2013 5th International Conference on Cyber Conflict
K. Podins, J. Stinissen, M. Maybaum (Eds.)

Divided by a Common Language: Cyber Definitions in Chinese, Russian and English

Keir Giles
Conflict Studies Research Centre
Oxford, UK
keir.giles@conflictstudies.org.uk

William Hagestad II
Red Dragon Rising
Bayport, Minnesota USA
hagestadwt@red-dragonrising.com

Abstract: During 2012, both the US and UK have signalled increased willingness to engage with Russia and China on cyber security issues. But this engagement will be extremely difficult to achieve in the absence of commonly agreed definitions, and even concepts, for what constitutes cyber security.

Russian and Chinese doctrine and writing emphasise a very different set of security challenges to those which normally concern the US and UK. There is the additional complication of direct translations of specific terms from Russian and Chinese which resemble English-language terms, and therefore give the misleading impression of mutual understanding, while in fact referring to completely different concepts.

A number of states including Russia and China, which do not subscribe to the Euroatlantic consensus on the nature and future of cyberspace, have already achieved a commonality in their views and language; while this language sometimes has no equivalent in English and is therefore imperfectly understood.

This paper examines these distinctions, comparing and contrasting terms and concepts in English, Russian and Chinese. This will illustrate the dangers involved in attempting to reach a consensus - or at the very least confidence and security building measures - with states with widely differing views on cyber security without first establishing a baseline of common definitions. Examples will show how previous attempts at doing so have been counter-productive and set back mutual understanding.

Keywords: *Russia, China, doctrine, terminology*

1. INTRODUCTION

At the end of 2012, a series of international events brought years of private dissension over the nature and future of the Internet into very public view. At the Budapest Conference on Cyberspace in October, and the World Conference on International Telecommunications (WCIT) in Dubai, a Euroatlantic consensus on an international space for free exchange of information and views clashed with an alternative model backed by Russia, China and other states, advocating national control of information space and an entirely different approach to managing content. Debates which until that point had been conducted bilaterally or through such fora as the United Nations Group of Government Experts were aired in public, leading to at times acerbic exchanges. In Budapest, on 3-5 October, European nations stressed the human rights aspects of cybersecurity, based on their understanding of internet freedom as a fundamental right (Budapest, 2012), leading an exasperated Chinese representative to ask whether he was at a conference on cybersecurity or on human rights (Samuel, 2012). And in Dubai, a proposed new set of International Telecommunication Regulations (ITR) struggled to gain the support of many of the 151 delegate nations, after strong opposition from Euroatlantic states led by a formidable US delegation (ITU, 2012).

The failure to reach agreement on fundamental principles affecting cyberspace was indicative of the fact that despite increased willingness during 2012 by the USA, UK and other nations to engage with Russia and China on cyber security issues, this engagement remains extremely difficult in the absence of commonly agreed concepts of what constitutes cyber security.

The UK's Cyber Security Strategy, issued in November 2011, states that "we will work internationally to develop international principles or 'rules of the road' for behaviour in cyberspace (UK Government, 2012) - language not dissimilar to that used by Russia and China when proposing an "International Code of Conduct" for information security (UN, 2011). But as well documented previously (Giles, Russia's Public Stance on Cyberspace Issues, 2012) (Thomas, 2001), Russian and Chinese doctrine and writing emphasise a very different set of security challenges to those which normally concern the US and UK, a disconnect which has thus far stymied progress toward mutual understanding.

Yet even before addressing divergences in attitude and threat perception, there is the more basic problem of absence of a common terminology between the major players in cyberspace. The definitions of such terms as cyber conflict, cyber war, cyber attack, cyber weapon, etc. used by the UK, USA, Russia and China do not coincide - even where official or generally recognised definitions exist in each respective language. Furthermore, direct translations of specific terms from Russian and

Chinese which resemble English-language terms, and vice versa, can complicate matters further by giving the misleading impression of mutual understanding, while in fact referring to completely different concepts.

This paper will seek to illustrate fundamental incompatibility between terms and concepts subscribed to in these four countries, by examining a number of Russian and Chinese concepts and by including reference to and comparison with US and UK policy statements. The intention is to point to the dangers involved in attempting to reach a consensus - or at the very least confidence and security building measures - between states with widely differing views on cyber security without first establishing a baseline of common definitions, and show how at least one previous attempt at doing so has been counter-productive and set back mutual understanding.

2. A DIFFERENT VIEW

The existence of this fundamental disconnect between the Euroatlantic view of information security and the Russia and Chinese approaches has long been recognised among the expert communities dealing with both countries. In the Russian case, one main distinction is the holistic approach to information security, as opposed to a siloed focus on cyber issues. As pointed out by Tim Thomas in a 2001 comparison of Russian and US information security definitions from official sources, "Thus, differently than the U.S., Russia views both the mind and information systems as integral parts of its concept of information security." (Thomas, 2001)

More recently, this consciousness has spread beyond subject matter experts to be generally accepted by policy-makers - including public recognition by senior UK figures that the lexicon of foreign counterparts is based on a fundamentally different conceptual approach to the nature of information, and thus of information security (GSF, 2012).

3. FINDING COMMON GROUND

Initiatives seeking harmonisation between Russian and English terminology appear mainly to come from the Russian side, at least in public. At a 2007 NATO-Russia workshop aimed at developing a common vocabulary to deal with information security issues, leading security official Anatoliy Streltsov stated that Russia hopes for the "development of [a] multilingual conceptual framework that will allow both politicians and specialists working in the field[s] of legislation, law enforcement and prosecution, to have a common approach to legal regulation." (Streltsov, 2007) Yet the stated objective of this harmonisation may serve as a deterrent in some cases:

the same speaker continued that:

> "The creation of such [a] conceptual framework will contribute to forming necessary conditions for harmonizing national legislations and for developing international agreements aimed to regulate relations in the field of providing information security of a single state and [of the] international community as a whole."

- language which could have been calculated to trigger neuralgia among those states who do not subscribe to the notion of national information space, or international treaties regulating information security.

An initiative by the EastWest Institute, confusingly labelled a "Russia-US Bilateral", sought to break this deadlock by introducing "a joint effort between American and Russian experts to seek consensus definitions around three key cluster areas of cybersecurity terminology". (EWI, 2011)

This laudable effort appeared at first sight to make ground-breaking progress in establishing a baseline of common understanding. Regrettably, this progress proved illusory, since the agreed definitions in each language did not actually match up with each other, leaving each side under the impression that consensus had been achieved but in fact remaining as far apart as ever.

For example, the English-language definition of "Cyber Warfare" reads:

> *Cyber Warfare is cyber attacks that are authorized by state actors against cyber infrastructure in conjunction with a government campaign*.

Whereas the Russian version below it reads:

> *Combat actions in cyberspace are cyber attacks carried out by states, groups of states, or organised political groups, against cyber infrastructure, which are part of a military campaign*.
>
> (*Боевые действия в киберпространстве - кибератаки, проводимые государствами (группами государств, организованными политическими группами), против киберинфраструктур, и являющиеся частью военной кампании*.) (EWI, 2011)

The differences between the supposedly harmonised definitions, and their implications, are clear enough to require little further elaboration. The difference between a "government campaign" and a "military campaign" when defining warfare is problematic enough; but the mention of "organised political groups", present in one language but absent in the other, would cause serious difficulties if an attempt were made to apply it to determining whether the online activities of

Russian state-sponsored groups such as *Nashi* in fact constituted undeclared "cyber warfare".

Nevertheless, the task of finding common ground between Russian and US experts on this topic should not be underestimated. EastWest Institute's attempt in Brussels in November 2011 to follow up the initial 20 terms with a further range of agreed definitions stalled on the inability to reach a common understanding of the fundamental term "information".

4. SOURCING

If seeking to compare and baseline terminology between languages, the question arises of where precisely to seek the "official" definitions espoused by each nation. Russia's Information Security Doctrine was issued in 2000 but is still the key public document governing official information (including cyber) policy. The doctrine lists threats and challenges but avoids precise technical definitions of the key terms used (Russian Government, 2000). In this, the document is not unique to Russia: the UK Cyber Security Strategy 2011, referenced above, does precisely the same. So in some cases a direct comparison of the interpretation of key terms from foundational documents is not possible, and inferences have to be drawn from usage and second-line documentation. In fact, in the absence of officially and publicly approved definitions, allowance must be made for usage of terms remaining in flux even within individual nations - one of the immediately noticeable changes between the initial 2009 version of the UK Cyber Security Strategy and the most recent version at the time of writing, issued in November 2011, was a graduation from the phrase "cyber space" to the word "cyberspace". This, while hardly a noteworthy change in itself, was indicative of the fact that even the most basic terms have yet to evolve into a settled and universally accepted vocabulary even in individual countries.

Fortunately, there is no shortage of official pronouncements and documentation from which to derive interpretations of key terms, as well as to establish that in addition to the difficulties of mismatched interpretations, Russia, China and the Anglosphere use a number of terms which denote important information security concepts in the home language, but which simply have no easily comprehensible equivalent when translated.

In the case of Russia, it should be possible to source and interpret many of these terms from those Russian documents which are intended for international consumption, given the persistent efforts over a number of years to promote the Russian view of information security to the world and gather supporters. One source of definitions which can be treated as representing the official view is the "Draft Convention on

International Information Security", which outlines Russia's desired end state for international agreement on governance of cyberspace as a subset of information security overall (Russian Government, 2011). This document has already been analysed in detail in a joint Russian-British commentary, which noted linguistic complications in its interpretation (CSRC, 2012). The case studies below examining specific points of lexical contention will further compare individual terms from the Russian document with their Chinese and English-language equivalents, where these exist.

5. CASE STUDIES – SPECIFIC TERMS

The table below gives the English, Chinese and Russian renderings of common information security terms. Yet as can be seen from the detailed examination of each term that follows, these literal translations are potentially misleading, since the concepts and assumptions that lie behind them vary so widely.

Table I. Key Cyber Security Terms

English	Chinese	Russian
information space	信 息空間 xìnxī kōngjiān	информационное пространство *informatsionnoye prostranstvo*
information warfare	信 息战争 xìnxī zhànzhēng	информационная война *informatsionnaya voyna*
information weapon	信息武器 xìnxī wǔqì	информационное оружие *informatsionnoye oruzhiye*
information security	信息安全 xìnxī ānquán	информационная безопасность *informatsionnaya bezopasnost*
cyber warfare	網絡戰爭 wǎngluò zhànzhēng	кибервойна *kibervoyna*
cyberspace	網絡空間 wǎngluò kōngjiān	киберпространство *kiberprostranstvo*
cyber security	網絡安全 wǎngluò ānquán	кибербезопасность *kiberbezopasnost*
network warfare	網絡戰 wǎngluò zhàn	сетевая война *setevaya voyna*

A. *"INFORMATION SPACE"*

Both Russia and China refer to "information space", a concept which is much less well established in the Anglosphere. In Russia's Draft Convention, "information

space" (информационное пространство, *informatsionnoye prostranstvo*) is defined as "the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure, and information itself" – although subsequent usage within the Convention shows that this definition itself is subject to flux. In Chinese, the equivalent phrase is 信息空間, rendered in PinYin as "Xìnxī kōngjiān". The Chinese definition of this phrase includes the following: "The main function of the information space for people to acquire and process data... a new place to communicate with people and activities, it is the integration of all the world's communications networks, databases and information, forming a "landscape" huge, interconnected, with different ethnic and racial characteristics of the interaction, which is a three-dimensional space." (Wasuo, 2000)

Thus the Chinese view "information space" as a domain, or landscape, for communicating with all of the world's population. This chimes with the Russian view of this space including human information processing, in effect cognitive space. This factor is key to understanding the holistic Russian and Chinese approaches to information security as distinct from pure cybersecurity, a fundamental difference from the Euroatlantic approach to the subject. As expressed by Timothy Thomas, "differently than the U.S., Russia views both the mind and information systems as integral parts of its concept of information security... China appears more like Russia than the U.S. in its understanding of information security, with its emphasis on the mental aspect of information security and its extended use of the term itself." (Thomas, 2001)

B. *"CYBERSPACE"*

By contrast, Russian and Chinese official references to "cyberspace" occur primarily in translations of foreign texts or references to foreign approaches. According to a US military definition, "Cyberspace...is the Domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures"; and consequently, "Cyberspace Operations [is the] employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid." (US DoD, 2010) But the Russian rendering киберпространство, *kiberprostranstvo*, and the Chinese 網絡空間, Wǎngluò kōngjiān, are merely subsets of "information space" and inseparable from it, unlike in Western treatment where "cyberspace" continues in some writing to be treated almost as a separate domain. Meanwhile, the natural Chinese term which comes closest to what English-language readers might understand as "cyberspace" is 虛擬

主機 , Xūnǐ zhǔjī, which could simply be translated as virtual host – no more than the necessary components for connecting a machine to a network for the specific purposes of communicating via protocols such as HTML, email and so on.

C. *"CYBER WARFARE"*

A similar pattern pertains with the phrase "cyber warfare". Unsurprisingly, this phrase is well defined in US terminology. The Joint US Military definition for "cyber warfare" is "an armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyber attack, cyber defense, and cyber enabling actions." (US DoD, 2010) The US definition is further elaborated with defensive and offensive capabilities in the cyber warfighting domain[1] – a distinction from other areas of the information space which has yet to find expression in public Russian writing on the subject, for example.

The difficulties encountered by EastWest Institute in attempting to harmonise Russian and English definitions of "cyber warfare" have been described above. In part this derives from the fact that in Russia and China, similarly to "cyberspace", the phrase "cyber warfare" is used primarily to denote potential US and allied activity (Giles, 'Information Troops' – a Russian Cyber Command?, 2011). Russia's Draft Convention does not make any reference at all to "cyber warfare". Meanwhile China's People's Liberation Army (PLA) uses the term 網絡戰, Wǎngluò zhàn, as a necessary vocabulary item to render "cyber warfare" specifically for understanding the way the Western world defines conflict in this new domain. Operations in the cyber realm are further defined as 網絡作戰, Wǎngluò zuòzhàn, network warfare

---

[1] The Joint Terminology for Cyberspace Operations; 2010-11 defines Defensive Counter-Cyber (DCC) and Offensive Counter-Cyber (OCC) operations.
Defensive Counter-Cyber (DCC) are "All defensive countermeasures designed to detect, identify, intercept, and destroy or negate harmful activities attempting to penetrate or attack through cyberspace. DCC missions are designed to preserve friendly network integrity, availability, and security, and protect friendly cyber capabilities from attack, intrusion, or other malicious activity by pro-actively seeking, intercepting, and neutralizing adversarial cyber means which present such threats. DCC operations may include: military deception via honeypots and other operations; actions to adversely affect adversary and/ or intermediary systems engaged in a hostile act/ imminent hostile act; and redirection, deactivation, or removal of malware engaged in a hostile act/ imminent hostile act." Offensive Counter-Cyber (OCC) are "Offensive operations to destroy, disrupt, or neutralize adversary cyberspace capabilities both before and after their use against friendly forces, but as close to their source as possible. The goal of OCA operations is to prevent the employment of adversary cyberspace capabilities prior to employment. This could mean preemptive action against an adversary." The Joint U.S. Military definition of Offensive Cyberspace Operations (OCO) is "Activities that, through the use of cyberspace, actively gather information from computers, information systems, or networks, or manipulate, disrupt, deny, degrade, or destroy targeted computers, information systems, or networks. This definition includes Cyber Operational Preparation of the Environment (C-OPE), Offensive Counter-Cyber (OCC), cyber attack, and related electronic attack and space control negation."

operations, and offensively, 網絡戰攻擊, Wǎngluò zhàn gōngjí, cyber warfare attacks (Zaiyao, 2006).

In all cases, as in the case of "cyberspace" described above, the phrase "cyber warfare" in Russian and Chinese writing describes foreign concepts and activities – denoting the foreign notion that information conflict could be restricted to the cyber domain as opposed to encompassing other areas of the "information space".

D. "INFORMATION WEAPON"

"Information weapon" is another phrase which is not in common usage in the Anglosphere, but used as a current term in Russian discourse – as, for example, in a presentation by Anatoliy Streltsov to the International Information Security Research Consortium on 2 October 2012 detailing Russian proposals for confidence building measures in cyberspace, specifically:

> "The adoption [of] international legal instruments, emerging norms of international humanitarian law, international security law and law of war as they apply to the use of the 'information weapon' in interstate conflicts"

In keeping with the broader Russian understanding of "information space", the term "information weapon" has an impressively broad application. The definition given in Russia's Draft Convention – "information technology, means, and methods intended for use in information warfare" – is in fact misleading, since it appears close to the English-language concept of a cyber weapon, whereas in fact usage both in this document and elsewhere makes it very clear that "information weapons" can be used in many more domains than cyber, crucially including the human cognitive domain. For instance, only one of the three following examples maps to the concept of a cyber weapon:

> "Propaganda carried out using the mass media is the most traditional and most powerful general-purpose information weapon... Information weapons are being actively developed at the present time based on programming code... Information weapons also include means that implement technologies of zombification and psycholinguistic programming." (Fedorov & Tsigichko, 2001)

E. "INFORMATION WARFARE"

In common with "information weapons", it is crucial to understand that "information warfare" itself in Russian and Chinese usage carries meaning which is specific, broad, holistic, and not rendered by the direct translation into English.

Western definitions of "information warfare" are varied but broadly speaking semantically equivalent. One uncontroversial definition dating from the 1990s reads:

> "Information warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries." (Arquilla & Ronfeldt, 1993)

However, more recently English-language military terms and concepts for cyberspace operations have almost eclipsed mentions of "information warfare" as a whole, whose components have to be sought under the separate headings of disciplines such as psychological operations, Influence operations, strategic communications and more.

Meanwhile, Russian and Chinese writing on the subject has more explicitly retained the more holistic and integrated view of information warfare as a distinct, but unified and complete discipline – as pithily described by Sergey Rastorguyev, a Russian writer on information theory and information warfare with a useful line in animal metaphors:

> "...the tortoise never understood, and now never will, that information war is the deliberate teaching of your enemy how to remove his own shell." (Rastorguyev, 2006)

This conceptual gap has been well documented elsewhere, and is well recognised among US and UK practitioners. It is important also to recognize that discussion of the subject among Chinese and Russian military academics has a particularly long and well-established history. The basis for Chinese information warfare doctrine is derived from earlier Chinese military doctrine up to and including Sun Tzu's "Art of War" and Sun Ping's "Military Methods" in the 6th and 4th centuries BC respectively. Modern Chinese military cyber strategists use these ancient military annals as a guiding tenet for modern-day cyber and information warfare military strategy.

The evolution of Chinese information warfare in the digital age begins notably with People's Liberation Army General (PLA) Major General Wang PuFeng in 1995. General Wang is considered by many in the Western world to be the founding father of Chinese information warfare theory. At the same time, PLA Senior Colonels Wang Baocun and Li Fei of the Academy of Military Science, Beijing, were examining and studying the United States military tenets of information warfare,

including the current writings on the digitized battlefield and informatisation of the military (Baocun & Fei, 1995). The eventual result was the decision by the Central Military Commission in late 2003 on building computerized armed forces and winning the new strategic goal of information warfare (Zhuangzhi, 2012).

The early and mid 1990s also saw Russian recognition that existing concepts of information warfare needed to adjust to new digital realities. As noted by information warfare theorist Vitaliy Tsygichko and others in 1995, "the development of a [US] national, and then an international, information superhighway" would "create new conditions for the effective employment of information weapons" and furthermore that "the prototype of this superhighway already exists. That is the Internet, a worldwide association of computer networks".

Tsygichko went on to warn that:

> Although we live in an era of global information systems and we understand that economic vegetation awaits the country if it is not connected to the world information space, we must precisely imagine that Russia's participation in international telecommunications and information exchange systems is impossible without the comprehensive resolution of the problems of information security. (Smolyan, Tsygichko, & Chereshkin, 1995)

6. CHINESE AND US INFORMATION SECURITY POLICY

This last quotation reminds us that the differences in definitions and understandings of key information security and cyber warfare terms between Russian, Chinese and English are more than an academic problem presenting a stimulating translation challenge. Since they form the underpinning for entire national approaches to the subject by major players in the cyber domain, it is important to understand how they affect policy and how conceptual differences extend into distinct policy approaches. The Russian approach to information security has been described, and contrasted with the Euroatlantic view, in previous work (Giles, Russia's Public Stance on Cyberspace Issues, 2012). The following section will describe and contrast Chinese and US information security policy, in order further to illustrate the conceptual gap and consequent challenges for mutual understanding.

In 2012 the State Council of Central People's Government of the People's Republic of China mandated that the security and protection of information technology would be a national Chinese priority (Gu Fa, 2012). The State Council's information security mandate states that the Council will "vigorously promote" development of various forms of information technology while ensuring the protection and importance of information security.

The importance assigned to information security in the official view from the State Council is not that dissimilar to the situation in the United States. At the same time, the incongruence between the United States cyber security order issued by the White House (available, at the time of writing, in draft form) and that of the Chinese is actually startling when compared directly. The US Executive Order on cyber security directs all US federal entities to develop their own guidelines for cyber security to protect national critical infrastructures (US Government, 2012).

Meanwhile, China's State Council mandate reflects an overarching concern for *all* information technologies, suppliers and infrastructures both civilian and governmental, including the People's Liberation Army. The State Council proclaimed that the country will "Improve the security and management, information security and protection of key areas…" through a series of specific improvement programmes (Gu Fa, 2012).

The first mandate of improvements includes a focus on all critical information systems and infrastructure with particular attention being paid to the security of information networks. Thus in this way the State Council is giving very specific official intent, rather than guidance, to Chinese civilian and government leaders regarding what they must protect and the importance of the role this plays in the overall State Council plan. Further classifications and definitions are detailed within the critical information systems ecosystem, including but not limited to national and private telecommunications systems, radio networks, and the internet. From this overarching taxonomy the State Council further delineates required areas to be secured, including basic information networks such as energy, transportation, financial and other related industries where a cyber attack would cause a detrimental effect to the People's Republic of China's civilian economy.

The US cyber security order offers no distinction between wholesale protection of conjoined US Federal and commercial infrastructure. Indeed, businesses within the United States must rely heavily on a self-educated information security profession to protect themselves from the vagaries of attacks delivered by or through cyber means. Conversely, the People's Republic of China dictates and assigns responsibility to all levels of both governmental and commercial entities to share the duty of protecting a holistic realm of national critical infrastructure.

The Chinese State Council continues to demonstrate a national sense of ownership by providing amplifying instructions as their commander's intent for securing national information systems. The Council specifies distinct actions to be taken going so far as to personify these actions by using the pronoun 您, (Nín) which is the Mandarin formal word for "you", thus rendering them a direct order. The actions the state and commercial leaders within China are to take include, but remain not limited to, information security planning which must be coordinated and synchronised. Within the synchronised operation of security facilities, "you"

must strengthen against and prevent the impact and negative effect of cyber-attacks. Information security management must include continued implementation and improvement of information security measures such as cyber-attack defeat systems, including countering attacks from the web, hardware, and software. Increased resilience of "anti-attack", tamper-proof, "anti-virus, anti-paralysis and anti-theft capabilities" is also specified.

The second definitive State Council action mandates the strengthening of governmental and classified information security systems. This particular statement also includes further amplification regarding the use of cloud based information systems, data centre facilities, and the prohibition of unauthorised software installation. The State Council further expects the establishment of a government website set up to perform audits, monitor and report. Chinese Government agencies will reduce the number of points at which they are connected to the internet, and strengthen information security and confidentiality protection monitoring, as well as implementing "a hierarchical system of protection of classified information systems, strengthening also the review mechanism of classified information systems." (Gu Fa, 2012)

The third element of State Council combined and coordinated information security guidance addresses the protection and security of industrial control systems (ICS). ICS security and protection must be achieved and maintained at Chinese facilities involved in the nuclear, aerospace, advanced manufacturing, petroleum and petrochemical, oil and gas pipelines, power systems, transportation, and water conservancy industries, urban facilities and what the State Council refers to explicitly as "the Internet of Things applications." The State Council also mandates a digital city construction safety and management policy, including regular safety checks, security audits and risk assessments. Regulation is to be strengthened, especially on those ICS that may endanger the safety of life and public property (Gu Fa, 2012).

The fourth information security mandate concerns the safeguarding of Chinese citizens' personal information, stating that "the protection of personal information is a necessary condition for the overall welfare of the People's Republic of China in the Information Age. Geographic, demographic, legal, statistical and other basic information resources will be afforded the utmost in digital protection and management. Similarly the protection of sharing information resources and the interoperability of security information systems is paramount." Clear sensitive information protection requirements are to include the strict regulation of all Chinese businesses, institutions, in order to "protect user data and national basic data throughout the entire information network of economic activity in the People's Republic of China". In relative terms, United States federal policy on cyber security is not prescriptive on protection of personal information, simply mandating that

commercial enterprises which fail to follow basic guidelines for the protection of personal information will be penalised monetarily.

In summary the People's Republic of China takes a proactive and holistic approach, directed from above, to protecting its overall national information security including both Chinese commercial enterprises and governmental entities. In contrast, the United States by and large gives direction only to federal entities to ensure awareness on what is vulnerable to cyber-attacks. Commercial organisations in the United States are not issued prescriptive instructions on ensuring their own protection, and are subjected to relatively light touch regulation in this field, trusted to protect their own digital interests.

Besides reflecting the approaches of the respective governments to centralised versus decentralised command, this distinction in approach between the two states provides a clear illustration of another disconnect between concepts of the internet which hinders international understanding: the Euroatlantic view of a free and open space, effectively self-governed by a broad range of stakeholders, as opposed to the state-centric view espoused by Russia, China and like-minded nations where it is the national government which carries responsibility for the domestic "information space". (CSRC, 2012)

7. CONCLUSION - OPTIONS FOR PROGRESS

The "UK non-Paper on Global Cyber-Security Capacity Building" presented at the Budapest Conference on Cyberspace noted that "it is crucial to develop the capacity and trust to cooperate internationally", and included in its list of "key dynamics" and "potential ways forward" a note that:

> "our response is often limited by the legal and political boundaries of our states or the boundaries of commercial interests. In many cases, our state- or organisation-based response is insufficient to counter the threat: **effective response depends on working collectively**." [emphasis in original] (UK Government, 2012)

Yet it included no indication or suggestion of any path towards achieving a meaningful dialogue with those international actors who do not share the UK vision of cyberspace. This is an indication that although broad dialogue continues bilaterally as well as in fora like the Organisation for Security and Cooperation in Europe (OSCE) and the UN, agreement or even mutual understanding are still distant. As noted in the introduction to this paper, public exposition of the two opposing views has only properly begun in the past year. Thus, the fundamental difference between these two views is only now achieving broader recognition.

Bilateral dialogue is particularly challenging in the case of the United States and

China. Attempts at engagement by the U.S. on cyber issues have been hampered by the need to address persistent reporting, including by commercial information security firms in the U.S., that hostile activity including cyber espionage and hacking is conducted by PLA units. China calls these claims "false", "unlawful" and "without merit" (Bloomberg, 2013). Official statements by the Communist Party of China (CPC) in conjunction with the PLA claim that first, the CPC does not condone hacking of any kind, and in fact has cracked down on unlawful criminal usage of computers since the creation and implementation of its municipal cyber police (China Police); and that second, there are no information warfare units active in the PLA (Japan Times, 2013) (LeClaire, 2013). Meanwhile, any action proposed by the U.S. against China is portrayed by China as further evidence that the US is seeking global escalation of information warfare (Jian, 2013).

In some cases, venues which might provide an opportunity for engagement between the opposing views do not succeed in doing so. In advance of the Budapest conference, lists of "International Cyber Documents" and "National Cyber Strategies" were provided for reference by delegates and the public on the conference website. Significantly, these lists of official national and multilateral statements only included those documents which subscribed to the Euroatlantic view of cyberspace: documents published or endorsed by Russia, China and like-minded states were either omitted entirely, or simply not submitted by those states in the first place (Budapest, 2012). Subsequently, according to delegates, much of the Russian address to the plenary session did not survive the interpreting process and therefore was lost on non-Russian speaking attendees - just as at the preceding London Conference on Cyberspace in November 2011, where the illusion of consensus was created by key caveats being omitted from the translation of the speech by Communications Minister Igor Shchegolev.

Despite the impression created by some public statements from the US and UK, Russia and China are not isolated in their view of information security: there are a large number of other states which share their views, and their concerns over hostile content as well as hostile code. At present, given the congruence between Russian and Chinese approaches and concepts, terminology and policy, it is far easier for Russia, China and like-minded nations to find common ground than it is for English-speaking nations to engage constructively with them. Those holding an optimistic view on the prospects for relations between Russia, China and the West would argue that this process of engagement has the potential to provide opportunities for productive dialogue on other topics - especially in an environment where some representatives of Russia and the USA in particular have repeatedly voiced the desire to find any possible areas for cooperation. What is certain is that in the absence even of a mutually comprehensible lexicon for describing the concepts within information security, any potential for finding a real commonality of views on the nature and governance of cyberspace remains distant.

REFERENCES

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is Coming! *Comparative Strategy , 12* (2), 141-160.

Baocun, W., & Fei, L. (1995). *Information Warfare*. Retrieved from Federation of American Scientists: http://www.fas.org/irp/world/china/docs/iw_wang.htm

Bloomberg. (2013, March 17). *Li Rejects U.S. Hacking Allegations Against China as Groundless*. Retrieved from Bloomberg: http://www.bloomberg.com/news/2013-03-17/li-rejects-u-s-hacking-allegations-against-china-as-groundless.html

Budapest. (2012). Budapest Conference on Cyberspace. Budapest.

Budapest. (2012). *International Cyber Documents*. Retrieved from Budapest Conference on Cyberspace: http://www.cyberbudapest2012.hu/international-cyber-documents

China Police. (n.d.). *Public Information Network Security Supervision*. Retrieved from Ministry of Public Security of the People's Republic of China: http://www.mps.gov.cn/English/menu_1_4_1.htm

CSRC. (2012, April). *Russia's 'Draft Convention on International Information Security' - A Commentary*. Retrieved from Conflict Studies Research Centre: http://conflictstudies.org.uk/files/20120426_CSRC_IISI_Commentary.pdf

EWI. (2011, April). *Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations*. Retrieved from EastWest Institute: http://www.ewi.info/cybersecurity-terminology-foundations

Fedorov, & Tsigichko. (2001). *Information Challenges to National and International Security*. Moscow: PIR Centre.

Giles, K. (2011). 'Information Troops' – a Russian Cyber Command? Tallinn: CCDCOE.

Giles, K. (2012). Russia's Public Stance on Cyberspace Issues. Tallinn: CCDCOE.

GSF. (2012, November 21). Cyber Security: Meeting The Challenges, Combating The Threats? *Global Strategy Forum seminar*. London.

Gu Fa. (2012). *State Council vigorously promotes the development of information technology and to effectively protect the information security*. Retrieved from http://www.gov.cn/zwgk/2012-07/17/content_2184979.htm

ITU. (2012, December 14). *New global telecoms treaty agreed in Dubai*. Retrieved from http://www.itu.int/net/pressoffice/press_releases/2012/92.aspx#.UOse-G9WySo

Japan Times. (2013, March 10). *China foreign minister denies hacking claims*. Retrieved from Japan Times: http://www.japantimes.co.jp/news/2013/03/10/asia-pacific/china-foreign-minister-denies-hacking-claims

Jian, Y. (2013, March 8). *Yang Jian: the United is promoting global "network arms race"*. Retrieved from People's Daily: http://military.people.com.cn/n/2013/0308/c1011-20718565.html

LeClaire, J. (2013, February 20). *China Denies Its Army Is Behind Hack Attacks*. Retrieved from Newsfactor: http://www.newsfactor.com/story.xhtml?story_id=111003TU8EJ9

Rastorguyev, S. (2006). *Information War. Problems and Models*. Moscow.

Russian Government. (2011, October 28). *Draft Convention on International Information Security*. Retrieved from Embassy of Russia to the UK: http://rusemb.org.uk/policycontact/52

Russian Government. (2000, September 9). *Information Security Doctrine of the Russian Federation*. Retrieved from Russian Ministry of Foreign Affairs: http://www.mid.ru/ns-osndoc.

nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b?OpenDocument

Samuel, C. (2012, October 11). *Some takeaways from the Budapest Conference on Cyberspace.* Retrieved from Institute for Defence Studies and Analyses: http://www.idsa.in/idsacomments/SometakeawaysfromtheBudapestConferenceonCyberspace_csamuel_111012

Smolyan, G., Tsygichko, V., & Chereshkin, D. (1995, November 18). A Weapon That May Be More Dangerous Than a Nuclear Weapon: The Realities of Information Warfare. *Nezavisimoye voyennoye obozreniye* .

Streltsov, A. A. (2007). Legal Groundwork for Information Security and Conceptual Framework. In J. van Knop, *A Process for Developing a Common Vocabulary in the Information Security Area.* IOS Press.

T'ung, M. T. (1967). On Protracted War. In *Selected Works of Mao Tse-tung* (pp. 113-114). Peking: Foreign Languages Press.

Thomas, T. L. (2001, July). *Information Security Thinking: A Comparison Of U.S., Russian, And Chinese Concepts.* Retrieved from Foreign Military Studies Office: http://fmso.leavenworth.army.mil/documents/infosecu.htm

UK Government. (2012). *The UK Cyber Security Strategy - Protecting and promoting the UK in a digital world.* Retrieved from http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf

UK Government. (2012). *UK non-Paper on Global Cyber-Security Capacity Building for the Budapest Conference on Cyberspace.* Retrieved from Budapest Conference on Cyberspace: http://www.cyberbudapest2012.hu/download/f/31/00000/UK_NON_PAPER_ON_CAPACITY_BUILDING%20-%20BUDAPEST_CONFERENCE.pdf

UN. (2011). International code of conduct for information security. *Annex to the letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.*

US DoD. (2010). *Joint Terminology for Cyberspace Operations.* US Department of Defense. Memorandum For Chiefs Of The Military Services Commanders Of The Combatant Commands Directors Of The Joint Staff Directorates.

US Government. (2012, September 28). *White House Cyber-Security Order.* Retrieved from http://www.securitydefenceagenda.org/Contentnavigation/Library/Libraryoverview/tabid/1299/articleType/ArticleView/articleId/3251/categoryId/64/White-House-cybersecurity-order.aspx

Wasuo, H. B. (2000). *Information Space.* Shanghai: Translation Publishing House.

Zaiyao, H. B. (2006). Honeypot technology architecture network warfare training virtual shooting range environment. Construction of a virtual target circumstances for cyber war training by honeypot technology. *Journal Of Huazhong University Of Science And Technology (Nature Science)* .

Zhuangzhi, X. (2012, July 29). *10 years, China's national defense and army building to achieve a historic leap.* Retrieved from Xinhua News Agency: http://www.gov.cn/jrzg/2012-07/29/content_2194324.htm