Defence Academy
of the United Kingdom

Defence Academy of the United Kingdom

Special Series

Cyber Probing: The Politicisation of Virtual Attack

Alex Michael

10/12

Cyber Probing: The Politicisation of Virtual Attack

Alex Michael

Key Findings

- The paper seeks to explain the offensive opportunities, effectiveness, simplicity (and deniability) offered by virtual attacks, by means of topical examples.

- Probing via networks is increasingly used by state and non-state actors to achieve political ends – often in cases where traditional warfare has been used in the past.

- The UK, while not ill-prepared to meet this problem, is putting itself at risk by using foreign companies linked closely to other government agencies.

- The UK needs to confirm it has appropriate capacity to deal with detection/protection/tracing of attacks. This in turn requires investment both of funding and of suitable, trained and experienced personnel.

Contents

Cyber Probing: The Politicisation of Virtual Attack

Alex Michael

Introduction

By common consent, cyberspace has emerged as an arena for conducting operations which is as important as land, sea, air, and space before it. Nonetheless with the relative novelty of network operations, cyberspace remains inadequately defended, policed and indeed comprehended.

The US Department of Defense (DOD) defines cyber warfare as "*the use of computers and the Internet to conduct warfare in cyberspace*". However, cyber warfare is merely one aspect of a much broader phenomenon, which in this paper we will term **cyber attacks**. Traditionally cyber attacks have been categorised into four separate spheres. These are:

- **Cyber crime** – such as identity theft/fraud. In essence this consists of conducting cyber attacks against individuals or private institutions for financial gain.
- **Cyber espionage** – This is operations conducted for the purposes of information gathering. Targets can include government departments or private sector industries.
- **Cyber terrorism** – Defining terrorism itself is difficult and controversial. Defining cyber terrorism is all the more so. Depending on one's understanding of terrorism, one can adduce a number of activities that take place in cyberspace which carry characteristics of cyber terror.
- **Cyber warfare** – These are military operations conducted in cyberspace; for instance an attack on critical national infrastructure carried out to achieve military aims by a state party.

This paper will investigate case studies illustrating all four; yet the cross-over between the spheres is now a significant factor in arriving at clear and workable definitions, due to erosion of dividing lines between the categories because of both social factors and the evolution of communications technology. This paper will argue that the cyber arena has now become far more politicised than traditionally thought. This however does not necessarily imply that all cyber attacks are politically motivated and can be directly associated with government actors; merely that both state and non-state actors around the world are beginning to seize opportunities that cyberspace provides. While non-state actors continue to exercise traditional means of protest such as sit-ins, civil disobedience, demonstration marches, and petitions; there are multiple examples of cyber attacks used to enhance or complement traditional actions as disruptive protest activity spills over into the networked world.

Just as a networked world presents opportunities, it also presents a potential Achilles' heel for sovereign states.

There is an image in the popular imagination of cyber attack used singlehandedly in Hollywood blockbuster fashion to bring about sudden massive disruption, or even the downfall of sovereign states. No instances of this kind of attack are known in the public domain; but what remains unremarked in the popular narrative is a constant ongoing background level of cyber attack as part of a holistic, coordinated programme to achieve the political, economic and social aims of nation states. These attacks are capable of causing disruption and exerting leverage as part of a well-considered and developed hybrid strategy planned for the long or short term. In this context, cyber attacks are used in conjunction with many other forms of pressure, ranging from physical protest to social and diplomatic approaches, to influence the target and attempt to force its hand. This is not warfare in the traditional sense, nor even in many of the new senses that have been proposed over the last decade; and the concept of a single crippling cyber strike, while engaging, appears at present to remain a remote likelihood. Yet while sovereign states are robust and enduring, under-estimation of the potential of cyber attack can expose fatal weaknesses in them.

This paper will use case studies to evaluate the success of cyber attacks by state and non-state actors as a tool to achieve aims which are congruent with those of sovereign states. While attribution of cyber attacks is a notorious problem, at the very least it can be said that many groups sponsored by, or claiming affiliation with, sovereign states, are carrying out criminal cyber attacks which promote those states' interests and policies.

'Chased By The Dragon – Offensive Cyber Activity From China'

> *"China's appreciation for the centrality of information as a tool of statecraft and military power has significant implications. Given the tremendous advances in information technologies both in terms of the rate of innovation and quality of improvements, China is well positioned to exploit this revolution. Just as China has surprised sceptical observers with its rapid developments in nuclear weapons, ballistic missiles, and space programs, the Chinese may similarly come to the forefront in IW".* [1]

China has taken great interest in the development of its cyber-warfare capability, which is the subject of intense scrutiny by the West. *Dragon Bytes*, written in 2004 by the US Foreign Military Studies Office (FMSO), charts the development of Chinese Information Warfare (IW) capability from 1999.[2] In 2007 the same organisation published *Decoding the Virtual Dragon*, a review of post-2003 developments. Both note the centrality and the resources that China dedicates to IW. There is no shortage of examples of the result.

Tibet

Researchers in internet security have long been aware of the apparently organised activities of Chinese hackers targeting western businesses and governments in attempts to extract as much information as possible from their networks. One of the most dramatic examples of an organised campaign of this nature was exposed in March 2009, when a security team discovered "*software capable of stealing information installed on computers in 103 countries from a network that targeted government agencies*".[3] It was established that the software infected more than 1,295 computers and nearly a third of these were so-called 'high-value targets'.[4] A report produced by Information Warfare Monitor highlighted some of those affected as embassies belonging to Germany, India, Thailand, Iran and Latvia as well as networks utilised by the administration of the Dalai Lama. The ten-month investigation,

[1] Toshi Yoshihara, 2001. *Chinese Information Warfare: A Phantom Menace or Emerging Threat*? [online] Available at: http://www.au.af.mil/au/awc/awcgate/ssi/chininfo.pdf [accessed: 19 Nov 09].

[2] Timothy L. Thomas, 2004. *Dragon Bytes, Chinese Information War Theory and Practice* (Fort Leavenworth, KS: Foreign Military Studies Office).

[3] Ben Worthen, 2009. *Wide Cyber attack is linked to China*, [online] published 30 March 2009. Available at: http://online.wsj.com/article/SB123834671171466791.html [accessed: 30 March 2009].

[4] Report carried out and published by Toronto based Information Warfare Monitor, http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

primarily initiated at the request of Tibetan exiles,[5] found that "*the Tibetan computer systems we manually investigated, and from which our investigations began, were conclusively compromised by multiple infections that gave attackers unprecedented access to potentially sensitive information*".[6] The mass infections, and the tools used to manage them and extract information from the compromised networks, received the name GhostNet.

Although Chinese hackers have continuously executed denial of service (DoS) [7] and malicious code attacks against the websites of pro-Tibetan administrations, Information Warfare Monitor determined that the sophisticated 'malware'[8] used in the GhostNet attacks enabled the attackers to steal files, capture passwords, and even activate the webcams of their victims, then retrieve the stolen information and return it to the network's controller. The malware was delivered to the target computers in seemingly legitimate email messages, which appeared to be sent from personal/professional contacts known to the target so as not to raise suspicions. The emails would contain links or attachments which when opened installed malicious content. This means that emails had been monitored for some time before the actual attacks, in order to ensure that when the malware was sent it would come from a source which appeared legitimate and trustworthy to the recipient.

Although the investigators of GhostNet stop short of attempting to prove direct complicity by the Chinese state in the attacks, gathering evidence on the activities of the exiled Tibetan leader and his supporters furthers Chinese state policy. Further circumstantial evidence linking China to the attacks emerged when a young woman working for Drewla[9] in Dharamsala attempted to visit her family in Tibet; she was arrested and imprisoned for two months, and during her interrogation was shown transcripts of her internet conversations. She was then warned that her group was under constant surveillance and informed she was no longer welcome in Tibet.

Such instances are far from unique. In 2008 Nart Villeneuve, a senior research associate at the Information Warfare Monitor, conducted an in-depth study of surveillance and security practices affecting TOM-Skype, the Chinese version of the popular communication tool Skype.[10] The investigation concluded that full transcripts of private conversations of TOM-Skype, and Skype users communicating with TOM-Skype users, were regularly scanned for keywords and this data then uploaded and stored on insecure servers in China. According to the report, millions of private messages ranging from sensitive political issues to business transactions were archived and downloadable from the insecure servers.

These instances emphasise the interception, monitoring and offensive capabilities of actors within China whether state or non-state, and the use of intrusive cyber attacks to achieve local, regional and international political aims.

[5] The request came after suspicions arose that systems had been compromised, after a foreign diplomat whom the Dalai Lama's office had contacted by email received a phone call from the Chinese government discouraging a meeting with the Dalai Lama.

[6] Information Warfare Monitor, 2009. *Tracking GhostNet: Investigating a Cyber Espionage Network*, [online] published: 29 March 2009. Available at: http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network [accessed: 23 November 2009].

[7] Denial of service attacks are primarily intended to block access to specific websites. This is usually achieved by sending a massive number of information requests to the site simultaneously. This overwhelms the site's server(s) and renders them unavailable to all.

[8] Malware is a contraction of "malicious software". The purpose of malware is to infiltrate and compromise a computer system, usually without the target's knowledge.

[9] Drewla is a non-governmental organisation that attempts to use Tibetans to engage online with young Chinese citizens to raise awareness about the Tibetan situation.

[10] Nart Villeneuve, 2008*. Breaching Trust: An analysis of surveillance and security practices on China's TOM-Skype platform* [online] Available at: http://www.nartv.org/mirror/breachingtrust.pdf [accessed: 12 Nov 09].

Rio Tinto

In April 2009 Xiong Weiping, chairman of the Chinese State Aluminium producer Chinalco, issued a press release regarding his company's plans for doubling its stake in the Rio Tinto Group.[11] Xiong's announcement referred to negotiations started earlier in the year when Chinalco and Rio Tinto had agreed a $19.5bn deal which would have increased the holdings of the Chinese state companies, already the largest single shareholder, from 9% to around 18% of stock. However, disputes over board representation, the arrival of new Rio Tinto Chairman Jan du Plessis in April 2009, and a separate stream of negotiation with the dual UK-Australian mining company BHP Billiton saw prospects for the Chinese deal gradually eroded, and in June 2009 Rio Tinto agreed to pay Chinalco a $195m severance fee as compensation for its withdrawal from negotiations.[12] So there was little surprise when Xiong told the media that he was "*very disappointed with the decision of the Rio Tinto board to withdraw their recommendation for this transaction*".[13] Given what followed, it may be that Xiong's "disappointment" should have been taken as a warning.

In July 2009 four Rio Tinto employees were detained in Shanghai by State Security agents over allegations that they had stolen state secrets. One of the four, Stern Hu, is an Australian citizen, while the others are Chinese nationals. Rio Tinto issued an immediate statement denying the accusations. The detention of the four followed not only the failed investment bid by Chinalco but also failure by Rio Tinto to meet demands for new pricing structures by the Chinese steel industry – the company's largest marketplace. Matters became worse in August 2009 when reports were published on *China Secret Protect Online*, a Chinese-language Web site that claims affiliation with the Communist Party's State Secrets Bureau. These reports, allegedly written by officials from the Bureau, claimed Rio Tinto was guilty of "deceit" and deliberately overcharging the country's steel mills more than $100 billion for iron ore.[14] The allegation was based, according to the report, on *"the large amount of intelligence and data from our country's steel sector found on Rio Tinto's computers".*[15]

If information – "*strong evidence to prove they* [the four Rio Tinto executives] *were spying and stealing China's state secrets*"[16] – was recovered from Rio Tinto's computers, one of the most likely methods for doing so was network infiltration, an idea that was given greater credence when "*Australian intelligence agents said that agents working for China had tried to hack into systems operated by Rio Tinto*".[17] The way in which information of this kind could be 'found' adds to China's international reputation for launching sophisticated cyber attacks. It was widely reported in December 2007 that the British Security Service (MI5) had warned major international companies, including Rolls-Royce, Shell and some of the UK's largest banks, of the high level of covert cyber attacks originating from China. Repeated allegations

[11] Rio Tinto is a diversified multinational mining and resources group established in the late 19th century and named after its first investment, a failing mining company situated on the Rio Tinto river in Spain. Since then, the company has grown to become one of the leading global producers of commodities such as aluminium, iron ore, copper, uranium, coal, and diamonds.

[12] Jamil Anderlini, 2009. *Chinalco's Chief defends Rio Bid*, The Financial Times 11 June 2009.

[13] Ibid.

[14] James T. Areddy, 2009. *China accuses Rio Tinto of deceit*. The Wall Street Journal. 10 Aug 2009. However, analysts noted that Rio's iron ore sales to China in the past six years had totalled only $42 billion. See David Robertson, 2009. *China backs away from newest Rio claims*, The Times, [online], published: 11 August 2009. Available at: http://business.timesonline.co.uk/tol/business/industry_sectors/natural_resources/article6790647.ece, [accessed: 11August 2009].

[15] Ibid.

[16] David Barboza, 2009. *China says Australian is detained in spy case*. New York Times, [online] published: 9 July 2009. Available at: http://www.nytimes.com/2009/07/10/world/asia/10riotinto.html?_r=1 [accessed: 12 July 2009].

[17] Ibid.

that US government departments such as the DoD have been hacked by China have seen the US take a forward-leaning stance in its cyber-security measures.[18]

The four detainees were not charged under China's compendious state secrets laws, but in August 2009 their arrest was formalised on suspicion of commercial bribery and trade secrets infringement, with formal charges brought in February 2010. Although the dropping of the espionage charges assisted in defusing a diplomatic row with Australia, the real damage in both commercial and political terms had already been done.

China is the world's leading steel maker and imports 500 million tons of iron ore each year.[19] China is heavily reliant on this trade, and takes the position that it is unreasonable for it to pay the same price as countries who import considerably less. In May and June 2009 Japan and South Korea agreed a 33% reduction in price for iron ore from Rio Tinto and BHP Billiton, whereas China had been looking for a reduction of up to 50%. Shan Shanghua, Secretary General of the CISA (China Iron and Steel Association) stated: "*China will not accept the price that the three biggest mining companies offered to other countries' mills. Since China imports nearly half of the worlds' iron ore output, it's fair for us to ask for a bigger price cut*".[20]

China's aggressive stance has had a significant impact, with Rio Tinto's share price falling 25% from its 2009 peak,[21] following the arrests and the stalling of iron ore price talks. And in November 2009, Sam Walsh, Chief Executive of the ore unit of Rio Tinto, agreed China could use a new pricing system, moderating the company's position regarding iron ore prices to Chinese steel mills. This conciliation followed on from statements in October that year by the company that *"mending relations with China, its biggest customer and shareholder, was a top priority after a year of tensions*'.[22] This approach of appeasement from Rio Tinto clearly highlights the leverage the Chinese had been able to exert on the company following the collapse of the investment bid from Chinalco.

Informed speculation suggested that China was either punishing Rio Tinto for abandoning the deal with Chinalco, or attempting to pressurise Rio Tinto into accepting a significant price reduction responding to the dramatic fall in share value. According to Bill Powell, senior writer for CNN Money, "*its fundamental interest in Chinalco buying into Rio Tinto was to break the stranglehold that Rio, BHP Billiton and Brazil's Vale have on global pricing for iron ore and other key commodities that China desperately needs - and will need for decades. (Today, those big three account for over 70% of globally traded iron-ore sales)."*[23] Rio Tinto's decision to walk away from the Chinalco deal was received as a severe loss of face in China, compounded when a subsequent deal between Rio and BHP Biliton was signed strengthening the monopoly.

[18] This is explained in more detail in Chapter 4.
[19] Tradingmarkets.com, 2009*. Analysis: China Seeks New Iron Ore Import Negotiation Mechanism*, [online] published: 19 August 2009. Available at: http://www.tradingmarkets.com/.site/news/Stock%20News/2488184/ [accessed: 19 August 2009].
[20] Xinhua: *China yet to receive Rio message about new pricing mechanism,* [online] published: 3 November 2009. Available at: http://english.peopledaily.com.cn/90001/90778/90861/6802537.html [accessed: 3 November 2009]
[21] James Regan, 2009. *Rio Tinto china iron ore talks inactive*, Reuters, [online] published: 4 September 2009. Available at: http://uk.reuters.com/article/idUKTRE58318F20090904 [accessed: 5 September 2009].
[22] Telegraph.co.uk, 2009. Rio *Tinto makes China top priority*, [online] published: 30 October 2009. Available at: http://www.telegraph.co.uk/finance/newsbysector/industry/mining/6470168/Rio-Tinto-makes-China-top-priority.html [accessed: 1 November 2009]
[23] Bill Powell , 2009*. Rio Tinto - China strikes back*, [online] published: 24 August 2009. Available at: http://money.cnn.com/2009/08/24/news/companies/china_rio_tinto.fortune/index.htm?section=magazines_fortuneintl [accessed: 24 August 2009]

China's recent security statements have repeatedly put forward the notion that the biggest threat to its future is the fight for resources and raw materials. The fact that China is overly reliant on foreign traders and their set prices is clearly a bone of contention. This provides background not only for China's attempt to buy a significant portion of Rio Tinto but also for its continuous efforts to reduce the price of iron ore since investment talks ended.

Yet even with aims achieved, concerns over China's cyber activity have not abated. The Age newspaper (Melbourne) claimed that Rio Tinto's iron ore team had purposefully avoided all meetings in China for more than a month due to apprehension that their emails and phones were bugged there[24] - while the Herald newspaper also suggested that senior Rio Tinto executives had been shadowed and intimidated on recent trips to Shanghai. Australian newspapers also stated that Chinese intelligence agents had attempted to access former Australian Prime Minster Kevin Rudd's phone and email account when he visited Beijing for the Olympics in 2008. Although this was never officially confirmed, Australian politicians instantly called for greater communications security.[25]

There are conditions for further confrontation between China and Australian mining companies. The Mongolian government had been in talks with a selected shortlist of bidders seeking to develop Mongolian coal deposits in the Tavan Tolgoi region. Among the bidders were BHP Billiton, Rio Tinto and China's Shenhua Energy. Tavan Tolgoi has estimated reserves of 6.5bn tons of coal, of which 2bn is believed to be high-grade and suitable for power station use.[26] The World Bank is aiding the Mongolian government with a strategy for the development of the infrastructure in the region, so development of the deposits would be assisted with the construction of towns, railways and roads, making a highly attractive proposition. The chance to diminish a foreign competitor's effectiveness in launching a bid in China's backyard could be too good an opportunity for China to ignore.[27]

Melbourne International Film Festival

China's overt and covert harassment of Rio Tinto was not the only cause of an increase in diplomatic tensions with Australia during 2009. The organisers of the Melbourne International Film Festival (MIFF) came under repeated cyber attack following its decision to showcase "The 10 Conditions of Love", a documentary on the head of the World Uighur Congress and activist for Uighur autonomy, Rebiya Kadeer. Although Kadeer now lives in the US, she has often been blamed by the Chinese government for instigating protests and riots inside the Xinjiang region. The MIFF decision to showcase the film drew severe criticism from China, with several Chinese directors boycotting the event after organisers refused a request from the Chinese consulate for the film to be withdrawn and for Kadeer's invitation to the festival to be rescinded. This stance led to hackers based in China infiltrating the MIFF website and replacing festival information with the Chinese flag and a barrage of anti-Kadeer messages.[28]

[24] Anne Barrowclough, 2009.*Rio Tinto executives arrested in china*, [online] published: 8 July 2009. Available at: http://business.timesonline.co.uk/tol/business/industry_sectors/natural_resources/article6664810.ece [accessed: 8 July 2009]

[25] David Barboza , 2009. *China says Australian is detained in spy case*. New York Times, [online] published: 9 July 2009. Available at: http://www.nytimes.com/2009/07/10/world/asia/10riotinto.html?_r=1 [accessed: 12 July 2009].

[26] BBC Monitoring: news.mn, 2009. *Mongolian Government in talks with around 10 shortlisted bidders on Tavan Tolgoi coal mine*, 10th November 2009 [accessed on 11th November 2009].

[27] In February 2010 it emerged that Mongloia's government had cancelled the auction of an estimated $2 billion stake in Tavan Tolgoi after deciding to hold onto 100% of the coal deposit and maintain full control. It is now speculated that the Mongolian government hopes to strike a deal with a global miner to develop the region on a contract basis, minus a significant holding.

[28] ABC News 26 July 2009 confirmed reports that "*The hacker has contacted the ABC saying he does not work for the Chinese Government and is just an ordinary, angry Chinese citizen who objects to the film*". Available at:

Subsequently, the site's online booking page was attacked resulting in its unavailability. Festival director Richard Moore's email account was overwhelmed with abusive messages following the MIFF decision to stand firm. Furthermore, members of the Australian general public who had bought tickets to the festival through the official MIFF website reported that their email accounts had been subjected to continuous spamming. At the time, Mr Moore said the breach had led to him receiving "*a virtual mini tsunami of emails that I can only describe as being vile… They're calling the Melbourne International Film Festival racist, scumbags, all sorts of things. I've probably received 60, 70, 80 of them and they're going to keep on coming every day."*[29] It is interesting to note that the Australian Broadcasting Corporation purchased the film, "The 10 Conditions of Love", but has yet to show it after cancelling a broadcast in December 2009 for reasons which remain to be explained.

The MIFF experience illustrates the adverse consequences of offending China for the networks of even small organisations, and furthermore show the willingness of groups based in China, whether state or non-state, to devote considerable energy to furthering the state's political and economic aims.

Operation Aurora

On January 12, 2010, four years after its much-criticised entry to the Chinese market, Google announced that it was '*no longer willing to continue censoring'* results on its Chinese site, Google.cn, citing infiltration of the Gmail accounts of a number of Chinese human rights activists. In a post on the official Google blog entitled *A new approach to China*, Google's Chief Legal Officer, David Drummond, admitted that Google like many large organisations faced cyber attacks of varying capacity on a 'regular basis'. [30] He continued that "*in mid-December [2009], we detected a highly-sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google. However, it soon became clear that what at first appeared to be solely a security incident-albeit a significant one-was something quite different*."[31]

Upon investigation Google detected that they had been just one of at least 20 companies similarly targeted in what has become known as Operation Aurora. The investigation revealed that dozens of Gmail accounts in China, Europe, and the United States belonging to advocates of human rights in China had been regularly accessed by third parties – the infiltration resulted from malware on the users' computers rather than a security breach at Google itself.

Although Google did not explicitly accuse the Chinese government, the statement in response that it was no longer willing to censor results on Google.cn did recognise that this might well mean having to shut down Google.cn, and potentially all offices in China.[32] It is increasingly rare for large organisations to be so open with an international audience concerning issues of data security and protection, but in the circumstances Google felt it had been given little choice other than to express its concerns and threaten to shut down

http://www.abc.net.au/news/stories/2009/07/26/2636770.htm?section=entertainment [accessed: 23 November 2009].

[29] ABC news, 2009. *MIFF 'sticking to guns' over Uighur film*, [online] published: 26 July 2009. Available at: http://www.abc.net.au/news/stories/2009/07/26/2636770.htm?section=entertainment [accessed: 23 November 2009].

[30] Google Blog, 2010. A New Approach to China, [online] published: 12 January 2010. Available at: http://googleblog.blogspot.com/2010/01/new-approach-to-china.html [accessed: 13 January 2010].

[31] Ibid.

[32] On 22nd March 2010 Google began redirecting users from Google.cn to Google.com.hk. However in June 2010 Google announced a 'new approach' by ensuring users make an 'active choice' after Beijing warned it could remove its licence to operate in the country. Chinese users are now sent to the Google.cn home page, however, a click anywhere on the screen will then divert the user to the Honk Kong site.

operations. By giving up its operations in China, Google knew it would also be giving up its 338 million internet users there (roughly one-third of the market), second only in search engine use to Baidu.com. Moreover, it would also risk losing billions of dollars in revenue from internet advertising.

Four years ago, on entry into China, Google ignored the criticism of free speech advocates, instead taking the view that increased access to information for Chinese internet users compensated for a degree of censorship. Nonetheless, in the last year Google's YouTube website has been blocked in China indefinitely for 'spreading pornographic videos', while Google Books has been forced to address issues with Chinese authors (as well as those elsewhere) over copyright infringement, leading to increasing tensions.

Google's tough public stance can be interpreted as an attempt to embarrass the Chinese government internationally and spread concern and disaffection (with the government) among the millions of Chinese users of Google.[33] US Secretary of State Hilary Clinton responded by criticising China's restrictions on the Internet and the silencing of dissidents and human rights campaigners. In response, China's Foreign Ministry spokesman Ma Zhaoxu said that such words could be harmful to US-China relations.[34] The consequences affect companies other than Google; the French, Australian and German governments have warned their electorates not to use Microsoft's Internet Explorer web browser after it appeared that security flaws in the browser could have been exploited to conduct the attack on Google.[35]

Operation Aurora has touched on a number of points of contention between the US and China, ranging from internet openness and cyber espionage, to freedom of speech and human rights. But it was far from the only "cyber issue" arising between the two countries, as will be explored further below.

The Red Hackers

The 'Red Hackers' are a group of privately organised patriotic Chinese hackers, motivated by nationalistic tendencies and often showing activity following instances of poor relations between China and another state. The groups identify targets, and disseminate attack tools via their websites to ensure mass participation. Hacking groups of this kind appear to be tolerated in the People's Republic of China (PRC) as long as their activities are directed abroad. Furthermore, given the fact that it appears unlikely at present that any Chinese citizen will ever be punished for external cyber warfare activity, and the persistent rumour that the People's Liberation Army (PLA) holds an annual competition to recruit the country's best hackers,[36] the indications are that groups like the Red Hackers have at the very least a loose affiliation with the military and government.

Chinese hackers, whether government backed or not, use cyber attacks as a disruptive mechanism to further their points of view or their country's aims. In much the same way as

[33] It has also been strongly rumoured that international popularity of the Google brand has soared since the fiasco began. The timing, not far from the official launch of Bing.com, also raises the possibility that the situation was modelled or timed by Google to raise awareness of its brand and retain its global standing.

[34] Timesonline, 2010. *China returns fire against US in Google-war,* [online] published: 23 January 2010. Available at: http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article6998017.ece [accessed: 28 January 2010].

[35] BBC, 2010. *Google phases out support for IE6*, [online] published: 30 January 2010. Available at: http://news.bbc.co.uk/1/hi/8488751.stm [accessed: 21 February 2010].

[36] Michael Smith, 2009. *Spy chiefs fear Chinese cyber attack*, [online] published: March 29 2009, The Sunday Times. Available at: http://www.timesonline.co.uk/tol/news/uk/article5993156.ece [accessed: 20 November 2009].

the western world imposes economic sanctions on states which it feels are upsetting the balance, Chinese hackers aim to cause as much disruption as possible to states and other actors who appear hostile or oppose Chinese aims. China's 2006 Defence White Paper states that the PLA's intention is to build informationised armed forces "*capable of winning informationised wars by the mid-21st century*".[37] The Chinese authorities have made it clear that they consider cyberspace a strategic domain which significantly helps redress the military imbalance between China and the rest of the world (particularly the United States).[38]

Europe

UK

Concern over Chinese tactics has also been raised in the UK Government. According to The Times, Chinese hackers targeted networks at the Foreign and Commonwealth Office (FCO) and other Whitehall departments in 2007 leading to the Director-General of the Security Service (SyS), Jonathan Evans, warning over 300 British businesses that they were under threat from Chinese cyber-attack. As recently as January 2010 the warning was reiterated by SyS, with accusations of China 'bugging and burgling UK business executives'.[39] A leaked report from SyS states that undercover intelligence officers from the PLA have approached a number of UK businessmen and women at conferences and exhibits with the offer of gifts such as cameras and memory sticks, which are infected with trojans,[40] enabling the Chinese authorities to access the target's computer remotely and harvest information.[41]

Intelligence chiefs have also reportedly warned ministers that equipment installed by Huawei (a Chinese telecoms company) in BT's new £10 billion communications network "*could be used to halt critical services such as power, food, and water supplies*".[42] Huawei was apparently established with significant financial support from the Chinese state and is led by Ren Zhengfei, a former director of the telecoms research arm of the PLA.[43] Although there has been no public acknowledgement in the UK that warnings against this company have been acted on, the US government did intervene and end attempts from Huawei to merge with US company 3Com (who provide security systems for the Pentagon) stating it would not be in US national interests,[44] after a Pentagon report noted Huawei as a key part of the cyber

[37] People's Republic of China, China's National Defense in 2006, Sect. II. Available at: www.china.org.cn/english/features/book/194485.htm [accessed: 28 January 2010].

[38] Information Warfare Monitor, 2009. *Tracking GhostNet: Investigating a Cyber Espionage Network*, [online] published: 29 March 2009. Available at: http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network [accessed: 23 November 2009].

[39] David Leppard, 2010. *China bugs and burgles Britain* [online] published: 31 January 2010, The Sunday Times. Available at: http://www.timesonline.co.uk/tol/news/uk/crime/article7009749.ece [accessed: 3 January 2010].

[40] "Trojan" refers to malware disguised as an innocuous program or file in order to induce the target to install or activate it on their computer, thus infecting the computer in order to, among other uses, allow a hacker remote access to the system.

[41] David Leppard, 2010. *China bugs and burgles Britain* [online] published: 31 January 2010, The Sunday Times. Available at: http://www.timesonline.co.uk/tol/news/uk/crime/article7009749.ece [accessed: 3 January 2010].

[42] Michael Smith, 2009. *Spy chiefs fear Chinese cyber attack*, [online] published: March 29 2009, The Sunday Times. Available at: http://www.timesonline.co.uk/tol/news/uk/article5993156.ece [accessed: 20 November 2009].

[43] Michael Smith, 2009. *Spy chiefs fear Chinese cyber attack*, [online] published: March 29 2009, The Sunday Times. Available at: http://www.timesonline.co.uk/tol/news/uk/article5993156.ece [accessed: 20 November 2009].

[44] India is another state that has been dubious of Huawei's attempted global expansions. In 2005 concerns arose in India during Huawei's endeavour to invest $60 million into its telecoms system. Once again government intervention led to the abandonment of the plans on national security grounds.

threat from China and highlighting its special relationship with the PLA. Accusations of misdemeanours from Huawei are nothing new: in 2003 they were indicted for stealing commercial secrets from US counterpart Cisco Systems. As recently as July 2010 Huawei failed to reach an agreement to buy 2Wire and Motorola's wireless equipment unit, even though the company is said to have offered over $100 million more than its rivals, due to the sellers concerns of Huawei's ability to gain US government approval to purchase the companies.[45]

Of particular concern is the fact that the contract for the UK governments' National Resilience Extranet (NRE) which has been rolled out slowly since January 2010, was won by BT as a prime contractor, in conjunction with Datel Ultra Electronics – opening the probability that the NRE will use infrastructure provided by Huawei. The NRE is due to assist the fire, rescue and other emergency services in sharing information and communicating during crises. It is expected to link more than 1,000 organisations, including emergency services, government departments, agencies and other key organisations. Its aim is not only to provide collaboration across the blue-light services and beyond, but also to allow sharing of restricted documents and information. Passing information of this kind, as well as critical operational or confidential personal data, across systems constructed by a PLA-sponsored organisation carries a clear risk of compromise, interference or theft – or indeed the potential for the NRE to be disabled on demand, creating havoc and further confusion in a crisis.[46]

Poland

In March 2010 a number of Polish ministerial officials received an email entitled 'the annual Cyber Security meeting April 05-08' which appeared to be sent from the Estonian Defence Ministry. The email seemed credible, professional, and given the fact that NATO's Cyber Defence Centre is located in Tallinn, Estonia, no eyebrows were raised. When opened, a PDF file attached to the message infected the officials' computers with malware. This led Poland's Internal Security Agency (ABW) to admit that in the first quarter of 2010 alone, government institutions had been threatened by severe cyber attacks on over 40 occasions, and that over 50% of such attacks (and those of less severity) had originated from China.[47]

Belgium

The Belgian government has also warned its citizens of Chinese cyber intrusions; with Justice Minister Jo Vandeurzen announcing that intelligence services had traced a number of attacks on the government's IT infrastructure back to China.[48] According to Vandeurzen, China is especially interested in Belgium, not just because it plays host to both the headquarters of NATO and the EU, but also due to its close ties in Africa. As a former colonial power, Belgium maintains close relations with the Republic of Congo, where China has significant mineral interests.

[45] Bloomberg, 2010. *Huawei Said to Lose Out on U.S. Assets Despite Higher Offers* [online] published: August 3 2010, Bloomberg News. Available at: http://www.bloomberg.com/news/2010-08-02/huawei-said-to-be-stymied-in-purchase-of-u-s-assets-on-security-concerns.html [accessed: 3 August 2010]

[46] Conversations by author with NRE officials led the NRE to state that *"BT are the 'prime' for the contract. They don't actually do anything other than sub-contract Ultra Electronics".*

[47] BBC Monitoring: Sylwia Czubkowska , 2010. *Criminals Pretended to be Estonian Defence Ministry*, published: 29 April 2010. Dziennik Gazeta Prawna, page A9, Warsaw.

[48] NATO Parlialmentary Assembley, 2009. *NATO and Cyber Defence*, [online]. Available at: http://www.nato-pa.int/default.asp?SHORTCUT=1782 [accessed: 12 January 2010].

US

American Conspiracy?

It is taken as read among officials and experts that hackers in China, some of which are to varying extents sponsored by the communist government and military, are engaged in aggressive attacks against the United States.[49] According to Kevin Coleman, a private security specialist and advisor to the US government on cyber security, the introduction of China's rumoured secure operating system, *Kylin*, [50] has ensured from a strategic standpoint that in the well-worn phrase, '*China is playing chess while the US continues to play checkers'* in the cyber arena.[51] In 2002 a number of large scale coordinated cyber attacks, which were given the name Titan Rain, were launched by China on US military and government network systems, leading to 20 terabytes of data being downloaded.[52] The attacks targeted US defence installations, Sandia National Laboratories, DoD, and NASA among many others. According to one assessment, "*Although the majority of data appears to have been benign, its massive quantity may one day prove to include items that the US deems classified at a later date. These attacks could be a staging ground, testing US defences, for future operations of a more serious nature".*[53]

In 2007, the Pentagon officially admitted that a Chinese military attack on the office of Defence Secretary, Robert M. Gates, had been detected. In the same year the Pentagon reported Chinese military hackers had prepared a detailed plan to disable America's aircraft carrier fleet with a devastating cyber attack. According to the report, "*The blueprint for such an assault, drawn up by two hackers working for the People's Liberation Army (PLA), is part of an aggressive push by Beijing to achieve 'electronic dominance' over each of its global rivals by 2050, particularly the US, Britain, Russia and South Korea*."[54] This was followed in November 2007 by Chinese virtual intruders infiltrating the US Naval War College's network, forcing the college to shut down its computer systems for several weeks.[55]

Not only do cyber penetrations have the potential for severe impact on US soil, but they also contain the ability to devastatingly damage US operations overseas, as the US military relies considerably on computer networks for military equipment and intelligence gathering. In November 2009 a report to Congress by the US-China Economic and Security Review Commission established an alarming increase in incidents of Chinese computer attacks on the US government and US companies. The 2009 Report to Congress stated that:

"In May 2008, the National Journal reported that Chinese cyber attacks may have been responsible for blackouts in 2003 and 2007 in New York and Florida, respectively. Attacks on critical infrastructure could be used to gain an advantage in a time of crisis or war.

[49] Bill Gertz, 2009. *China blocks U.S from Cyber Warfare*, Washington Times [online] published: 12 May 2009. Available at: http://www.washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/ [accessed: 13 May 2009].

[50] Kylin's existence is denied by the Chinese authorities but is rumoured to be a secure operating software China has developed making its networks impenetrable.

[51] Bill Gertz, 2009. *China blocks U.S from Cyber Warfare*, Washington Times [online] published: 12 May 2009. Available at: http://www.washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/ [accessed: 13 May 2009].

[52] Ed Pilkington, 2009. *China winning cyber war Congress warned*, The Guardian 20 November 2009.

[53] Jason Fritz, 2008. *How China will use cyber warfare to leapfrog in military competitiveness*, Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies: Vol. 8: Iss. 1, Article 2. Available at: http://epublications.bond.edu.au/cm/vol8/iss1/2

[54] The Times, 2007. *China's cyber army is preparing to march on America, says Pentagon* [online] published: 8 September 2007. Available at: http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2409865.ece [accessed: 10 September 2007].

[55] Ibid.

Specifically seeking such targets is consistent with authoritative PLA writings on computer network operations''.[56]

This illustrates willingness on the part of the attackers to test the disruptive potential of cyber attacks, as well as simply using them to gather information.

The report noted a significant rise in incidents of Chinese attacks and also stated that China had the intent and capability to instigate cyber attacks anywhere in the world at any given time.[57]

The Northrop Grumman report prepared in October 2009 for The US-China Economic and Security Review Commission noted the central role of the PLA in state-sponsored cyber operations. Rumours are persistent that many individuals are trained in cyber operations at Chinese military institutions, and the report noted that:

The PLA is training and equipping its force to use a variety of IW tools for intelligence gathering and to establish information dominance over its adversaries during a conflict. PLA campaign doctrine identifies the early establishment of information dominance over an enemy as one of the highest operational priorities in a conflict… The PLA is reaching out across a wide swath of Chinese civilian sector [sic] *to meet the intensive personnel requirements necessary to support its burgeoning IW capabilities, incorporating people with specialized skills from commercial industry, academia, and possibly select elements of China's hacker community.*[58]

According to James Mulvenon, a Washington-based specialist on the Chinese military, "*At a fundamental level, the Chinese view cyberwar as an overt tool of national power in a very different way from the United States… The U.S. is still uncomfortable exercising that power, but the Chinese — and the Russians — are very comfortable with the deniability and using proxies, even though the actions of those proxies could have enormous strategic consequences*."[59]

It must be noted that the Chinese government has repeatedly rejected all claims of intrusive activity,[60] announcing that there is no evidence it is behind the attacks and instead insisted that the speculation is part of a sophisticated propaganda campaign against China. In response to the November 2009 Report to Congress by the US-China Economic and Security Review Commission, Chinese Foreign Ministry spokesman Qin Gang responded that the report *"ignores the facts and is full of prejudice and ulterior motives… we advise this so-called commission not to always view China through tinted glasses".*[61] Investigators of the attacks, while rarely directly accusing the Chinese state of involvement, have little difficulty in demonstrating that the source of the attacks is physically located in China.

[56] Report to Congress of the US-China Economic and Security Review Commission, One Hundred Eleventh Congress - First Session. November 2009. p180

[57] Ibid.

[58] Northrop Grumman Corporation, ''*Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*'' (contracted research paper for the U.S.-China Economic and Security Review Commission, June 2009), pp. 7–8. Available at: http://www.uscc.gov/researchpapers/2009/NorthropGrummanlPRClCyberlPaperlFINALlApproved%20Reportl16Oct2009.pdf

[59] Simon Elegant, 2009. *Cyberwarfare: The Issue China Won't Touch*, [online] published: 18 November 2009. Available at: http://www.time.com/time/world/article/0,8599,1940009,00.html [accessed: 20 November 2009].

[60] In 2007 and 2008, China was publicly accused of hacking into government facilities by officials in Australia, France, Germany, India, Japan, New Zealand, South Korea, the US and the UK.

[61] Guardian.co.uk, 2009*. China slams US report warning of spying by Beijing,* Guardian.co.uk, 23rd November 2009. Available at: http://www.guardian.co.uk/world/feedarticle/8822569, [accessed: 12th December 2009].

‘Caught In a Cyber Bear Trap’

Joel Brenner, the former US National Counterintelligence Executive at the Office of the Director of National Intelligence, revealed that although cyber activities from China are widespread, especially "*Chinese penetrations of unclassified DoD networks*”, Brenner was considerably more concerned by the sophisticated nature of Russian attacks, which he believes are rarely discovered. This is in contrast to what he claims as the Chinese ‘relentlessness approach’, far less concerned about being implicated (as seen in the Tibetan example above) and regularly seen operating inside US electricity grids.[62] Attacks originating in Russia, like those that come from the PRC, are not purely focussed on one or two sovereign states, or in one specific format. As the following case studies highlight, attacks from Russia over the past few years have taken many different forms and affected many different states for very different reasons.

Estonia 2007

Russia’s 2007 cyber attacks on Estonia highlighted the severe incapacitating effect cyber warfare assaults against a state can provide at minimal cost. Attacks were launched on a significant number of Estonian websites in retaliation for the contentious removal of a Russian monument to Soviet soldiers in Tallinn. The relocation of the memorial led to protests by ethnic Russians in Estonia, with over one thousand people arrested, and one killed. The Estonian embassy in Moscow was besieged and the Estonian Ambassador attacked; economic sanctions from Russia followed and a Russian State Duma delegation arrived in Tallinn demanding the Estonian (democratically elected) government step down.

The fact that cyber attacks were just one of a range of pressures which the Estonian government had to deal with simultaneously illustrates a critical point: at important junctures in international conflict, cyberspace may not be the only battlefield. Estonian “cyber Tsar” Heli Tiirmaa-Klaar recounts how in the early stages of the crisis the government was preoccupied with the riots on the streets of Tallinn as the immediate and visible concern, and were less than impressed with ‘some geek coming and saying do you know we are under cyber attack as well’.

Meanwhile in cyberspace, Estonian official websites suffered a surge of Distributed Denial of Service (DDoS) attacks from large botnets,[63] jamming servers and disabling sites. In addition to attacks managed by botnets, Russian activists distributed batch files and scripts for individuals to launch their own assaults (typically unsophisticated “ping floods”) against lists of target websites and e-mail addresses.

Despite being initially less visible, the eventual effect on Estonian business and society was at least as damaging as the rioters on the streets. Estonia consciously adopted a high-tech approach to development of its post-Soviet infrastructure – for instance choosing initially not to attempt to overhaul the creaking and inadequate Soviet telephone system, but instead moving directly to mobile networks as a replacement. The country is among the closest in Europe to developing into an e-society - 98% of Estonians utilise online banking while 90% do their tax declarations online.[64] The Estonian government actively promoted research and

[62] Bill Gertz, 2009. *China blocks U.S from Cyber Warfare*, Washington Times [online] published: 12 May 2009. Available at: http://www.washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/ [accessed: 13 May 2009].

[63] Botnets are groups of computers infected with malware and remotely controlled via a command and control server by a “botherder”, who can use the botnet for a number of purposes, including DoS attacks. Typically multiple botnets are used simultaneously in an attack.

[64] Heli Tiirmaa-Klaar speaking at the IQPC Cyber Warfare 2010 Conference in London, 27-28th January 2010.

development of internet services, such as the popular communications tool Skype, an Estonian invention.

However this dependence on computer networks also presents a vulnerability, as proven by the attacks in 2007. After a few weeks of continuous virtual assault the raids abruptly ended, but not before the Estonian authorities had been forced effectively to disconnect the state from the rest of the world. The sites targeted included government websites, websites of political parties, large news organisations, major banks and specialist communication networks. The damage inflicted was estimated to have run into costs of tens of millions of euro.[65]

Estonia was limited in its capacity to counteract the threat. The attacks predominantly emanated from outside the country, inevitably leading to internet connections outside Estonia being disconnected – one symptom being Estonian nationals finding they could not use their bank cards abroad.[66] Ironically, this disconnection process, which did eventually enable normality to resume, also ensured that the Estonian media was largely unable to enlighten the rest of the world of the severity of its situation. The cyber assault led to NATO dispatching a number of its chief cyber-terrorism experts to Tallinn to assist the Estonians in shoring up their electronic defences.[67]

Although Russia's ambassador in Brussels, Vladimir Chizhov, denied any wrongdoing by the Russian authorities, it is clear that the attacks were not carried out by just a small number of unconnected individuals. Estonian officials identified one of the ringleaders of the cyber campaign, and subsequently claimed that he was connected to the Russian Security Services. It was then announced that the network addresses of some attackers belonged to the Russian presidential administration and other government agencies in Moscow. According to Silver Meikar, a member of Parliament in the governing coalition who follows information technology issues in Estonia, "*based on a wide range of conversations with people in the security agencies there are strong indications of Russian state involvement*".[68]

If the Russian state itself has not admitted responsibility (while at the same time failing to condemn the attacks), the same cannot be said of the "patriotic youth movement" Nashi. [69] Konstantin Goloskov, a Nashi militant, personally informed the Rosbalt news agency that he was involved in the attacks, while denying any and all influence from official Moscow. It must be mentioned that Estonian websites themselves were not the only sites besieged. Russian newspapers critical of the governments' handling of the controversy, along with the liberally-inclined Ekho Moskvy radio station, had their websites attacked.

[65] Simon Tisdall , 2010*. Cyber-warfare 'is growing threat,* [online] The Guardian published: 3 February 2010. Available at: http://www.guardian.co.uk/technology/2010/feb/03/cyber-warfare-growing-threat [accessed: 10 February 2010].

[66] Jason Richards, 2009. *Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security*, International Affairs Review Volume XVIII, No. 1: 2009.

[67] It has been widely reported that NATO's Combined Cyber Defence Center of Excellence was established in Tallinn as a response to the attacks; in fact plans for the CCDCOE were well in hand before May 2007.

[68] Peter Finn, 2007. *Cyber Assaults on Estonia Typify a New Battle Tactic,* Washington Post, [online] published: 19 May 2007. Available at: http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html [accessed: 10 March 2009].

[69] Nashi is a pro-Kremlin political youth movement in Russia with similar nationalistic tendencies to the Red Hackers of China. They have been accused by opposition parties in Russia of cyber spying and malicious activity. They have also been accused by the Estonian authorities of instigating the riots and looting which swept across the Estonian capital in 2007.

Georgia 2008

Cyber attacks on Georgia during the brief war with Russia in August 2008 were more sophisticated and intense than the Estonia example, suggesting a maturation of the process. They also provided the first example of cyber assaults being coordinated with traditional military action, even if not necessarily by a Russian government agency. As soon as conventional fighting had begun Russian cyber experts had created the forum StopGeorgia.ru, where visitors were able to view large lists of Georgian websites being targeted, those which had been successfully taken down, and access simple instructions and programs to download to join in the attack.[70] Unlike in the case of Estonia, instructions were freely available for taking part in attacks and penetrations using more sophisticated techniques, including SQL injections for accessing confidential information from databases held on web servers. Highly disruptive DoS attacks were repeatedly launched at Georgian newspaper websites, and the websites and email accounts of government officials.

In a further indication of the increased sophistication of the attacks, two of Georgia's highest profile hacker sites – and hence a prime locus for organising cyber resistance and counter-strike – were targeted pre-emptively.[71] Meanwhile, however, other Georgian cyber experts had learnt from Estonia in 2007 and retaliated by targeting Russian news sites, and redirecting those sites to pro-Georgian media outlets.[72]

Despite the more developed nature of the attacks on Georgia, their net effect was less dramatic. Unlike Estonia, Georgia has demonstrated a relatively slow transition to internet usage for everyday activities; so the concentrated cyber attacks "merely" disabled a few government websites, limiting Tbilisi's ability to connect with sympathisers and allies around the world,[73] but had relatively little effect on the daily life of citizens. Possibly the highest profile attack was the simple defacing of President Mikheil Saakashvili's website, placing his image alongside one of Hitler, before the site was taken down temporarily.

Besides technical elements, the most significant aspect of the Georgian cyber attacks remains that this was the first time a cyber offensive had been directly tied to conventional military attack. This will not be the last time such attacks are carried out simultaneously, using all the key advantages of cyber attack such as low cost, simplicity, popular involvement, difficulty of attribution, and the possibility of huge return on investment in the form of impact on and disruption to the target.

Cyxymu

In August 2009, shortly before the anniversary of the Georgian conflict, cyber attacks aimed at a single individual resulted in widespread disruption of internet use worldwide. A large-scale coordinated group of DDoS attacks brought down large parts of popular social networking sites Twitter, Facebook and the Russian-owned blog service LiveJournal. The

[70] Shaun Waterman, 2008. Analysis: Russia-Georgia cyberwar doubted, [online]. Available at: http://www.spacewar.com/reports/Analysis_Russia-Georgia_cyberwar_doubted_999.html [accessed: 10 September 2009].
[71] www.hacker.ge and www.warez.ge
[72] Kevin Coleman. 2008. Cyber War 2.0 – Russia V. Georgia.[online] published: 13 August 2008.Available at: http://www.defensetech.org/archives/004363.html [accessed: 10 July 2009].
[73] The effectiveness of the attacks on government communications networks was such that during the armed conflict, the Georgian Ministry of Foreign Affairs had to return to distributing communiqués and press releases by fax – as with the author's department.

attempted target, Cyxymu, is a well known blogger, who for four years had expressed severe criticism of Moscow's policies in the Caucasus region.[74]

It is believed, by Cyxymu and many Western experts, that the attacks were an attempt to suppress his blog and keep his voice from being heard. However many Russian experts are either firmly pointing the blame at patriotic youth movement Nashi, or suggesting that the attacks stemmed from Cyxymu attempting to influence the media in Georgia and the west.

While this instance also serves to demonstrate use of cyber attacks to further national political ends, unlike the two previous case studies, it can be contested that the ultimate benefactor of the cyber attacks was in fact Cyxymu and his supporters (i.e. the target). The severe global impact of the attacks on Cyxymu brought attention to him and his cause that few legitimate means could have achieved.

Kyrgyzstan

For a little under two weeks in January 2009, DoS attacks were launched against the small, under-developed Central Asian state of Kyrgyzstan. These caused major disruption to two of its four Internet Service Providers (ISPs), together accounting for more than 80% of Kyrgyzstan's bandwidth, shutting down a number of websites and making basic functions such as email all but unusable.

Kyrgyzstan hosts an American airbase near the town of Manas. On 3rd February 2009, then Kyrgyz President Kurmanbek Bakiyev announced that Manas would soon be closed, claiming that economic considerations and a negative public attitude towards the base contributed to the decision. Following the news of the airbase closure came the announcement of a new agreement between Russia and Kyrgyzstan in which Russia will donate $2 billion in loans and $150 million in financial aid.[75] It is generally accepted that the two events are connected, and that Russian financial assistance was offered on the stipulation that US forces were removed from Manas. It has also been suggested that the cyber attacks experienced in Kyrgyzstan immediately prior to this decision were in fact attempts to silence the online voice of the Kyrgyz opposition who had been very critical of the ruling government's decision.[76]

[74] The user name, Cyxymu, refers to the town of Sukhumi in the disputed Georgian region of Abkhazia, as transliterated in the "Volapük" system of representing Cyrillic characters favoured by some parts of the Russian-speaking internet community. In 2008 LiveJournal had been pressurised by the Russian authorities into removing Cyxymu's site and posts, before reinstating it seven months later in May 2009.

[75] Isabel Gorst, 2009. *Kyrgyzstan to shut US military base*, [online] published: 4 February 2009. Available at: http://www.ft.com/cms/s/0/8d9e47de-f227-11dd-9678-0000779fd2ac.html [accessed 20 March 2010].

[76] Danny Bradbury, 2009. *The Fog of Cyber War*, The Guardian, [online] published 5 February 2009. Available at: http://www.guardian.co.uk/technology/2009/feb/05/kyrgyzstan-cyberattack-internet-access [accessed: 20 March 2010].

‘A Global Issue – Not Just a Superpower Issue’

Although this paper has primarily emphasised Russian and Chinese state/non-state actors as the responsible parties in a number of highly publicised virtual attacks, the issue is actually much larger and geographically widespread.

Baidu

Baidu, Google.cn’s main competitor in China, has itself been the victim of a number of hacking attempts in early 2010. On 12th January 2010, Baidu’s site was inaccessible for over four hours, after the front page of the site was replaced by the Iranian flag, a shattered Star of David and the words ‘Iranian Cyber Army’. Although the Chinese authorities have expressed scepticism regarding the origins of the attack, Chinese hacker group the ‘Honker Union’ took the opportunity to retaliate against a number of Iranian websites by replacing pages with Chinese flags and patriotic slogans. Given current diplomatic rows between the West and China over the handling of Iran’s nuclear programmes and ambitions, many Chinese figures have remained suspicious as to whether they are attempts by the US and EU to effect a deterioration in Sino-Iranian relations. It would be unwise to assume that the attacks were the actions of the Iranian Cyber Army purely on the grounds of the claims of the attackers. In fact on 20th January 2010, Chinese news agency Xinhua reported that Baidu had filed a lawsuit against the US firm Register.com which manages its domain registration, seeking damages and accusing the firm of gross negligence. It is unclear as to precisely who has attacked whom and their reasons for doing so; but what is clear is that regardless of whether it is American/European hackers attempting to deceive in order to unsettle relations between Iran and China at grass roots level, or whether it is Iranian hackers attempting to hit their Chinese counterparts, or even Chinese hackers playing a deception game all of their own, the beauty of this virtual battleground is that the effects are instantaneous but the ambiguity can potentially last for ever.

This is not the first high profile case of the Iranian Cyber army. In December 2009 it successfully managed to redirect Twitter.com users to websites containing anti-American messages. This once again highlights the use of cyber attacks for purely political aims, separate from the already well-established concept of attacks for economic gain or direct sabotage.

Egypt/Algeria

The political motivations for cyber attack can vary widely. In a slight variation to the cases explored thus far, Egyptian and rival Algerian activists launched a number of virtual attacks on each other in October 2009 prior to a significant football World Cup qualifying match. [77] Media and government sites from both states were targeted. The tense situation between the states led to a number of riots and arrests at the game, leading to a play-off being held on neutral territory to minimise disruption. In response Algerian hackers defaced the websites of Egyptian President Hosni Mubarak and the state-run Al Ahram newspaper, triggering a number of interruptions to service.[78] Meanwhile Egyptian hackers focussed attention on the Algerian daily Echourouk El Youmi chat forum. The riots and electronic attacks led to the Egyptian government recalling its ambassador to Algeria and summoning the Algerian Ambassador in Cairo to the Egyptian Foreign Ministry for talks.

[77] In a further example of concurrent cyber and physical activity, the Algerian team bus was pelted with rocks in Cairo, and Egyptian businesses in Algiers were looted.

[78] The front page of the President’s website was changed to show this statement: “In the name of Allah, the Beneficent, the Merciful, I am KADER11000 Algerian hacker. I have successfully hacked the websites of the Egyptian newspaper Al Ahram as a response to any violation of the rights of my country and Eshorouk newspaper.”

Iraq

In the absence of a commonly agreed definition of cyber attack, a range of different types of network exploit can be found on the borderline between cyber and physical activity. In December 2009, the Wall Street Journal reported that militants in Iraq were intercepting live video feeds directly from US Predator drones, using SkyGrabber software available on the internet for as little as $26.[79] It later emerged that the video footage had not been encrypted, ensuring the debate continues whether this was in fact a 'hack' or simply 'free viewing'. The US has acknowledged its mistake, and recognised that if wireless home networks are now rarely found unencrypted, it therefore seems ludicrous that crucial operational information from US drones is not.[80] It is important to note that at no point does it seem that the drones could have been manipulated to change course; merely that the insurgents could stream live images from the drones and view what their US controllers were viewing. Nonetheless the implications for operations relying on or even just involving Predator UAVs are obvious.[81]

Israel

The Israeli Defence Force (IDF) has been extremely open in its preparations for what it describes as the 'growing cyber warfare threat'. Head of Military Intelligence Major-General Amos Yadlin stated in December 2009 that the IDF was establishing the capacity to protect networks and launch their own cyber attacks, warning of the growing threat to Israel from around the world.[82]

There is some justification for this emphatic approach, given Israel's often fractious relations with its neighbours and the rest of the world. Following the controversial Israeli boarding of aid ships destined for Gaza in May 2010, the website of the Jerusalem Post came under retaliatory virtual attack from a number of activists based around the world. The Jerusalem Post reported that thousands of abusive e-mails had been sent to staff and general enquiry addresses in attempts to crash the system. Furthermore, the Post's email spam filter had to decipher 4,000 emails in a matter of seconds, while hacks were also attempted on the firewall protecting the system.

The Jerusalem Post had earlier seen a sharp rise in hacking attempts originating in Turkey,[83] believed to be a reaction to the wider diplomatic tensions between the two. In early 2010, Israeli Deputy Foreign Minister Danny Ayalon summoned the Turkish ambassador over a new serial thriller (Valley of the Wolves) on Turkish TV depicting Mossad agents as baby snatchers – shortly after a prime-time TV show called "Ayrilik" (Farewell) on Turkish State television portrayed the IDF as deadly and homicidal. Earlier, Ankara had decided abruptly to end its annual joint air force parade with Israel in response to operations in Gaza. There is no evidence that Turkish authorities are involved in attacks on Israeli targets; but it is highly possible that an increasingly technically capable and politically interested public see use of the Internet as a means to protest and express their disaffection, while at the same time maintaining perceived anonymity.

[79] The Wall Street Journal , 2009*. Insurgents Hack U.S Drones*, [online] published 17 December 2009. Available at: http://online.wsj.com/article/SB126102247889095011.html [accessed: 12 January 2010].
[80] In private conversation with the author, it has been suggested that the decision not to encrypt was deliberate in order to favour image quality over security, given restrictions on memory and bandwidth.
[81] For instance, Scott Ruston, in a blog on Comops, highlighted the potential for such footage to be used in Information Operations against the US by intelligent insurgents linking the footage to other footage showing drones killing civilians, emphasising the narrative of evil US invaders who kills innocent Muslims.
[82] Yaakov Katz, 2009. *IDF bolstering computer defences in face of growing cyber threat*, The Jerusalem Post, 18 December 2009.
[83] The Jerusalem Post is not the only English language media site that has seen increased hacking attempts; Jerusalem Online's main page recently featured a Turkish image from the Valley of the Wolves.

Overall, a growing trend can be seen of coordination of cyber attacks with concerted action in the physical world – be it organised social unrest, as in Estonia, military action as with Georgia, or arrests and intimidation as with Rio Tinto. In each case, an overall purpose can be discerned, and a hybrid strategy perceived.

‘Global Responses’

The US has carried out a reorganisation for defending computer networks with the establishment of the National Cybersecurity Center in March 2008, and a National Cyber Investigative Joint Task Force. It has increased the scope of the US Computer Emergency Readiness Team (US-CERT), intended to provide government officials with an early warning system to gain better situational awareness, earlier identification of malicious activity and a more comprehensive network defence, and expanded its EINSTEIN Program which helps identify unusual network traffic patterns and trends which signal unauthorised network traffic so security personnel are able quickly to identify and respond to potential threats.

Similarly the government of New Zealand has created a Police National Cyber Crime Centre (NC3) which has been set up to protect New Zealanders from increasingly sophisticated online scams and provide technical investigative skills to police; as well as to liaise with its international counterparts.

Australian Attorney-General Robert McClelland launched the state’s first ever comprehensive cyber security strategy in late November 2009. The strategy presents the roles, responsibilities and policies of Australian intelligence, cyber and policing agencies to protect Australian internet users. The strategy identified that the number one priority for the Australian government was to ‘*improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest’*. Furthermore, the strategy includes the creation of a new Australian government Computer Emergency Response Team, CERT Australia, which was began operating in January 2010.

A View from the UK

The UK’s previous Labour government set a target that every home in Britain would have access to broadband internet speeds of 2 Mega bits per second (Mbps) by 2012. Prior to forming a coalition government, the Conservative party had promised to deliver speeds of 100 Mbps to the ‘majority’ of homes by 2017, paid for by the BBC licence fee and private investors. This drive for better connections also requires an awareness that the more dependent a nation state is upon virtual networks, the more vulnerabilities it exposes. Therefore as the UK’s dependence on the internet continues to increase, it is essential that new means are used to protect the public from an Estonian-type scenario .

In June 2009 former Prime Minister, Gordon Brown, presented to Parliament a Cyber Security Strategy paper which outlined the challenges to cyber security and the need to contain them. Emphasising the UK’s need for a coherent approach to cyber security, the paper signalled the creation of two departments “*that the UK needs in order to weave together new and existing work to make cyber space a safe, secure and resilient place where we can live and work in confidence”.*[84] Both organisations were established in September 2009, and were to be operational by the end of March 2010. The first unit is the Office of Cyber Security (OCS) which aims to *“provide strategic leadership for and coherence across Government. The OCS will establish and oversee a cross-government programme to address priority areas in pursuit of the UK’s strategic cyber security objectives”.* [85] The second unit is the Cyber Security Operations Centre (CSOC) which will complement and command existing groups, with the aims of actively monitoring cyber space and coordinating incident response; enabling comprehensive understanding of attacks against UK networks

[84] Cyber Security Strategy, 2009. Cabinet Office. Avaialable at: http://www.cabinetoffice.gov.uk/reports/cyber_security.aspx [accessed: 16 February 2010].
[85] Cyber Security Strategy, 2009. Cabinet Office. Avaialable at: http://www.cabinetoffice.gov.uk/reports/cyber_security.aspx [accessed: 16 February 2010].

and users; providing better advice and information about the risks to business and the public.[86]

How far the UK's new units will go to closing the gap remains to be seen. However, with a reported budget of only £130,000 for the 2009-2010 period (and only 19 staff) for the OCS, and no separate allocation for the CSOC (which in effect is an already existing department of GCHQ), it is unlikely that the units will establish a significant counter threat over and above that already in place in GCHQ. Prior to the election, these points were noted by the Conservative Party, who criticised the new units for their ability to only analyse threats instead of taking action against them and instead pledged to set up a Cyber Threat and Assessment Centre (CTAC) to function as a single reporting point for all cyber security incidents. Post-election, little has been heard of this initiative.

One positive approach that has emerged since the election is the announcement by Security Minister Baroness Neville-Jones of a national competition to find the next generation of UK cyber experts. The Cyber Security Challenge's main aim is to fill the current void in cyber experts the UK can call on.[87] The innovative approach mirrors that of the speculation surrounding Chinese competitions of the same vain. Winner's prizes include bursaries towards university and internships at premier security companies.[88]

The April 2010 joint report from Information Warfare Monitor and Shadowserver Foundation noted that cyberspace ensures "*Countries no longer have to spend billions of dollars to build globe-spanning satellites to pursue high-level intelligence gathering*".[89] Just a few months earlier the UK Ministry of Defence's Development, Concepts and Doctrine Centre (DCDC) had issued a report expressing the notion that the cyber vulnerability of potential adversaries is far less expensive to exploit than it is to wage conventional warfare – and exploitation is infinitely harder to detect and attribute.[90] The report coincided with the Defence Green Paper 2010 which also insisted that the UK would have to develop an offensive and defensive cyber capability to deter and counteract the threats.

There is growing acceptance that future defence needs and the threats we are likely to face are evolving faster than UK defence and security thinking, and that the wars and confrontations of the future require a fundamentally new approach to training and equipping the Armed Forces.[91] As stated by Chief of the General Staff General Sir David Richards in January 2010:

"Defence must respond to the new strategic, and indeed economic, environment by ensuring much more ruthlessly that our armed forces are appropriate and relevant to the context in which they will operate rather than the one they might have expected to fight in in previous

[86] Cyber Security Strategy, 2009. Cabinet Office. Avaialable at: http://www.cabinetoffice.gov.uk/reports/cyber_security.aspx [accessed: 16 February 2010].
[87] BBC, 2010. *UK seeks next generation of cyber security specialists*, 26 July 2010 [online] Availabe at: http://www.bbc.co.uk/news/technology-10742588 [accessed: 28 July 2010].
[88] Cyber Security Challenge, 2010. Available at: https://cybersecuritychallenge.org.uk/ [accessed: 3 August 2010].
[89] Information Warfare Monitor & Shadowserver Foundation, 2010. *Shadows in the cloud: Investigating Cyber Espionage 2.0*, [online] published 6 April 2010. Available at: http://www.nartv.org/mirror/shadows-in-the-cloud.pdf [accessed: 10 April 2010].
[90] DCDC, 2010. *Global Strategic Trends – out to 2040,* fourth edition. Available at: http://www.mod.uk/NR/rdonlyres/D70F2CC7-5673-43AE-BA73-1F887801266C/0/20100202GST_4_Global_Strategic_Trends_Out_to_2040UDCDCStrat_Trends_4.pdf
[91] Con Coughlin, 2010. *We must prepare for cyber conflict - but not forget wars we fight today,* The Telegraph [online] published: 5 February 2010. Available at: http://www.telegraph.co.uk/comment/columnists/concoughlin/7163435/We-must-prepare-for-cyber-conflict---but-not-forget-wars-we-fight-today.html [accessed: 16 February 2010].

eras. Too much emphasis is still placed on what Secretary Gates calls 'exquisite' and hugely expensive equipment… Having learnt the lessons taught by AQ, the Taliban and many other non-state actors, and thought how to exploit them perhaps on an 'industrial' scale, why would even a major belligerent state choose to achieve our downfall through high risk, high cost traditional means when they can plausibly achieve their aims, much more cheaply and semi-anonymously, using proxies, guerrillas, economic subterfuge and cyber warfare?"[92]

The question has already arisen in the context of Estonia of what acts constitute a cyber probe and which exploits are considered acts of war. Several years on from the clear example of Estonia, there is still no global consensus on what specifically comprises an act of war in the virtual arena – indeed in some quarters the question has been actively avoided, since to define an attack would necessarily lead to a call for action to counter it.

Estonian Defence Minister Jaak Aaviksoo highlighted implications of the 2007 attacks for European security, summarising:

"At present, NATO does not define cyber attacks as a clear military action. This means that the provisions of Article V of the North Atlantic Treaty, or, in other words collective self-defence, will not automatically be extended to the attacked country… Not a single NATO defence minister would define a cyber-attack as a clear military action at present. However, this matter needs to be resolved in the near future." [93]

Nevertheless, more than three years on, cyber attack is still a contentious issue in the development of NATO's new Strategic Concept, with experts from some member states doggedly resistant to broadening or even defining the reference in the North Atlantic Treaty to "armed attack".

But it is critical that "rules of the game" are established swiftly for cyberspace as they are for physical domains, in order to achieve clarity on what constitutes a first strike requiring a military response. This is particularly the case given another key feature of cyber attacks – the fact that unlike in the physical domains, they can be prepared and launched in extremely short timeframes and with absolutely no warning.[94]

[92] CGS General Sir David Richards at IISS, 2010. *Future Conflict and Its Prevention: People and the Information Age*. Available at: http://www.iiss.org/recent-key-addresses/general-sir-david-richards-address/ [accessed: 16 March 2010].

[93] Ian Traynor, 2007. *Russia accused of unleashing cyberwar to disable Estonia*, [online] The Guardian published: 17 May 2007. Available at: http://www.guardian.co.uk/world/2007/may/17/topstories3.russia [accessed: 10 January 2010].

[94] As the saying among informed cyber specialists goes, "That war lasted 15 seconds. You can take the rest of the day off".

Conclusion

"The People's Republic of China (PRC) may be a global power economically but its military lacks force projection beyond the Asia Pacific region. Its traditional military hardware is one to three generations behind the US and Russia. In light of these deficiencies it is probable that cyber warfare will provide China with an asymmetric advantage to deter aggression from stronger military powers as they catch up in traditional military capabilities. Cyber warfare would also allow China to leapfrog by means of technology transfer and exploiting adversary weaknesses".[95]

Cyber attacks are already an effective tool, not just for criminals, "terrorists" or small non-state groups, but also for states themselves, looking to gain advantage in a competitive and globalised world. Hans Elmar Remberg, Vice President of the German Office for the Protection of the Constitution (Germany's domestic intelligence agency) believes that "*across the world the PRC is intensively gathering political, military, corporate-strategic and scientific information in order to bridge their technological gaps as quickly as possible*".[96] However, as the case studies in this paper have shown it is not only China engaging in anti-social activities online.

It must also be noted that the Chinese themselves have become extremely suspicious of Information Warfare campaigns against them. According to Chinese officials, in November 2009 the Chinese Military Defence website was subjected to 2.3 million intrusion attempts in its first month online. There is no way of knowing how accurate this statement is but it clearly reflects concern. In January 2010 Zhou Yonglin, deputy chief of the operations department of China National Computer Network Emergency Response Team (CNCERT), gave an interview to Xinhua not only dismissing Google's allegations but also claiming that the country was in fact itself the world's biggest victim of cyber attacks. Furthermore, it would be naïve to assume that only China and Russia have been involved in virtual espionage. McAfee's 2009 annual report on cyber crime stipulated that at least five of the major powers in world politics are engaged in cyber war activities. McAfee even went as far as naming these states as China, France, Israel, Russia and the United States and accused them all of developing advanced offensive cyber capabilities. The recently formed Cyber Command in America, led by General Keith Alexander, has as its main task the protection of US military networks and readiness to launch offensive cyber attacks on enemies. However, it must be noted, as underlined by the Estonia case, that those most at risk from cyber warfare probes are those nations which have become most dependent on computer networks. Those less dependent have less to fear from cyber attack. As Richard Clarke, special advisor for Cyber Security to former US President George Bush, states: "*Other nations, like North Korea, have such limited cyberspace and cyber dependence that there is almost nothing to defend. America's connectivity to the rest of the world is unlimited and controlled by no plan or agency*".[97] Clark and Levin reiterate this,[98] but are positive that "*the Obama administration recognizes that the United States is utterly dependent on internet-based systems and that its*

[95] Jason Fritz, 2008. *How China will use cyber warfare to leapfrog in military competitiveness*, Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies: Vol. 8: Iss. 1, Article 2. Available at: http://epublications.bond.edu.au/cm/vol8/iss1/2

[96] Tkacik,, John J Jr. 2007. *Trojan Dragons: China's Cyber Threat*. Available at: http://www.heritage.org/Research/asiaandthepacific/bg2106.cfm [accessed: 20 March 2009].

[97] Richard Clarke, 2009. *War from Cyberspace*. The National Interest, number 104, Nov/Dec 2009. p31-36.

[98] Wesley K. Clark is a retired four-star General and was Supreme Commander of NATO from 1997 to 2000. Peter L. Levin was the founding CEO of the cybersecurity company DAFCA and is now Chief Technology Officer and Senior Adviser to the Secretary at the Department of Veterans Affairs.

information assets are therefore precariously exposed. Accordingly, it has made electronic network security a crucial defense priority".[99]

Michael Lesk of Rutgers University sums the threat up perfectly: "*on balance, the Estonian cyber war ought to be a wake-up call. Producing so much disruption for so little money has to be attractive to many groups. We know that people with evil intentions watched what happened, we can only hope that people with good intentions watched as well*".[100]

The examples in this paper highlight the necessity for the UK to invest in capability to monitor and detect hostile network activity, and to protect critical systems. The formation of the OCS and CSOC will be wasted effort without significant investment in trained and experienced personnel, not to mention unwavering political backing. Furthermore, the UK government must accept warnings from its intelligence agencies, and eschew communications infrastructure provided by organisations which appear to be closely linked with agencies of foreign governments. Therefore, the UK must follow the example of the US and India over possible mergers with Huawei and similar entities.

At the time of writing, the cyber activity associated with the 2008 war between Georgia and Russia is commonly cited as the closest the world has seen to "cyber warfare". Yet it should be emphasised that attacks on Georgia fell short of what could be called offensive operations – for instance, it would appear that critical national infrastructure was not targeted. Given the examples listed in this paper, it appears that at present states and non-state actors have been largely content with symbolic, limited or demonstrative attacks to further their political aims. However, absent this restraint, the consequences of future attacks could be far more serious than has been seen to date.

In testimony before the US Congress, experienced Pentagon cyber expert Sami Saydjari stated that a mass cyber attack could in effect leave 70% of the US without electrical power for up to six months. According to Saydjari, all major powers are "desperate" not only to find ways to defend against, but also means to produce, what he called "maximum strategic damage".[101] As the UK and other Western nations continue their drive to conduct more and more of their citizens' and their government's business online, this is a reality that must not be overlooked: vulnerabilities will only increase as dependencies do.

[99] Clark and Levin, 2009. *Securing the information highway: how to enhance the United States' electronic Defenses.* Foreign Affairs, Nov/Dec 2009.

[100] Michael Lesk, 2007. The new front line: Estonia under cyberassault, IEEE Security and Privacy, July/August 2007 (vol. 5 no. 4) pp. 76-79.

[101] The Times, 2007. *China's cyber army is preparing to march on America, says Pentagon* [online] published: 8 September 2007. Available at: http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2409865.ece [accessed: 10 September 2007].

Disclaimer

The views expressed in this paper are entirely and solely those of the author and do not necessarily reflect official thinking and policy either of Her Majesty's Government or of the Ministry of Defence.

ISBN 978-1-905962-89-1

Published By:

Defence Academy of the United Kingdom

Defence Academy of the UK
R013 Greenhill House
Shrivenham
SN6 8LA
England

Telephone: (44) 1793 785534
Fax: (44) 1793 785953
Email: Publications.hq@da.mod.uk
http://www.da.mod.uk/r-and-a-b

ISBN 978-1-905962-89-1