Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

COMMENTS AND OPINIONS

A Chinese perspective on cyber war

Li Zhang

Li Zhang is Director of the Institute of Information and Social Development Studies at the China Institutes of Contemporary International Relations (CICIR) in Beijing (a group of experts on crisis management and strategic and policy research on cyber security), and one of the co-sponsors of the Sino-US Cybersecurity Dialogue hosted by CICIR and the Center for Strategic and International Studies (CSIS) in the United States.

Keywords: cyber war, Chinese perspective, cyber power, cyber warfare, cyberspace.

The attacks on Estonian networks in April of 2007 are generally seen by Western nations as the first case of national-level cyber attacks (the impact of the attacks was mostly national, although the channel of attack may have been international). Additionally, the network attacks experienced by Georgia in August 2008 are considered the first instance of a coordinated traditional and cyber war. The United States and other Western nations regard these two cyber battles as causes for great attention and much reflection. They believe that although a 'cyber Pearl Harbor' has yet to occur, cyber warfare has now become a reality.

On 16 May 2011, the United States caused a stir with the high-profile release of its International Strategy for Cyberspace,[1] which drew a roadmap for the future of cyberspace, defined what role the United States will play, and stressed developing norms of responsible state behaviour in cyberspace. While there are various interpretations of the newly promulgated US internet strategy within the international community, there are two points that are hard to deny. First, the new strategy is very important, loaded with meaning. With this policy statement, the United States is determining the direction for the future development of

doi:10.1017/S1816383112000823

cyberspace. Second, the new strategy will not be accomplished in one fell stroke. Rather, it represents an all-out effort by the United States, over many years, to build its cyber power. Furthermore, this strategy is regarded by the United States as the foundation from which to carefully plan an inevitable outcome.

In its new strategy, the United States says it is prepared to use military force when necessary to 'respond to hostile acts in cyberspace'.[2] As this is the first time it has asserted its right of self-defence as a fundamental standard for conduct in cyberspace, the United States has thereby announced to the world its conception of cyber military strategy.

The foundation of cyber war: cyber power

Confronted with media hype over cyber warfare, China has consistently maintained a cool-headed perspective. On the one hand, China disapproves of ignorantly overplaying the significance of cyber war; on the other, it seeks to promote vigorous discussion by taking part in academic exchanges with its international counterparts. As early as 2009, scholars in both China and Japan held bilateral discussions about working together in order to research issues related to 'Hegemony in the Internet Era'. Based on the results of research done by peers in the West, they jointly proposed the concept of 'cyber power'.[3] They believe that when studying a country's ability to conduct cyber warfare, one must consider that this depends upon the country's cyber power. The term 'cyber power' comprehensively refers to a country's capability to both take action and exert influence in cyberspace. It is composed of a number of essential factors that include:

1. Internet and information technology (IT) capabilities: specifically consisting of a country's technological research and development (R&D) and innovation capabilities, its ability to promote and apply these capabilities to industry, and its ability to use these technologies to transform industries.
2. IT industry capabilities: whether a country possesses monopolistic IT industry leaders such as IBM, Microsoft, Intel, Google, or Apple. In the 1980s, these corporate giants primarily produced telecommunications equipment, semiconductors, and computers; in the 1990s, production shifted to hardware and software – including independent manufacturing of computers, mobile phones,

1 'International Strategy for Cyberspace – Prosperity, Security and Openness in a Networked World', The White House, May 2011, available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. All internet references were accessed in September 2012, unless otherwise stated.

2 *Ibid.*, p. 14.

3 In the 1990s, some scholars in the United Kingdom and United States proposed the concept of 'cyber power' or 'information power'. See Tim Jordan, *Cyberpower: The Culture and Politics of Cyberspace and the Internet*, Routledge, London/New York, 1999; Joseph S. Nye, *The Paradox of American Power: Why the World's Only Superpower Can't Go it Alone*, Oxford University Press, Oxford/New York, 2002; Franklin Kramer, Stuart Starr, and Larry K. Wentz (eds.), *Cyberpower and National Security*, National Defense University Press, Potomac Books, Washington, DC, 2009.

https://doi.org/10.1017/S1816383112000823 Published online by Cambridge University Press

and semiconductor chips. Now this industry also wants to monopolize the associated applications and services. The direction of future development is the monopolization of global information flow.

3. Internet market capabilities: this consists of the size and scale of a country's domestic internet infrastructure, the correlating degree of integration of key IT infrastructure, the number of internet users, the number of computers owned, and so on.
4. The influence of internet culture: whether or not the national language is one that is commonly used on the Internet (English or Chinese, for example), what are the website languages of choice in the country, what are the content, quantity, and quality of the country's websites, what is the level of influence of the country's websites both domestically and internationally, and so on.
5. Internet diplomacy/foreign policy capabilities: a country's bargaining power and influence in modern international internet administration organizations such as the Internet Corporation for Assigned Names and Numbers, Internet Governance Forum, and International Telecommunication Union. This factor considers the extent to which, through methods such as fighting internet crime, constructing next-generation networks, and assigning domain names, a country can use its influence to play a leading role in the international administration of the Internet.
6. Cyber military strength: a country's ability to defend key national and military IT infrastructure from attacks, and its network deterrence and offensive ability – including its ability to steal secrets and to prevent others from stealing its secrets.
7. National interest in taking part in a cyberspace strategy: it is not sufficient that a country merely possesses part or all of the capabilities listed above. In addition, a country's cyber power depends upon whether or not there exists the desire to possess and use that power. The cyberspace strategy must have theoretical guidance, behavioural norms/criteria for action, and a strategic plan.

We need only use the above-mentioned criteria to form a tentative estimate of the cyber power of the United States, China, and other great nations of the information era. It is not difficult to draw the conclusion that in cyberspace, the United States' strength is unequalled, giving it a strong position with unmatched advantages.

A sober look at cyber warfare

China's stance is that the nations of the world should cherish the value of cyberspace – the first human-made space – and should firmly oppose the militarization of the Internet. China advocates for the peaceful use of cyberspace. It maintains a position of 'no first use' of cyber-weapons, nor will it attack civilian targets. Yet, due to the complexity of the interconnected system, it is hard to draw a precise line between civilian and military networks while dual-use technology is prevailing in

https://doi.org/10.1017/S1816383112000823 Published online by Cambridge University Press

cyberspace. China's views are that the current UN Charter and the existing laws of armed conflict all apply to cyberspace – in particular the 'no use of force' and 'peaceful settlement of international disputes' imperatives, as well as the principles of distinction and proportionality in regards to the means and methods of warfare. However, the issue of how to apply *jus ad bellum* and *jus in bello* still faces intense debate.

The technological and 'virtual' qualities of the Internet are unique characteristics of an entirely new man-made space. New network-related technologies, services, and applications are constantly emerging. Therefore, many traditional social concepts and rules, as well as the current framework of international law, cannot/should not be applied in their entirety to the new world of cyberspace. Accordingly, new information and communication technologies can serve to support the establishment of new rules and concepts. Compared to other public spaces throughout history, this is unique. Human knowledge and understanding among policy-makers lags far behind technological development – even those in charge have no past template to follow. New situations and new problems constantly emerge. As a result, relevant laws are bound to continue to require readjustment. This principle applies to our management of this information society and even more so to the use of force in cyberspace.

China believes that it is possible to revise or clarify existing international rules so that they can apply to cyberspace, as well as to create new rules. Thus, although the existing laws on armed conflicts and general international principles may all apply to cyberspace, there are still many issues that need clarification, such as attribution of a cyber attack to its perpetrator and how to determine whether the damage caused was proportionate so that self-defence was legal. The international community should, therefore, revise existing laws – but it is important that this international legal framework maintains sufficient openness and flexibility. Whether addressing cyber warfare, cyber conflicts, the use of cyber weapons, cyber arms control, and the right of self-defence, or addressing network neutrality, third-party rights and responsibilities, and the obligations of non-state actors, there is only one fundamental goal: namely, to avoid the use of force or threat of force to the greatest extent possible and to prevent the outbreak of cyber warfare. The threshold for lawful use of force in the cyber domain should be high – it should not be that this concept allows for unchecked uses of cyber attacks. Otherwise, public misperceptions and irresponsible media hype will simply serve to increase erroneous judgements and distrust between countries, making the so-called 'online arms race' more fierce.

It should be noted that China itself faces serious internet threats. According to the annual report of the National Computer Network Emergency Response Technical Team Coordination Center of China (CNCERT or CNCERT/CC), the security situation of Chinese public networks and critical infrastructure is serious. Cyber attacks targeting China and initiated abroad increased significantly in the first half of 2012, mostly from the United States, Japan and South Korea.[4]

4 Available (only in Chinese) at: http://www.donews.com/net/201210/1678402.shtm.

https://doi.org/10.1017/S1816383112000823 Published online by Cambridge University Press

According to a spokesman from China's Ministry of Defence, the Ministry of Defence website and the People's Liberation Army (PLA) military networks suffered 80,000 attacks per month which were launched from outside China.[5] Nowadays, more and more phishing websites built abroad are targeting financial institutions in China. It is necessary for China to adopt defence and security measures in accordance with its national interests and security. This is an internationally accepted practice – for example, the United States, France, the United Kingdom, Korea, Japan, India, and other countries have set up Cyber Command departments, and furthermore, these countries have made no secret of their desire to enhance their cyber attack capabilities. Meanwhile, the United States, France, NATO, South Korea, and Japan have all conducted a series of network warfare exercises. Additionally, Western media speculates non-stop about the imminent outbreak of cyber war. China's own sense of crisis and insecurity in cyberspace is also growing, but the announcement of the creation of its 'online blue army' immediately provoked comments from foreign media, government officials, and scholars. Some countries in the international arena are manipulating public opinion, hoping to contain China and prevent it from building up its cyber warfare capacity. They are using China's behaviour as a pretext from which to expand their own cyber warfare capabilities.

China is aware that the United States and other Western countries are actively using defence contractors such as Lockheed Martin, Boeing, Northrop Grumman, and Raytheon for cyber-weapon development and deployment. These companies, one after another, are taking aim at the cyber weapons market. *The Financial Times* recently said that these groups of companies have formed a 'cyber-security military-industrial complex' to 'sell software to the US government that can break into and degrade or destroy an enemy's computer network, as well as programmes aimed at blocking such attacks'.[6] According to industry statistics, the cyber weapons market in the United States alone, which includes the expenditures of private companies, is worth nearly US $100 billion. In September, the United States, Australia, and New Zealand signed a new document that added cyber attacks as a specific category of conflict in their mutual defence treaty (ANZUS).[7] US officials said this was the first time a US bilateral defence treaty had formally dealt with cyber warfare. Given this serious state of affairs, China is increasingly worried about the prospects for peace in cyberspace.

5 Available (only in Chinese) at: http://www.mod.gov.cn/affair/2012-03/29/content_4354898.htm.

6 Joseph Menn, 'Defence groups turn to cybersecurity', in *The Financial Times*, 10 October 2011, available at: http://www.ft.com/intl/cms/s/0/84697a96-b834-11e0-8d23-00144feabdc0.html#axzz2BeHfWRvK.

7 'U.S., Australia to add cyber realm to defense treaty', in *Reuters*, 14 September 2011, available at: http://www.reuters.com/article/2011/09/15/us-usa-cyber-australia-idUSTRE78E05I20110915.

https://doi.org/10.1017/S1816383112000823 Published online by Cambridge University Press

Increased efforts for dialogue with other countries on cooperation in cyberspace

My personal view is that China – based upon the 'International Code of Conduct of Information Security'[8] recently proposed by itself and Russia – should further propose building a safe, reliable, fair, orderly, and peaceful cyberspace. The speech from HE Ambassador Wang Qun at the First Committee of the 66th Session of the UN General Assembly on Information and Cyberspace Security[9] last year, as well as Secretary of Treaty and Law Huang Huikang's speech at the Budapest Cyberspace Conference recently,[10] reflected a similar opinion and position on cyberspace. Although there is not yet a strategy for cyber security and cyber-related issues in China, the country's view is clear: it wants to actively contribute to developing legal rules applicable to cyberspace. So far the Chinese government has put forth some basic principles, namely:

- The principle of full respect for the rights and freedoms in cyberspace. This principle would consist in seeking to respect each country's national laws, to obtain and disseminate the right to information, and to respect other human rights and basic freedoms. At the same time, an emphasis should be placed on the fact that a country has jurisdictional rights over any domestic or foreign activity that could threaten its security. It also has administrative control over, and the right and responsibility to maintain the security of, its national cyberspace. This is to say that the traditional international norms of sovereignty, territorial integrity, and political independence should be extended into the realm of cyberspace. Personal information and privacy should also be under protection, just as in the offline world.
- The principle of balance. Technology itself is neutral; its good or evil consequences depend on the user. As a result, we must strike a balance between freedom and control, rights and obligations, and security and development. We shall aim not to hinder legitimate uses and innovation of technology, yet we shall also seek to prevent the spread of harmful information and the precipitation of a variety of incidents that may threaten national, and even international, security.
- The principle of the peaceful use of cyberspace. This principle involves protecting key global information technology infrastructures and other civilian-use information systems from being targeted; not exploiting data communication technologies, including networks, to launch attacks, commit aggression, or manufacture threats to international peace and security; ensuring the

8 Ministry of Foreign Affairs of the People's Republic of China, 'China, Russia and other countries submit the document of International Code of Conduct for Information Security to the United Nations', 19 March 2011, available at: http://www.fmprc.gov.cn/eng/zxxx/t858978.htm.

9 Speech by HE Ambassador Wang Qun at the First Committee of the 66th Session of the UN General Asssembly on Information and Cyberspace Security, New York, 20 October 2011, available at: http://www.fmprc.gov.cn/eng/wjdt/zyjh/t869580.htm.

10 See Bruce Sterling, 'Cyberspace with Chinese characteristics', in *Wired*, 8 October 2012, available at: http://www.wired.com/beyond_the_beyond/2012/10/cyberspace-with-chinese-characteristics-%E7%BD%91%E7%BB%9C%E7%A9%BA%E9%97%B4/; and

https://doi.org/10.1017/S1816383112000823 Published online by Cambridge University Press

non-proliferation of cyber weapons and related technologies while opposing the militarization of cyberspace; and asking nations, non-state actors, and even individual users to take responsibility for their behaviour on the Internet, while stopping any behaviour that threatens peace and the orderly development of cyberspace. Any disputes over the above-mentioned norms should be resolved peacefully and without the use or threat of force.

- The principle of equitable development. This includes addressing the digital divide; safeguarding the rights and interests of 'weak' countries; and opposing exploitation by those who have the technological advantage in cyberspace (leaders) – that is, those who may use international information network resources, crucial infrastructure, or core technology products and services in order to weaken other countries' independent control over information technology and services, or to threaten other countries' political, economic, and social stability.

To conclude, I would like to quote some remarks from US Vice-President Joe Biden, delivered at the London Cyberspace Conference in early November 2011: 'The Internet has become the public space of the 21st century... [I]n the next 20 years more than 5 billion people in the world will be online... And the next generation of Internet users has the potential to transform cyberspace in ways we can only imagine.... [T]he Internet is neutral. But what we do there isn't neutral...'.[11] At the same time, China also proposed that 'the world should join hands to great efforts to strengthen international exchanges and cooperation in the network area, [and] work together to build a peaceful and safe, open and orderly harmonious cyberspace'.[12] Every country has the obligation to not permit the Internet to be harmed and to not permit a cyber war to break out. How can we make the Internet more secure, more open, more trustworthy, more productive? In addition to the creation of rules and regulations, we will need patience, resolve, and outside direction – there are no shortcuts that may be used to do this.

11 Office of the Vice-President, 'VP's remarks to London Cyberspace Conference', The White House, 1 November 2011, transcript and video available at: http://www.whitehouse.gov/the-press-office/2011/11/01/vps-remarks-london-cyberspace-conference.

12 Secretary of Treaty and Law of the Ministry of Foreign Affairs Huang Huikang's speech in Budapest, available at: http://news.xinhuanet.com/tech/2012-10/05/c_113280788.htm.

https://doi.org/10.1017/S1816383112000823 Published online by Cambridge University Press