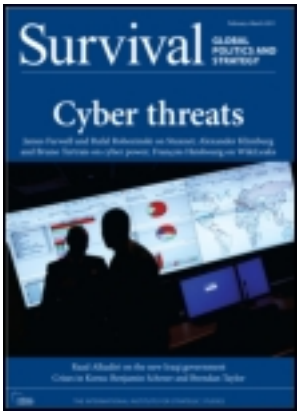

Survival
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/tsur20

Mobilising Cyber Power

Alexander Klimburg

Available online: 28 Jan 2011

To cite this article: Alexander Klimburg (2011): Mobilising Cyber Power, Survival, 53:1, 41-60

To link to this article: http://dx.doi.org/10.1080/00396338.2011.555595

Mobilising Cyber Power

Alexander Klimburg

Cyber crime, cyber terrorism and cyber warfare share a common technological basis, tools, logistics and operational methods. They can also share the same social networks and have comparable goals. The differences between these categories of cyber activity are often razor thin, or only in the eye of the beholder. From the perspective of a cyber warrior, cyber crime can offer the technical basis (software tools and logistic support) and cyber terrorism the social basis (personal networks and motivation) with which to execute attacks on the computer networks of enemy groups or nations.

An article in a Russian military journal from 2007 declared that

> isolating cyberterrorism and cybercrime from the general context of international information security is, in a sense, artificial and unsupported ... it is primarily motivation that distinguishes acts of cyberterrorism, cybercrime, and military cyberattacks … [without knowing the motivation one cannot] qualify what is going on as a criminal, terrorist or military-political act. The more so that sources of cyberattacks can be easily given a legend as criminal or terrorist actions.[1]

This reflects what has long been presumed to be a basic assumption of cyber power in Russia, China and perhaps elsewhere: non-state actors can

Alexander Klimburg is a Fellow at the Austrian Institute for International Affairs and an adviser to governments on cyber security. He is the principle author of a forthcoming European Parliament study on cyber warfare.

Survival | vol. 53 no. 1 | February–March 2011 | pp. 41–60 DOI 10.1080/00396338.2011.555595

be used by the state, overtly or covertly, to execute plausibly deniable cyber attacks.

Even with the most advanced intelligence-collecting abilities, it is unlikely that a proficient cyber attacker can be positively identified.[2] Some forms of attack are easier to attribute than others, in particular computer-network exploitation (usually computer espionage and the theft of sensitive data). As data has to be 'exfiltrated' (that is, it has to travel back to the perpetrator), such attacks are more readily traceable. This means, however, that states have an interest in maintaining or tolerating proxy organisations that could be implicated in this type of activity and other forms of attack, such as distributed denial of service, which can be conducted by an average computer user with the right tools. That these can be damaging in their own right was most famously illustrated in the purported Russia-based attacks on Estonia in 2007, which severely disrupted many Internet-based services (including e-mail and banking). Denial-of-service attacks are generally more difficult to attribute than network-exploitation attacks.[3]

Logic bombs can be massively destructive

Although data theft represents a direct threat to national security (and private business), network-exploitation attacks are also the basis for one of the most dangerous types of cyber attacks, the unnoticed planting of hidden 'logic bombs'. These hidden files or software packages are relatively small and, as they do not need to communicate, are extremely difficult to locate. Once triggered, the logic bombs can be massively destructive: in 2008, for example, a logic bomb planted by a disgruntled employee in the network of US mortgage giant Fannie Mae would have wiped out all 4,000 servers if it had been allowed to detonate.[4] A former US secretary of the Air Force and senior adviser to President Ronald Reagan has claimed that the CIA used a logic bomb in 1982 to destroy a Soviet gas pipeline. It 'was programmed to go haywire, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to the pipeline joints and welds. The result was the most monumental non-nuclear explosion and fire ever seen from space.'[5]

Less sophisticated, but more visible, denial-of-service and web-defacement attacks are undertaken by non-state groups presumably acting

with at least tacit state support. Computer-network exploitation attacks can require considerable resources, and many observers believe that the more sophisticated attacks could only be undertaken by state actors. There are, however, indications that even highly advanced espionage attacks, requiring hundreds of hours of programming and with a clear political focus, are being executed by non-state actors, albeit for the benefit of a state. For example, a noted US cyber expert argues that the Stuxnet worm, which infected computers in at least 11 countries and was apparently targeted at the Iranian nuclear programme, was created in a modular fashion – programmed in 'chunks' by teams that probably had no idea of the larger project. This was an indication that the project had been contracted out to a number of organisations involved in cyber crime.[6] As an analyst at the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn pointed out, 'if [as a nation state] you want to have this type of [plausibly deniable] cyber capability, you need to be able to accept a certain level of cyber crime'.[7]

A nation's cyber power has three dimensions: coordination of operational and policy aspects across governmental structures, coherency of policy through international alliances and legal frameworks, and cooperation of non-state cyber actors.[8] While the first two dimensions are important, the nature of cyberspace is such that a major portion of a state's cyber capabilities lies outside direct government control in the business and civil-society sectors. To create an integrated national capability in cyber power, the non-state sector must be induced to cooperate with government. For Western democracies, the most important dimension of cyber power is thus the ability to motivate and attract one's own citizens, an inward-focused soft-power approach that is fundamental for creating a 'whole of nation' cyber capability.[9]

This 'whole of nation' approach to security policy – the joint integrated application of state (whole of government) and non-state (business and civil society) efforts to attain common objectives – has only recently begun to be applied in US government circles.[10] The West, and the United States in particular, has been relatively slow to realise the importance of integrated national capabilities in cyber power. Russia and China both have highly capable and highly visible non-state cyber capabilities that interact with their

governments. Understanding how these elements are induced to support or carry out government policy is at least as important as understanding what the actual capabilities are.

Patriot hackers, netizens and the Chinese military

Chinese hackers have been behind a significant number of high-profile cyber attacks on a number of countries. The United States, nearly every EU country and probably the EU itself have experienced a Chinese cyber attack of one kind or another. Of major cyber attacks publicly reported since 1999, two-thirds or more were probably directly associated with hackers in mainland China. Most media reports point out that these attacks are probably non-governmental in nature, but often say that the hacking is officially sponsored. There is no doubt that the Chinese authorities exercise some influence over the non-state hackers. On the first anniversary of the collision of a US surveillance plane and a Chinese fighter in April 2001, the US Defense Department braced itself for a repeat of the widespread attacks launched by Chinese 'patriot hackers' that had defaced a number of US government websites the previous year. According to the Pentagon, they were prevented: 'the government of China asked them not to do that'.[11] The operative word is 'asked', not 'told': Beijing has long been concerned with its large hacker population, over which it can only exercise a limited degree of control.

The Internet and the blogosphere represent a considerable challenge to Chinese Communist Party rule. While China only has a small civil society, it does have the most active 'netizens', or participants in cyber society, in the world, as well as the greatest number of Internet users by far. According to some reports, China now has 50 million bloggers.[12] While this number can be disputed, the majority of blogs on the World Wide Web are indeed in Chinese. The Internet has achieved unparalleled importance in Chinese society, and represents one of the few outlets for dissent or free expression. Chinese bloggers can be quite militant in their views, and enjoy a wide and committed readership. But the vast majority of posts related to foreign policy or security are highly nationalistic and chauvinistic, and are usually tolerated by the government.[13] Posts on Tibet, democracy, religion and poli-

tics in general, however, tend to be taken down by the supposed 30,000 public censors within a day or two of publication. Chinese bloggers have developed a range of countermeasures to deal with the censors, including using long parables and metaphors, double entendres that play on the tonal nature of Mandarin, a growing range of technical tricks and simple guile.[14]

The central government, however, is hitting back at the very core of the blogosphere: its reputation for independence and honesty. It was recently revealed that Beijing maintained a programme to finance bloggers 'at times of public-opinion crisis'. There are reportedly as many as 30,000 such agents, all paid by the government, and apparently including some of the most well-known and trusted 'dissident' bloggers.[15] The People's Liberation Army (PLA) militia and reserve system is another important avenue for co-opting netizens. If an able-bodied male between 18 and 35 is not part of an active or reserve PLA unit, he should in theory be automatically part of a local militia.[16] Under the programme for the National Defence Reserve Forces, moreover, many of China's technical (and particularly information-technology) students are automatically considered to be part of the Chinese defence organisation.[17] Technical students are often drafted for one- to four-week training sessions to reinforce this status, and are considered to be part of the general (or ordinary) militia.

Militia units are creating information warfare units

It has been widely reported that the PLA has integrated cyber-warfare units into its standard field-army organisation from 2003 onwards.[18] The first exercises supposedly occurred as early as 1998.[19] Besides active-duty and reserve PLA units, many militia units have also announced that they are creating information warfare/operations units. The Guangzhou City militia, for example, built up a dedicated information-warfare battalion, organised around a provincial telecommunications company as a headquarters, as early as 2003. This battalion had 'computer-network-warfare' as well as 'electronic-warfare' companies, both with clearly defined and integrated computer-network attack units.[20]

It is possible for Chinese men to belong to the militia without ever having worn a military uniform. For many students in technical universities it is

a de facto condition of enrolment. Many civilian institutions, especially state-owned enterprises, have a militia role as well. What is new is that such organisations, previously paper tigers, have been given a new lease of life, becoming proficient cyber-war actors. As the Taiwanese Defence Ministry has put it, 'the PLA has established professional IO Units that … will wage information operations against its enemies with joint military and civilian participation'.[21]

The number of potential recruits for this system is staggering. In 2007, China had over 25m students in state universities, not including those in private training or specialist technical programmes.[22] Millions of information-technology personnel are employed in state-affiliated enterprises. Given these numbers, and the likely number of Chinese patriot hackers who may be part of military structures, it is not surprising that most cyber attacks on the United States come from China. The cyber-security company iDefense has tracked over 250 named hacker groups in China.[23] No more than 1,000–5,000 hackers are likely to be part of such para-governmental structures or programmes, but the informal membership could be up to ten times that figure. Many of the attacks are probably actively encouraged to distract hackers from turning their talents to more anti-state activities. Organised hacker competitions and the like are not only attempts to identify good talent, but to keep that talent safely occupied.

In support of a similar US effort to identify talent, the White House website posted the following example:

> Tan Dailin was a graduate student at Sichuan University when he was noticed (for attacking a Japanese site) by the People's Liberation Army (PLA) in the summer of 2005. He was invited to participate in a PLA-sponsored hacking contest and won. He subsequently participated in a one-month, 16-hour per day training program where he and the other students simulated various Cyber invasion methods, built dozens of hacking exploits, and developed various hacking tactics and strategies. He was chosen for the Sichuan regional team to compete against teams from Yunnan, Guizhou, Tibet, and Chongqing Military Districts. His team again ranked number one and he won a cash prize of 20,000 RMB.

> Then, under the pseudonym Wicked Rose, he formed a group called Network Crack Program Hacker (NCPH) and recruited other talented hackers from his school. He found a funding source (an unknown benefactor) and started attacking US sites. After an initial round of successful attacks, his funding was tripled. All through 2006, NCPH built sophisticated rootkits and launched a barrage of attacks against multiple US government agencies. By the end of July, 2006, NCPH had created some 35 different attack variants for one MS Office vulnerability. During the testing phase, NCPH used Word document vulnerabilities. They switched to Excel and later to PowerPoint vulnerabilities. The result of all of this activity is that the NCPH group siphoned thousands, if not millions, of unclassified US government documents back to China.[24]

Apparently, Tan Dailin's first reaction upon hearing his work had been discussed in the Western media was to ask: 'will the FBI send someone to arrest me?'[25] This statement, taken at face value, does not indicate someone who was very close to the PLA system. There are probably hundreds of such patriot-hacker groups active in China.[26] And these groups are a real threat. In 2007, the Pentagon alone had between 25 and 27 terabytes of data (over 5,000 DVDs' worth) exfiltrated.

According to an FBI expert, these groups comprise

> 25-year-olds or 17-year-olds [who] have 40-year-old fathers who happen to be working within institutions. Very often the opportunistic exploitation of a particular low-tech approach is derived through that chain, completely informally, rather than through somebody sitting in committee and deciding let's build 500 botnets that we're going to use to attack the Tibetan community.[27]

The problem for Western analysts is thus the multiple identities of Chinese actors. It is possible for an information-warfare militia unit to be, at the same time, a university IT department, an online advertising agency, an online gaming clan, a patriot-hacker team, and a local cyber-crime syndicate

engaged in software piracy. Which identity happens to be most important for an individual is dependent on circumstances.

A common interpretation of China's national cyber capability is that the Chinese Communist Party aims to be able to regularly use its netizens to attack or spy on its foreign enemies, and to use indirect control through organisational affiliation with national defence frameworks to integrate them into national policy. While elements of Chinese military doctrine can support this view, the evidence indicates a more fundamental primary objective.[28] The bulk of Chinese cyber activity is directed at internal control, either directly (through propaganda, censorship and collusion) or indirectly (through schemes designed to bind and co-opt potentially dangerous individuals, in particular netizens and patriot hackers). As with traditional informer systems found in most authoritarian states, the real targets of this system are not the people being spied upon (or, in cyberspace, being attacked). The targets are rather the spies themselves, who are thus co-opted by the state and become less likely to turn against the regime. The system puts process before outcome, or 'collection over analysis',[29] meaning that most of the large network-exploitation attacks are highly opportunistic and not really connected to the Chinese leadership's overall intelligence-gathering priorities or cyber-warfare plans. This does not mean that unofficial Chinese cyber capabilities do not directly or indirectly support the aims of the Chinese government, but for Beijing the primary aim of the integrated national capability is not offensive but defensive: an attempt at 'internal pacification' of potential subversives.

Hacker patriots, cyber crime and the *siloviki*

Russians also have been involved in hostile cyber acts. It is usually unclear whether the perpetrators are state or non-state actors; the two often work closely together. One of the earliest cyber campaigns, known as *Moonlight Maze*, occurred in 1998–2000. A large amount of confidential information was stolen from the US Department of Defense, Department of Energy, NASA, and a number of private institutions. According to some reports, the attacks were traced back to the Russian Academy of Sciences in Moscow, and were

undertaken by Russian cyber criminals, possibly with the active encouragement or even support of the Federal Security Service (FSB).[30] In 2007 and 2008 debilitating cyber attacks were launched against Estonia and Georgia. Other, less publicised attacks targeted Lithuania, Kyrgyzstan, Ukraine, Kazakhstan, the United Kingdom, the United States and other countries. In nearly all cases it is unclear whether the Russian government was involved, directly or indirectly, in the attacks.

It is certain, however, that cyber criminals played a substantial role in almost all these attacks, either tacitly as providers of logistic services, or directly, particularly by executing network-exploitation (cyber espionage) attacks. Gangs of politically motivated hackers – so-called 'hacker patriots' – also played significant roles. In both cases there are strong connections to the Russian security services, and to the Kremlin. Former members of the security services, known as the *siloviki,* have steadily gained influence within the Russian government, a process that corresponded with the rise of Vladimir Putin.[31] In 2006 it was reported that up to 78% of 1,016 leading political figures in Russia had previously served in organisations affiliated with the KGB or FSB.[32] The rise of the *siloviki* marks the end of a process ongoing since the early 1990s. While the details are murky and contentious, the 1990s saw an explosion of high-level profiteering and intrigue, with a vicious power struggle between the various security services and establishment of strong links between them and criminal elements.[33] The FSB was the clear winner of this struggle.

While the FSB was on the rise, so was Russian cyber crime. Many public reports have pointed to the role of the Russian Business Network (RBN), described by the *Economist* as the world's foremost cyber-crime organisation, as a provider of the logistic basis for cyber attacks.[34] RBN is the only criminal organisation identified by NATO as a major threat.[35] Some 40% of global cyber crime, estimated in 2007 as worth over $100 billion, is said to be directly due to RBN.[36] It was the world's foremost spammer, child-pornography distributor and producer of malware and phishing software. It delivered these services in part through various botnets, including the world's largest (*Storm*), which in 2008 was responsible for 20% of all spam e-mail globally, and provided these and many other services to cyber crimi-

nals and hacker patriots. The network has also been accused of facilitating the attacks on Georgia in July–September 2008.[37]

The patronage of high-ranking government officials has been suspected since the start of the network. The head of RBN, 'Flyman', is said to be the nephew of a well-known politician from St Petersburg.[38] This purported family link, the fact that RBN-run Internet networks were never shut down for long, and that no members of RBN have been arrested by the Russian authorities are all indications of special treatment by the security services. Although the main RBN front organisations were supposedly shut down by Russian authorities and went largely off line in 2007, the network is said to have reconstituted abroad in a number of new organisations, and is estimated as having a yearly turnover over of over $2bn.[39] Servers and malware products associated with RBN are, however, still in use and being maintained, indicating that at least part of the network is still active.

Part of the network is still active

The amount of open activity and fierce competition in the Russian hacker scene is matched by the venality and material focus of the hackers. Many events and media outlets cater to this scene, the focus of which is, in effect, stealing from the West. Much of Russian society sees cyber crime directed towards the West as a form of gentlemen's misdemeanour, or even in heroic terms. The courts and the security services seem to echo this opinion. Individuals indicted for cyber crimes have had charges dropped, and have appeared as advisers to the Russian government.[40]

The Russian security services often attempt to co-opt or recruit cyber criminals and hacker patriots. Many of the latter operate against 'anti-Russian forces' with the support of the security services. Attacks by hacker patriots against pro-Chechen websites in 2002–04 were described by the Tomsk FSB office as not being illegal and simply an 'expression of their political position, which is worthy of respect'.[41] The Tomsk FSB office is able to draw on students from Russia's top computer-science university and has been accused of a host of activities, including instigating the theft of e-mails and other data from scientists at the University of East Anglia in 2009 to support Russia's interests at the Copenhagen climate summit that December.[42]

One example (reported by *Novaya Gazeta* in May 2008) of attempted recruitment by the security service involved Anton Moskal, who was mistakenly identified as the owner of a hacker website dedicated to attacking anti-Russian forces, and was contacted by phone by a member of Russian intelligence, calling not from the FSB directly, but from the inter-departmental National Antiterrorism Centre (NAC), which like the FSB has been actively trying to recruit hacker patriots for a number of years. The caller had little technical knowledge but tried to recruit Moskal for future 'patriotic activities'.[43]

There are indications that the security services are not the only entities trying to actively recruit hacker patriots. The Nashi and Young Guard youth groups, created by Putin's ideological chief Vladislav Surkov, have been active in recruiting technical individuals for their cause. Nashi is highly organised and modelled directly on Soviet youth movements, with the clear objective of preventing a 'colour revolution' directed against the Kremlin.[44] Konstantin Goloskov, a Nashi 'commissar' and assistant to Sergei Markov, a member of the Duma, claimed credit for organising the 2007 attacks on Estonia.[45] Markov said the attacks were 'purely a reaction from civil society ... and, incidentally, such things will happen more and more'.[46]

White hats, private business and US civil society

Most Western nations do not have Internet militias on the scale that China and Russia do, and they probably do not use cyber crime as a tool of cyber power, as there are often legal restrictions against it. But that is not to say that the liberal democracies, and the United States in particular, do not have considerable non-state national cyber capabilities. In fact, US national resources alone may dwarf all others. Mobilising these resources involves the cooperation of public-minded citizens and profit-minded companies.

Companies that are part of critical-infrastructure-protection (CIP) programmes and the defence-industrial base are marked by official links to the government security apparatus, including secure communication networks and regular exchanges of confidential information, predominantly on cyber-security threats. Critical-infrastructure protection has become an urgent priority for many Western nations, and there are a number of

programmes and systems that seek to engage the private companies responsible for such critical services as telecommunications, water, power and financial services. Under the overall frameworks of public–private partnerships, thousands of companies have entered into special trust relationships with the state. The UK maintains a dedicated organisation, the Centre for Protection of National Infrastructure, which also plays a significant role in helping defend British industry from cyber crime. There are many similar organisations throughout Europe, and the EU has declared the protection of critical infrastructure an overriding security priority.[47] With some exceptions, involvement of the private sector in these programmes is voluntary and most direct costs are borne by government. In the United States, the defence-industrial base operates closely with the federal government, sometimes taking over operational tasks even in intelligence collection. Private companies engaged directly in security and defence work can be so closely entwined with the state that, from the outside, there can be hardly any clear distinction between the two.[48] The most significant work is still done in the private sector outside these public–private exchanges, and the information- and communications-technology sector as a whole continues to be the lynchpin of cyber security.

The most important work is being done by software and hardware companies, to find bugs in their systems and deliver the relevant patches or fixes; the vast majority of attacks come through holes or mistakes in programs.[49] Dedicated security companies such as McAfee have built up considerable expertise and resources for detecting and eliminating threats on the Internet, and can be considered on the front line of the fight against cyber crime. Finally, there is the power held by system-critical companies, which has not often been tested. One example is Google's spring 2010 dispute with the Chinese government, which damaged China's image and was notable for the close cooperation between Google and the US State Department.[50] Google is certainly considered by the Chinese to be a component of US power.

Perhaps the least understood aspect of Western countries' national capabilities is the highly active civil society and the large volunteer community that, in effect, built most of the Internet. The groups behind the technical

side of the Internet are certainly not your average government committee. The Internet Engineering Task Force, for example, which has since 1986 developed many key software protocols and technical fixes that the Internet depends on, is famously anarchic, lacking official rules, membership criteria or much more than a basic organisation. In fact, the task force has no legal existence; it is part of the Internet Society, one of the founding organisations of the Internet. The members of the task force, according to one member, 'reject Kings, Presidents and voting. We believe in rough consensus and running code'.[51] The 300–1,300 software engineers who meet, usually, three times a year don't vote on proposals. Instead, they hum. Whichever group is perceived to have 'hummed louder' carries the day.[52]

Hackers are traditionally distinguished as 'white', 'grey' or 'black hats'. Black hats operate beyond the law, for purely nefarious purposes, while grey and white hats actively support cyber-security efforts. Such cyber volunteers have more than once saved the Internet from itself. In 2008, for example, 27-year-old self-employed security tester Dan Kaminsky discovered that a relatively simple design flaw in the Domain Name System, which is responsible for translating Internet Protocol address (IP) numbers into more readable website addresses, made it possible to, in effect, reroute web traffic at will, allowing him to impersonate any website (including login websites) that he chose. Instead of using his super-exploit to steal money with impunity, he embarked on a complicated and highly secretive effort to work with the top programmers in his field to find a fix for the problem – all without gaining a dollar in the process.[53] He did get a great deal of recognition from the technical community, and presumably a secure livelihood as well. Kaminsky was voted in June 2010 to be one of the world's 'seven key holders of the Internet', the ultimate back-up in case of a world-wide cyber meltdown.[54]

The Task Force is famously anarchic

Beyond such individual technological volunteerism, liberal-democratic civil society, academia and policy think tanks have been involved in cyber-security policy discussions for years and play a central role in the US government's formulation of cyber-security policy. Increasingly, specialised research groups such as the US Cyber Consequences Unit have also

become active, as have specialist political activist and lobbying groups such as the Electronic Frontier Foundation and others dedicated to specific cyber issues such as 'net neutrality'.

Finally, the collective influence of bloggers and other notable players is increasing. One increasing phenomenon is the formation of Security Trust Networks (STNs),[55] voluntary investigators that provide a function loosely located between investigative journalism and computer forensics. The impact of these networks can be considerable. *Operation Grey Goose* investigated the Georgia cyber attacks and concluded that there was a high level of circumstantial evidence pointing to involvement by the Russian security services.[56] The Information Warfare Monitor discovered an entire purported Chinese cyber-spy network (*GhostNet*) focused on the Tibetan government in exile.[57] Most recently, a volunteer group called the Cyber Security Forum Initiative investigated the Stuxnet attacks.[58] The work of these groups is mostly concentrated on attacker attribution, to lift the cyber veil the attackers hide behind. Unencumbered by the structures and concerns of governmental security services, they are able to speculate freely as to possible state involvement in the attacks – information and analysis that is often used by the media in their reports.

These groups represent perhaps the most significant weapon against state-sponsored but disguised and putatively deniable attacks. Government officials have suggested that the relative decline of overt and 'noisy' cyber attacks from Russia, and the corresponding decline of the youth-group Nashi, could be a direct result of the publicly discussed conclusions of *Grey Goose* and other Security Trust Networks.[59] As Joseph Nye has pointed out, true cyber deterrence can well rest on the soft power of reputational costs once attacks are widely publicised.[60] Although the information generated by volunteer groups is not conclusive beyond reasonable doubt, it is, at present, good enough for CNN, if not for cruise missiles.

* * *

Volunteer groups integrate (but do not subjugate) themselves into a national capacity with only personal morality as their motivation. From the point of

view of the activists and researchers who represent this capability, the world is not a complicated place. Cyber-security guru Mikko Hypponen summarised this view succinctly at a conference at the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn in 2009. 'In the end', Hypponen said, 'it is just about good versus evil'.[61] Cyber-security volunteers collaborate with state institutions for no other reason than – in specific cases, at least – they identify with the implicit or explicit aims of their governments.

Sometimes, to be sure, the moral motivations of civil-society actors may lead to activity that goes against the state's perception of its interests, as in the case of Wikileak's mass dump of US State Department cables. For an integrated national cyber capability to work, government needs to be able to trust civil society as much as civil society needs to trust government. But most people can agree on the difference between valid disclosure and transparency in the public interest and simple political voyeurism. The WikiLeaks affair may, in fact, have enhanced the respect of many civil-society actors for how parts of the US government work. As political commentator Timothy Garton Ash said, 'My personal opinion of the State Department has gone up several notches'.[62]

Many Russian and Chinese hackers will also identify with the aims of their own governments. But the risks that they might disagree vigorously, and with dangerous consequences for the regime, is one reason these governments are forced to exercise some control over these actors. If non-state cyber actors in the West are not to be co-opted through paramilitary structures (as in China) nor coerced through shadowy intelligence and criminal networks (as in Russia), they must be motivated to cooperate with government aims. Appealing to patriotism will not be sufficient; they must be able to trust their government to do the right thing. Similarly, government needs to trust these groups as well. Encouraging mutual trust is perhaps the most important element in developing an integrated national cyber capability.

Notes

1 'Russian Federation Military Policy in the Area of International Information Security: Regional Aspect', *Military Thought*, vol. 16, no. 1, January 2007.

2 There have been repeated indications that the US intelligence community in particular has developed some special methods of actor attribution. Ian Lobban, head of the UK's GCHQ, speaking at the IISS on 12 October 2010, followed US Deputy Secretary of Defense William J. Lynn in hinting attribution was sometimes possible, 'but it was very, very hard'. See http://www.gchq.gov.uk/press/cyber_iiss.html.

3 For more on the Estonian attacks see Tom Espiner, 'How Estonia's Attacks Shook the World', ZDNet, http://www.zdnet.com.au/insight/security/soa/How-Estonia-s-attacks-shook-the-world/0,139023764,339288625-3,00.htm.

4 Thomas Claburn, 'Fannie Mae Contractor Indicted for Logic Bomb', *Information Week*, 29 January 2009, http://www.informationweek.com/news/security/management/showArticle.jhtml?articleID=212903521.

5 Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War* (New York: Presidio Press, 2004), p. 269.

6 Personal communication, IISS Power in Cyberspace Workshop, London, 28 October 2010.

7 Personal communication with author.

8 These dimensions can be referred to as 'integrated government capability', 'integrated systems capability' and 'integrated national capability', respectively.

9 Cyber power has been defined as 'the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power' (Stuart H. Starr in Franklin D. Kramer, Stuart H. Starr, Larry Wentz,'Cyber power and National Security', National Defense University, 2009). Starr and colleagues, however, approach the issue primarily from a military perspective, and raise a number of yet unanswered questions. A slightly broader view was offered by Joseph Nye, who considers the most important application of soft (cyber) power to be outward-facing, influencing nations, rather than inward facing. See Joseph S. Nye, Jr, *Cyber Power* (Cambridge, MA: Belfer Center, Harvard Kennedy School, May 2010), http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

10 See 'GAO: U.S. Slow to Implement President's Cyber Security Strategy', Homeland Security News Wire, 20 October 2010, http://homelandsecuritynewswire.com/gao-us-slow-implement-presidents-cyber-security-strategy. One of the earliest mentions of the whole-of-nation approach occurred in Australia as early as 1997, in a press release announcing the Foreign and Trade Policy White Paper; see http://www.foreignminister.gov.au/releases/1997/fa106_97.html. For a more recent analysis see Anthony M. Forestier, 'Effects-Based Operations: An Underpinning Philosophy for Australia's External Security?', *Security*

Challenges, vol. 2, no. 1, 2006, pp. 1–20, http://www.securitychallenges.org.au/ArticlePDFs/vol2no1Forestier.pdf.

11 Quoted in Pamela Hess, 'China Prevented Repeat Cyber Attack on US', UPI, 29 October 2002.

12 Mike Sachoff, 'Chinese Bloggers Reach 50 Million', WebProNews, 7 January 2009, http://www.webpronews.com/topnews/2009/01/07/chinese-bloggers-reach-50-million.

13 Rebecca MacKinnon, 'China Tightens Internet Controls in the Name of Fighting Porn, Piracy, and Cybercrime', RConversation, 14 December 2009, http://rconversation.blogs.com/rconversation/2009/12/china-tightens-internet-controls-all-in-the-name-of-fighting-porn-piracy-and-cybercrime.html.

14 For examples of netizin tricks to avoid censorship, see Nigel Inkster, 'China in Cyberspace', *Survival*, vol. 52, no.4, August–September 2010, pp. 55–66.

15 Melinda Liu, 'Blog the Record Straight', Newsweek.com, 28 February 2009, http://www.newsweek.com/id/186996.

16 Military Service Law of the People's Republic of China, 1984, Article 35, available at http://www.novexcn.com/military_service_law.html.

17 See 'PLA Reserve Forces', GlobalSecurity.org, 27 April 2005, http://www.globalsecurity.org/military/world/china/pla-reserve.htm.

18 Zhou Ye, 'Jiefangjun Zixunhua budui jinnian chengjun' ('PLA Cyberwarfare Units Deployed this Yea'), Zhongguo Shibao, 15 March 2003.

19 'Information Warfare', *Daily Herald*, 20 August 2001, available at http://www.DailyHerald.com.

20 Timothy L. Thomas, 'Comparing US, Russian, and Chinese Information Operations Concepts', draft report, available at http://www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf.

21 Taiwan Ministry of National Defense, *Quadrennial Defense Review 2009*, p. 25, http://www.mnd.gov.tw/qdr/en_menu.htm.

22 '25 Million Students at University in China', *People's Daily Online*, 18 October 2007, http://english.peopledaily.com.cn/90001/90776/90881/6285275.html.

23 US–China Economic and Security Review Commission, 'China's Propaganda and Influence Operations, Its Intelligence Activities that Target the United States, and the Resulting Impacts on U.S. National Security', hearing transcript, 30 April 2009, available at http://www.uscc.gov/hearings/2009hearings/transcripts/09_04_30_trans/09_04_30_tr.

24 See 'The United States Cyber Challenge', http://www.whitehouse.gov/files/documents/cyber/The United States Cyber Challenge 1.1 (updated 5-8-09).pdf.

25 Simon Elegant, 'Enemies at the Firewall', *Time*, 6 December 2007.

26 US–China Economic and Security Review, 'China's Propaganda and Influence Operations'.

27 *Ibid*.

28 See, for example, Wei Jincheng, 'Information War: A New Form of People's War', excerpted from the Military Forum column, *Liberation Army Daily*, 25 June 1996, available at http://www.fas.org/irp/world/china/docs/iw_wei.htm; see also Liang Qiao

and Xiangsui Wang, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999); Dai Qingmin, 'On Integrating Network Warfare and Electronic Warfare', *China Military Science*, February 2002, pp. 112–17; Timothy L. Thomas, 'Chinese and American Network Warfare', *Joint Forces Quarterly*, no. 38, July 2005, pp. 76–83; Wang Pufeng 'The Challenge of Information Warfare', excerpted from *China Military Science*, Spring 1995, available at http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm.

29 US–China Economic and Security Review, 'China's Propaganda and Influence Operations'.

30 Leigh Armistead, *Information Operations: Warfare and the Hard Reality of Soft Power* (Washington DC: Brassey's, 2004).

31 R.C. Paddock, 'The KGB Rises Again in Russia', *Los Angeles Times*, 12 January 2000.

32 Evgenia Albats, 'Siloviks in Power: Fears or Reality?', Interview with Olga Kryshtanovskaya, *Echo of Moscow*, 4 February 2006.

33 Mish Glenny, *McMafia: Crime Without Frontiers* (London: The Bodley Head, 2008).

34 'A Walk on the Dark Side', *Economist*, 30 August 2007, http://www.economist.com/displaystory.cfm?story_id=9723768.

35 'The (Evil) Cyber Empire', *Newsweek*, 29 December 2009, http://www.newsweek.com/2009/12/29/the-evil-cyber-empire.html.

36 Rhys Blakely, Jonathan Richards and Tony Halpin, 'Cybergang Raises Fear of New Crime Wave', *Times*, 10 November 2007, http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2844031.ece; Peter Warren, 'Hunt for Russia's Web Criminals', *Guardian*, 15 November 2007, http://www.guardian.co.uk/technology/2007/nov/15/news.crime.

37 'The Russian Business Network: Attacking Georgia and Stealing from Americans', Infragard, 2009, available at http://www.nationalstrategies.com/pdf/publicSafety_GovSec_RussianBusinessNetwork.pdf. However, other reports have indicated that the Georgian attacks were directly attributable to the Russian security services mimicking RBN networks. See, for example, *Project Grey Goose Phase II Report: The Evolving State of Cyber Warfare*, Greylogic, 20 March 2009, http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report.

38 Warren, 'Hunt for Russia's Web Criminals'.

39 Vernetti Gianmaria, 'The Power of Networking: An Insight on the Russian Business Network', *Bright*, 1 July 2010, http://flarenetwork.org/report/enquiries/article/the_power_of_networking_an_insight_on_the_russian_business_network.htm.

40 Brian Krebs, 'Following the Money: Rogue Anti-Virus Software', *Washington Post*, 31 July 2009, http://voices.washingtonpost.com/securityfix/2009/07/following_the_money_trail_of_r.html; see also the open letter from Duma Deputy I.V. Ponomarev to the Deputy Minister of Internal Affairs, available at http://krebsonsecurity.com/wp-content/uploads/2010/05/ivptrans.pdf.

41 See Paul Goble, 'FSB Encourages, Guides Russia's "Hacker-Patriots"',

Window on Eurasia, 27 May 2007, http://windowoneurasia.blogspot.com/2007/05/window-on-eurasia-fsb-encourages-guides.html.

42 See 'Inside the Mind of a Russian Hacker', BBC, 11 March 2010, http://news.bbc.co.uk/2/hi/8561910.stm; and Shaun Walker, 'Was Russian Secret Service Behind Leak of Climate Change Emails?', *Independent*, 7 December 2009, http://www.independent.co.uk/news/world/europe/was-russian-secret-service-behind-leak-of-climatechange-emails-1835502.html. The release of the e-mails was probably timed to influence the 2009 Copenhagen climate summit, and the stolen archive was disseminated by uploading to a server in Russia. The question of FSB involvement, however, is speculative.

43 See Roland Oliphant, 'Patriot Hackers', *Moscow News*, 18 August 2008, http://themoscownews.com/proetcontra/20090818/55385636.html. An older transcript of the RUNet post referred to the 'National Antiterrorism Centre' (NAC); most other sources speak of a 'National Antiterrorism Committee' (NAK) that was set up by Putin in 2006. It is unknown if the NAC refers to an operational structure within the NAK or is an intentional or unintentional misattribution.

44 Steven L. Myers, 'Youth Groups Created by Kremlin Serve Putin's Cause', *New York Times*, 8 July 2007, http://www.nytimes.com/2007/07/08/world/europe/08moscow.html.

45 Charles Clover, 'Kremlin-backed Group Behind Estonia Cyber Blitz', *Financial Times*, 11 March 2009, http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html.

46 See Robert Coalson, 'Behind The Estonia Cyberattacks', Radio Free Europe/Radio Liberty, 6 March 2009, http://www.rferl.org/Content/Behind_The_Estonia_Cyberattacks/1505613.html.

47 For an introduction to the topic, see Jacques Barrot, 'Critical Cooperation', Public Service, 2 October 2009, http://www.publicservice.co.uk/feature_story.asp?id=12759.

48 Dana Priest and William M. Arkin, 'A Hidden World, Growing Beyond Control', *Washington Post*, 19 July 2010, http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growning-beyond-control. Many of the more than 850,000 persons in the United States holding Top Secret clearance are not civil servants.

49 While most of these vulnerabilities previously discovered had been in operating systems such as Microsoft Windows, in recent years client-side applications such as Adobe Acrobat or Flash have accounted for 80% of the vulnerabilities discovered for attack purposes. See Linda McGlasson, 'New Report: Cyber Attacks Exploit 2 Vulnerabilities', Bankinfo Security, 15 September 2009, http://www.bankinfosecurity.com/articles.php?art_id=1776.

50 See, for example, Edward Wong, 'China Rebuffs Clinton on Internet Warning', *New York Times*, 22 January 2010, http://www.nytimes.com/2010/01/23/world/asia/23diplo.html.

51 Attributed to Dave Clark, for example in Paulina Borsook, 'How Anarchy

Works – On Location with the Masters of the Metaverse, the Internet Engineering Task Force', *Wired*, October 1995, http://www.wired.com/wired/archive/3.10/ietf.html.

52 See Scott Brandner, 'IETF Structures and Internet Standards Process', http://www.ietf.org/meeting/78/documents/78newcomers.pdf.

53 See Joshua Davis, 'Secret Geek A-Team Hacks Back, Defends Worldwide Web', *Wired*, 24 November 2008, http://www.wired.com/techbiz/people/magazine/16-12/ff_kaminsky.

54 More specifically, the 'seven key-holders' hold parts of the 'root' encrypted key that would be used to 're-sign' the top-level domains within the new Domain Name System Security Extensions Internet protocol system being deployed globally. See, for example, Adam Hadhazy, 'Internet "Key Holders" are Insurance Against Cyber Attack', msnbc.com, 30 July 2010, http://www.msnbc.msn.com/id/38486293/ns/technology_and_science-science/.

55 See Alexander Klimburg, 'Whole of Nation Cybersecurity', in Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underground* (Cambridge, MA: O'Reilly Media, 2009), pp. 119–21.

56 Brian Krebs, 'Report: Russian Hacker Forums Fueled Georgia Cyber Attacks', *Washington Post*, 16 October 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html.

57 See Paul Maidment, 'GhostNet in the Machine', Forbes.com, 29 March 2009, http://www.forbes.com/2009/03/29/ghostnet-computer-security-internet-technology-ghostnet.html.

58 See Peter Apps, 'Analysis – Cyber Defenders, Attackers Probe Stuxnet's Secrets', Reuters.com, 28 October 2010, http://in.reuters.com/article/idINLDE69Q1PV20101028.

59 Personal communications with US and UK government officials.

60 Nye, *Cyber Power*.

61 Mikko Hypponen, lecture at the NATO CCDCOE Conference in Tallinn, 2009.

62 Quoted in Fareek Zakaria, 'WikiLeaks Shows the Skills of U.S. Diplomats', *Time*, 2 December 2010, http://www.time.com/time/world/article/0,8599,2034284,00.html.