company (EADS)	Defence contractor	No details
January 2012	Actividentity Smart Cards	Security company	Backdoor Trojan
June 2012	ThyssenKrupp	Defence contractor / Steel	No details
October 2012	The New York Times	Media	Targeted attack
January 2013	Reporters Without Borders	Media	Watering hole attack
March 2013	Indian Defence Ministry	Government	Spear phishing attack

In the UK, as far back as 2007 Jonathan Evans (then the director-general of MI5) wrote privately to 300 chief executives of banks and other businesses warning them that their IT systems were under attack from 'Chinese state organisations'. Subsequently, in 2010, MI5 accused China of bugging and stealing from UK business executives in order to blackmail them into betraying sensitive commercial secrets.[21] The media often cite unrealistically large figures for the value of intellectual property theft online. However, while IP can be costed, it's far from clear that the value is actually lost.[22]

One high-profile case of Chinese economic intelligence gathering has been widely reported in Australian media. The attempted merging of BHP Billiton and Rio Tinto, which would have created the largest iron ore exporter in the world, led to consternation in the Chinese mining industries. The Chinese were anxious that the merger would create a monopoly that would be able to exert greater control over the pricing of minerals largely exported to China. Subsequently, both BHP's and Rio Tinto's computer networks were penetrated by hackers from China, who were gathering information on the merger and on

Table 2: Australian cyberattacks reported in the media

Date	Target	Industry	Type of attack
Attributed to: China			
September 2007	Defence Department + other agencies	Government	No details
2007/2008	BHP Billiton - Rio Takeover	Mining	No details
July 2009	Rio Tinto - Stern Hu	Mining	No details
July 2009	Melbourne International Film Festival	Arts	Vandalism
April 2010	Fortescue Metals Group	Mining	No details
April 2010	The Australian Associated Press (AAP)	Media	Distributed denial of service (DDoS)
April 2010	'A financial institution in Australia'. (Knock-on effects to Optus & News Ltd.)	Financial/Media/ Telecommunication	DDoS
May 2011	Woodside Petroleum	Oil and gas	No details - ongoing
March 2013	Reserve Bank of Australia	Central Bank	Malware
Atttibuted to: Chinese Government/ intelligence			
April 2010	News Limited	Media	DDoS
September 2010	BHP - Via Blake, Cassels & Graydon LLP + others	Mining/ Law firms	Malware
March 2011	Ministerial computers (APH) + Parliament house network	Government	Malware

the advisory companies assisting the deal. Not long afterwards, the Chinese state-backed company, Chinalco, became active as a blocking bidder for Rio Tinto. This led to the collapse of the merger and the loss to shareholders of potentially millions of dollars as a result.[23]

The gathering of terabytes of economic, political, technological and military information by the Chinese doesn't always necessarily lead to its successful exploitation. For a start, because China doesn't have a core mechanism to pull intelligence together into a common government position, much of the information will be shelved or not reach those who could exploit it most powerfully.

Another danger arises from the autonomy that the agencies work with. The central leadership lacks control over who perpetrates attacks, and where and how attacks are made, which could lead to incidents spiralling out of control before the leadership can put a halt to them. However, a cynic would say that the plausible deniability and 'invisibility cloak' that this offers the central leadership is a fortunate coincidence.

It's also true that stealing information isn't the same as being able to use it. For example, during the Cold War, the Soviets ended up many generations behind the US in computing technology because they couldn't develop equipment that they had copied from stolen US blueprints quickly enough. In the Chinese case, the success of their operations will depend on their ability to convert their skills at cloning other's technology into comprehensive research and development and a true innovation culture. The shift from imitation to innovation will be the true challenge for China, and it's not clear that the shift has started yet.

Conclusions

Current reporting of Chinese intelligence operations describes it as working on an industrial scale under various named approaches to intelligence collection, including 'human wave', 'mosaic' or 'thousand grains of sand'. While the scale of Chinese cyber-operations isn't in question, the sophistication of some of their methods is. This could offer an insight into why they're caught so frequently. There's no doubt that the US is far more powerful and methodologically advanced in cyberspace than China. However, Peter Mattis has written that perceiving Chinese intelligence just in terms of its scale is not helpful and detracts from a fuller analytical understanding of Chinese intelligence capabilities and operations.[24] There's a need for a greater understanding of how the different intelligence agencies compete with one another, how they interact, how they formulate useful products and, indeed, how frequently this is achieved.

While Chinese intelligence agencies are collecting vast quantities of data, what happens to it once it's collected is relatively unknown. We're not certain how the data is processed and analysed, and whether it ever becomes a fully usable intelligence product that's of value to Chinese policymakers (as noted above, China has no equivalent to Australia's Office of National Assessments).[25] We need a clearer understanding of how the data is used and collated, but open source researchers can only go so far in their understanding of this process. It is incumbent upon those within the classified world to gain a deeper understanding of Chinese data collection mechanisms in order to fully understand how much practical use is made of the data in China's strategic political and economic decisions.

Finally, while China is following a process of 'informatisation' its own networks are becoming increasingly susceptible to network attack. It's often overlooked in the public debate that China is highly dependent upon cyberspace for its military and civilian government programs, and so has just as many vulnerabilities to attack as much of the Western world, if not more—as Chinese diplomats are all too eager to remind us when accusations are made against them.

Australian policy implications

The nature and tempo of Chinese cyber-activities have policy implications for the Australian Government. This is an issue that can't be ignored: it must be addressed in order to build an increasingly mature relationship with China. Six policy implications for Australia can be identified:

1. Both the US and the UK have 'called out' China publicly for its cyberattacks. Australia needs to work out what its public position is on this. At present, it doesn't have one.

2. It's necessary to engage China in a dialogue about cyber issues so that some common ground and limitations on cyber-activities can be set out. The US and China have agreed to set up a working group on cybersecurity (announced by US Secretary of State John Kerry in April 2013) to try to find common purpose on the issue.[26] Australia would do well to look for similar dialogues on cybersecurity with China and other regional partners, as this issue will only grow in importance over the coming years. This is especially important in the light of the growing economic relationship between Australia and China.

3. The Australian Government must develop an updated version of the 2009 Cyber Security Strategy as a matter of urgency.

In such a rapidly technologically evolving environment, it's unacceptable for such a policy to be left without an update for four years. A Cyber White Paper, later changed to a Digital Economy White Paper, was promised for delivery in 2012, but we're still awaiting it's arrival. It's expected that when it does arrive it will have a downgraded security component. The white paper should contain a clear examination of the threat picture in cyberspace, in order that both government and businesses can prioritise the issue accordingly.

4. There's a need for a government statement to provide some clarity on the nature of the threat in cyberspace. At present, the loudest voice discussing such threats is the media.

5. The next major international conference on cyberspace, at which nations will look to build common ground on cyber issues, will take place this year in Seoul. There's a need to develop a coherent Australian position for the conference, and that position should be representative of both the public and the private sectors.

6. We've reached a time when cyber issues have to be a component of government-to-government dialogues. Those issues are now strategically important, so they have to be incorporated into the 'two plus two' ministerial meetings that are taking place regionally. In that way, the groundwork for common positions that stem malicious cyber-activity can be laid. Otherwise, state-to-state relationships will be damaged.

Notes

1 Peter Mattis, 'The analytic challenge of understanding Chinese intelligence services', *Studies in Intelligence*, 56(3), September 2012, available from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-3/pdfs/Mattis-Understanding%20Chinese%20Intel.pdf.

2 Richard A Clarke & Robert K Knake, *Cyber war: the next threat to national security and what to do about it*, Harper Collins, New York, 2010, 47–51.

3 'China maps out informatization development strategy', People's Republic of China Embassy in Washington DC, 11 May 2006, available from http://www.china-embassy.org/eng/xw/t251756.htm.

4 Lt General Qi Jianguo, quoted in James Bellacqua & Daniel Hartnett, 'Article by LTG Qi Jianguo on international security affairs', CNA in-house translation, 2013, available from http://www.cna.org/sites/default/files/research/DQR-2013-U-004445-Final.pdf.

5 Nigel Inkster, 'Chinese intelligence in the Cyber Age', *Survival*, 2013, 55(1):45–61.

6 Peter Mattis, 'The analytic challenge of understanding Chinese intelligence services', *Studies in Intelligence*, 56(3), September 2012, available from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-3/pdfs/Mattis-Understanding%20Chinese%20Intel.pdf.

7 Nigel Inkster, 'Chinese intelligence in the Cyber Age'.

8 Since the establishment of the MSS in 1983, much of the MPS domestic intelligence function has been taken away from the organisation.

9 Bryan Krekel, Patton Adams & George Bakos, *Occupying the information high ground: Chinese capabilities for computer network operations and cyber espionage*, prepared for the US–China Economic and Security Review Commission by Northrop Grumman Corp, 7 March 2012, available from http://origin.www.uscc.gov/sites/default/files/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf.

10 Desmond Ball, 'China's cyber warfare capabilities', *Security Challenges*, 2011, 7(2):81–103.

11 Jill Stark, 'US follows Australia in naming Huawei as a possible security threat', *The Sydney Morning Herald*, 8 October 2012, available from http://www.smh.com.au/it-pro/security-it/us-follows-australia-in-naming-huawei-as-a-possible-security-threat-20121007-277ad.html.

12 Maggie Lu Yueyang, 'Australia bars Huawei from broadband project', *New York Times*, 26 March 2012, available from http://www.nytimes.com/2012/03/27/technology/australia-bars-huawei-from-broadband-project.html?_r=0.

13 'Huawei—the company that spooked the world', *The Economist*, 4 August 2012, available from http://www.economist.com/node/21559929.

14 'Huawei—the company that spooked the world'.

15 For a full account of 3PLA, see Mark Stokes, Jenny Lin & LC Russell Hsiao 2011, T*he Chinese Liberation Army signals intelligence and cyber reconnaissance infrastructure*, Project 2049 Institute, available from http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf.

16 Nigel Inkster, 'Chinese intelligence in the Cyber Age'.

17 Scott Henderson, 'Beijing's Rising hacker Stars: How Does Mother China React?', *IQ Sphere*, Fall 2008, p. 25.

18 Nicole Perlroth, 'Hackers in China attacked the Times for last 4 months', *The New York Times*, 30 January 2013, available from http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0.

19 Larry M Wortzel, *China's approach to cyber operations: implications for the United States*, testimony before the Committee on Foreign Affairs, House of Representatives, 2010, available from http://origin.www.uscc.gov/sites/default/files/Congressional_Testimonies/LarryWortzeltestimony-March2010.pdf.

20 Richard Fisher, quoted in Alex Newman, 'China's growing spy threat', *The Diplomat*, 11 September 2011, available from http://thediplomat.com/2011/09/19/chinas-growing-spy-threat/.

21 David Leppard, 'China bugs and burgles British business executives', *The Sunday Times*, 4 February 2010.

22 Andrew Davies, 'Your system might be at risk: Australia's cyber security', *ASPI Policy Analysis*, 31 May 2011, available from http://www.aspi.org.au/publications/publication_details.aspx?ContentID=296&pubtype=9

23 Christopher Joye, 'It's global cyber war out there', *Australian Financial Review,* 2 January 2013, available from http://www.afr.com/f/free/national/it_global_cyber_war_out_there_94da3CY7Avufi9jp5d0JTI

24 Peter Mattis, 'China's misunderstood spies', *The Diplomat*, 31 October 2011, available from http://thediplomat.com/2011/10/31/china%E2%80%99s-misunderstood-spies/?all=true.

25 Nigel Inkster, 'Chinese intelligence in the Cyber Age'.

26 Terril Yue, *US, China agree to work together on cyber security*, Reuters, 13 April 2013, available from http://www.reuters.com/article/2013/04/13/us-china-us-cyber-idUSBRE93C05T20130413.

About the author

Tobias Feakin is ASPI's senior analyst specialising in national security.

Important disclaimer

About Special Reports

Generally written by ASPI experts, Special Reports are intended to deepen understanding on critical questions facing key strategic decision-makers and, where appropriate, provide policy recommendations. In some instances, material of a more technical nature may appear in this series, where it adds to the understanding of the issue at hand. Special Reports reflect the personal views of the author(s), and do not in any way express or reflect the views of the Australian Government or represent the formal position of ASPI on any particular issue.

ASPI
Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
Web www.aspi.org.au

ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

RRP $5.00 ISSN 2200-6648

BECOME A MEMBER

JOIN NOW TO RECEIVE PRINTED PUBLICATIONS AND MORE

Join Australia's liveliest minds writing today on defence and strategic issues. ASPI produces ***Strategy***, ***Strategic Insights***, ***Special Reports***, and specialist publications including ***The Cost of Defence*** and an upcoming ADF capability annual.

ASPI's work is at the cutting edge of new thinking on defence and security.

Thoughtful, ground-breaking and often controversial, ASPI leads the public debate on these issues. Become a valued part of the ASPI team today!

Join now and we will post your choice of 3 free publications from our recent publications list.

Future subjects include:

- **Australia as a Southern Hemisphere power**
- **Australia's defence cooperation program**
- **Implications for strategic changes in the Middle East**
- **Options for Australia–Indonesia cooperation**
- **Maritime rivalries in the Indo-Pacific**
- **ADF capability annual**

TELL A FRIEND ABOUT ASPI

Join Australia's liveliest minds writing today on defence and strategic issues. Each year the Australian Strategic Policy Institute (ASPI) will produce up to six issues of ***Strategy***, and a number of other publications on issues of critical importance to Australia and the Asia–Pacific.

Thoughtful, ground-breaking and often controversial, ASPI leads the public debate on defence and security issues.

JOIN ASPI

Name

Position

Company/Organisation

❑ Government **❑ Non-Government**

Address

City **State** **Postcode**

Country

Telephone

Email

SELECT 3 FREE PUBLICATIONS

❑ Facing the dragon: China policy in a new era
❑ Planning the unthinkable war: 'AirSea Battle' and its implications for Australia
❑ Strategic contours: The rise of Asia and Australian strategic policy
❑ Two steps forward, one step back: Indonesia's arduous path of reform
❑ Beyond bin Laden: Future trends in terrorism
❑ Our near abroad: Australia and Pacific islands regionalism
❑ Forks in the river: Australia's strategic options in a transformational Asia

INDIVIDUAL	❑ 1 year *$199*	❑ 2 years *$378*	❑ 3 years *$537*
STUDENT*	❑ 1 year *$99*	❑ 2 years *$188*	❑ 3 years *$263*
CORPORATE (Oct 06+)	❑ 1 year *$649*	❑ 2 years *$1233*	❑ 3 years *$1752*

* (STUDENT ID _____)

To join
1) Subscribe online www.aspi.org.au
2) Mail to Level 2, 40 Macquarie St, Barton ACT 2600, or
3) Phone (02) 6270 5100 or fax (02) 6273 9566

❑ Cheque ❑ Money Order ❑ Visa ❑ MasterCard ❑ AMEX ❑ Diners

Payable to Australian Strategic Policy Institute ABN 77 097 369 045

Name on card

Card no.

Expiry Date **/** **Total Amount $**

Signature

This will be a **TAX INVOICE** for GST purposes when fully completed and payment is made.
Please note specialist publications are not included.