Establishing norm of behavior in Cyberspace

Chunmei Kang Qiang Zhao Hao Shen
China Academy of Engineering Physics

1. Chance and challenge in the field of cyberspace

In general, cyberspace implies the vast and growing logical domain composed of public and private networks and virtually every networked device in the world. There are more than four billion digital wireless devices in the world today.[1] Individuals and communities worldwide connect, socialize, and organize themselves in and through cyberspace. From 2000 to 2010, global Internet user increased from 360 million to over 2 billion people. [2] Almost a third of the world's population uses the Internet and countless more are touched by it in their daily lives. The growth of networks supports prosperous economies and society.

Moreover, the continuing growth of networked systems, devices, and platforms means that cyberspace is embedded into an increasing number of capabilities upon which states and people rely to complete their mission. People trade goods and services in cyberspace, moving assets across the globe in seconds. In addition to facilitating trade in other sectors, cyberspace is itself a key sector of the global economy. Cyberspace has become an incubator for new forms of entrepreneurship, advances in technology, and new social networks that drive our economy and reflect our principles. Today, the society is increasingly relying on networked information systems to control critical infrastructures and communications systems essential to modern life. Critical life-sustaining infrastructures that deliver energy (electric power, oil and gas) and water, food, transportation (rail, air, merchant marine), finance and banking, information and telecommunications, public health, emergency services etc. all depend on networked information systems.

In addition to opportunities, cyberspace also brings significant challenges to our society. Today, resources for conducting harmful cyberspace attacks are widely available and inexpensive, creating a low cost of entry for any adversary. The tools and techniques developed by cyber criminals are increasing in sophistication at an incredible rate, and many of these capabilities can be purchased cheaply on the Internet. Well-planned attacks on key nodes of the cyberspace infrastructure have the potential to produce network collapse and cascading effects that can severely affect critical infrastructures locally, nationally, or possibly globally. Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to Nation's critical infrastructures, economy, or national security. Many state' networks and information infrastructure that these states depend on for their operations suffer from exploiting, penetrating, disrupting, degrading and sabotage from states and non-state actors. Potential cyber attacks include:

- Theft or exploitation of data. Successful penetrations would lead to the loss of thousands of files from networks;

- Disruption or denial of access or service that affects the availability of networks, information, or network-enabled resources. Given the integrated nature of cyberspace, computer-induced failures of power grids, transportation networks, or financial systems could cause massive physical damage and economic disruption.
- Destructive action including corruption, manipulation, or direct activity that threatens to destroy or degrade networks or connected systems.
- Anti-government activities. Some antigovernment group may make political statements, or express personal disgruntlement to their government which could be devastating to national security.

2. Challenge in cyberspace governance

Because of the global nature of cyberspace, the vulnerabilities that exist are open to the world and available to anyone, anywhere, with sufficient capability to exploit them. According to information released by China Internet Network Information center (CNNIC), Past of a years, China Internet continues to maintained fast development momentum. To the end of November 2011, Chinese Internet users has over 500 million with penetration rate of 37.7%. As network has become more and more popular in China, it has become a field with more and more importance in national security. China as a developing country is far less capable of maintaining Internet security than the developed counties, facing a much bigger threat of online attacks. In recent years, China's vulnerable network has become a victim of major overseas hacker attacks. Qian Xiaoqian who is deputy director of China Internet Information Office, pointed out on the fifth Sino-US Internet Forum that 4.5 million Chinese PCs had been attacked by Trojan viruses from IPs abroad in 2010, an increase of more than 16 times from 2009.

Information released by National Internet Emergency Center in 9th August 2011 during annual meeting of Chinese Internet Security showed that 4635 Chinese government websites were attacked last year, nearly half come from outside. In 2010, monitoring data from the state Emergency Center show that nearly 480,000 Trojans controlled terminal IP, of which 221,000 is located outside. Among them, America (14.7%) and India (8.0%) are the two biggest states the virus originated. In addition, a total of 13782 zombies network controlled terminal IP, 6531 of them located outside, the top three are the United States (21.7%), India (7.2%) and Turkey (5.7%). According to data submitted by Internet network security information member units designated by the Ministry of Industry and Information, more than half of hostile domains which implement China pages linked to horse, fishing and other malicious wrongdoing registered abroad.

This has made us realize that the inter-connectivity of information and cyber networks has contributed to making countries of the world "a community of common destiny" in which our security is inseparably linked together. From this view, Internet censorship and governance should be established gradually. We realize that "while the internet should be free, it should not be lawless," as was said by Smith who is the chairman of the *House Judiciary Committee, United States.*

During the process of facilitating and pushing application of Internet, the world's major countries has paid great attention to the governance of cyberspace and its serious impact on national security. For example, cyberspace was first treated as an independent military operation domain except for the air, land, maritime and space domains by the U.S. National Military

Strategy which was released in 2004.

We all agree that cybercrime should be inhibited and international norms and measures on cybercrime should be developed bilaterally and multilaterally, but establishing cyberspace governance is a complex issue and should be considered and discussed carefully. For example, it was thought that Domain Name System (DNS) blocking and filtering is an effective measure when we take charge of illegal sites, yet, there are technical issues need to be considered thoroughly. If Internet Service Providers (ISPs) block a Web site, it should alter records in the net's system for looking up DNS, users couldn't navigate to the site. Yet, this method require ISP introduce false information into DNS. Opponent of this measure consider this would harm the usefulness of the Domain Name System Security Extensions (DNSSEC), a set of protocols developed by the Internet Engineering Task Force (IETF) for ensuring internet security. A white paper by the Brookings Institution wrote that "The DNS system is based on trust," adding that DNSSEC was developed to prevent malicious redirection of DNS traffic, and other forms of redirection will break the assurances from this security tool, which means core internet infrastructure may be changed.

kchm 31/12/11 6:03 PM
Formatted: Font color: Auto, English (US)

kchm 31/12/11 6:03 PM
Formatted: Font color: Auto, English (US)

ISPs can also adopt method to sniff for traffic going to a blacklisted site and simply block it. Yet, this would undermine the integrity of the Domain Name System. Some technical researchers in the field of IT even call DNS blocking the end of the internet since it may limit generalization and popularity of Internet. In addition, the validity of DNS blocking was suspected. Edward J. Black, president and CEO of the Computer and Communications Industry Association, wrote in the Huffington Post that "Ironically, it would do little to stop actual pirate websites, which could simply reappear hours later under a different name, if their numeric web addresses aren't public even sooner. Anyone who knows or has that web address would still be able to reach the offending website." As the technical capability and sophistication of users is improving, some new technology may be developed for circumventing DSN blocking. It was said some US-funded "internet in a suitcase" allow users to circumvent manipulated DNS server which made the Internet governance even more difficult.

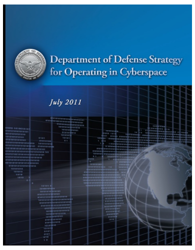
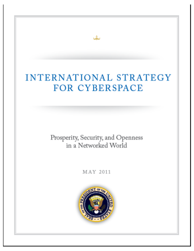
In a lawsuit judged in November 2011, both of DNS blocking methods mentioned above were applied. Luxury goods maker Chanel won court orders against hundreds of websites trafficking in counterfeit luxury goods. A federal judge in Nevada has agreed that Chanel can seize the domain names in question and transfer them all to US-based registrar GoDaddy, where they would all redirect to a page serving notice of the seizure. In addition, a total ban on search engine indexing was ordered. The judge ordered "all Internet search engines" and "all social media websites"—explicitly naming Facebook, Twitter, Google+, Bing, Yahoo, and Google—to "de-index" the domain names and to remove them from any search results. But the domain might not even be registered in the States, for instance, and the judge ban on search engine and social media indexing apparently extends to the entire world.

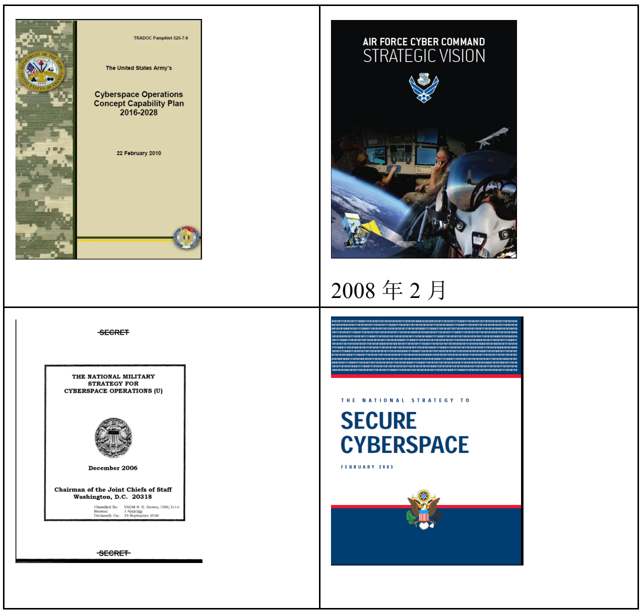
Cybercrime detection is also proved to be a challenge. Unlike cybercrimes such as child pornography which could be blocked voluntarily by media websites using methods that begin by detecting skin tones, other cybercrimes such as copyright infringement is hard to be detected. Media websites must rely on copyright holders to bring offending material to its attention. Just as the copyright lawsuit mentioned above, the luxury goods maker Chanel hired a Nevada investigator to order from three of the 228 sites in question. When the orders arrived, they were reviewed by a Chanel official and declared counterfeit. The other 225 sites were seized based on a

Chanel anti-counterfeiting specialist browsing the Web. This increases difficulties of cybercrime detection.

As the attack tools and methodologies are becoming widely available, the technical capability and sophistication of users bent on causing havoc or disruption is improving. Because of the increasing sophistication of computer attack tools, an increasing number of actors are capable of launching nationally significant assaults against critical infrastructures and cyberspace.

The conception of cyberspace operations domain makes Internet governance a more complex issue. The U.S. published several documents related to cyberspace in recent years, see Fig.2. Some of them are released by Department of defense, others by the U.S. government. What concerned us is that the U.S. Cyberspace strategy is gradually changed from strategic defensive to strategic offensive. In December 2006, Chairman of the Joint Chiefs of Staff issued "National Military Strategy for Cyberspace Operations (NMS-CO)" which is a product of significant reflection and debate within U.S. military and government. [3] NMS-CO is the US Armed Forces' comprehensive strategic approach for using cyberspace operations to assure US military strategic superiority in the domain. In the document, cyberspace is not only treated by the U.S. military as cyberspace-specific operations domain, but also for ensuring success in the other domains including air, land, maritime and space domain. It was said that "the integration of offensive and defensive cyberspace operations, coupled with the skill and knowledge of our people, is fundamental to this approach." In fact, as early as 2004, U.S. National Military Strategy pointed out that "The Armed Forces must have the ability to operate across the air, land, maritime, space and cyberspace domains of the battlespace." Here, cyberspace was first mentioned as an independent domain in the U.S. official documents. In 2010, DoD established U.S. Cyber Command (USCYBERCOM) as a sub-unified command of USSTRATCOM. The "International Strategy for Cyberspace" which was released by the U.S. government in 2011 stated the U.S. was "to build and enhance existing military alliances to confront potential threats in cyberspace".[1] The document makes explicit that a cyberattack is casus belli for a traditional act of war and the U.S. will " reserve the right to use all necessary means—diplomatic， informational， military，and economic—as appropriate and consistent with applicable international law，in order to defend our Nation， our allies， our partners， and our interests."

 Department of Defense Strategy for Operating in Cyberspace July 2011	 INTERNATIONAL STRATEGY FOR CYBERSPACE Prosperity, Security, and Openness in a Networked World MAY 2011



2008 年 2 月

Fig.1. Documents released by the States in recent years. See Refs.[1-6]

From the point of view of military operations, counter-offensive cyberspace operations against cyberattack from hostile countries faces at least three questions. First, how to confirm sources of attack are government origin or personal origin? Anyway, cyberattacks require only commodity technology and enable attackers to obfuscate their identities, locations, and paths of entry. When states' infrastructures are attacked by cyberhacker form a distance, how the state affirm sources of attack? Second, decision making process is too short for cyberspace operation. The lack of geopolitical boundaries and natural boundaries of the electromagnetic spectrum allows cyberspace operations to occur rapidly nearly anywhere. Commanders in cyberspace war need to make decisions in a very short time that were previously incomprehensible. Thus, possibilities of making wrong decisions would increase. Third, the concept of cyberspace operation would block development and popularization of Internet.

kchm 31/12/11 6:03 PM
Deleted: from hostile countries in the military counter-offensive cyberspace operations at least three problems facing

kchm 31/12/11 6:04 PM
Deleted:

3. Discuss and conclusion

Though cyberspace typically describes the flow of digital data through the network of interconnected computers which ascribes it to a "virtual" property, it has "real" effects on military, civil and private sector which depend on computers for daily operations. At presents, the information and cyberspace security represents a major non-traditional security challenge confronting the international community. Inter-connectivity of information and cyber networks has contributed to "make countries of the world "a community of common destiny" in which states' security is inseparably linked together".[7] Therefore, international community should view this issue from the new perspective of "a community of common destiny" and work together towards a peaceful, secure and equitable information and cyber space.

The issue of cyberspace is now beyond technical issue, it is also an issue related to social, political, economic and cultural issues of a country, which makes it an issue need to be considered carefully. In our opinion, the following norms should be established in the field of cyberspace.

(1) The principle of peace

The international community should engage in active preventive diplomacy and promote the use of information and cyber technology in advancing economic and social development and people's welfare and in maintaining international peace, stability and security. *At the same time,* countries should work to keep information and cyberspace from being a new battlefield, prevent an arms race in information and cyberspace, and settle disputes on this front peacefully through dialogue.

(2) The principle of sovereignty

While ensuring the healthy development and effective utilization of information and cyber space, it is also necessary to keep information and cyber technology from being turned into another tool to interfere in internal affairs of other countries.

The sovereignty countries have the right and responsibility to protect, in accordance with their respective national laws and regulations, their information and cyber space and critical information infrastructure from threats, disturbance, attack and sabotage. In this area, respect for sovereignty and territorial integrity enshrined in the UN Charter and other universal basic norms of international relations should also be respected.

The sovereignty countries should establish mutual respect and enhance understanding. Different countries have different historical and cultural traditions, different levels of economic and social development. It is normal of existing different opinion toward view of Internet, we shouldn’t focus on the differences, but should be in a mature, responsible manner, respect and take care of each other's concerns, seek common ground for mutual cooperation and development through frank dialogue and exchange. Such common topics and issues may include: forensics and attack attribution; protection of networks and systems critical to national security, indications and warnings; protection against organized attacks capable of inflicting debilitating damage to the economy; foster the establishment of national and international watch-and-warning networks to detect and prevent cyberattacks as they emerge etc.

(3) Rule of law

We should build and sustain an environment in which norms of responsible behavior guide states’ actions. Adherence to such norms brings predictability to state conduct, helping prevent the misunderstandings that could lead to conflict.

International society could firstly try to establish criminal law in cyberspace to inhibit antiterrorism and criminal behavior such as child pornography. This cooperation is most effective and meaningful when the countries have common cybercrime laws, which facilitates evidence-sharing, extradition, and other types of coordination.

（4）Technical standards in Internet governance

Unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them. Considering its complexity and importance on people's life and national security, technical standards and governance structures should be established step by step among international societies after careful discuss, norm of behavior should be reached after considering national security with various interests, but not only to those counties with strong advantage in the field of cyberspace and information technology.

kchm 31/12/11 6:06 PM

Deleted: ~~, but not only to those countries with strong advantage in the field of cyberspace and information technology~~.

References:

[1] International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World, (May, 2011).

[2] DOD, Department of Defense Strategy for Operating in Cyberspace, (July 2011).

[3] C.o.t.J.C.o. Staff, The National Military Strategy for Cyberspace operations, (December 2006).

[4] T.U.S. Army, The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028, (22 February 2010).

[5] B.A. Air Force. Air Force Cyber Command, LA, Air Force Cyber Command Strategic Vision, (FEB 2008).

[6] U.S. government, The National Strategy to Secure Cyberspace, (Feb. 2003).

[7] W. Qun, Speech by H.E. Ambassador Wang Qun at the First Committee of the 66th Session of the GA on Information and Cyberspace Security (Oct. 2011).