International Cyberspace Considerations

General (Ret) Ron Keys, RK Solutions;
Jim Ed Crouch, NSCI
May 17, 2010

National Security Cyberspace Institute, Inc. (NSCI)

Through the combination of research and education, NSCI supports public and private clients aiming to increase cyberspace awareness, interest, knowledge, and/or capabilities. NSCI is committed to helping increase security in cyberspace whenever and wherever possible. NSCI publishes a bi-weekly newsletter (*CyberPro*), has published numerous whitepapers on various cyberspace topics, maintains an online cyber reference library, and has established an email distribution list for sharing cyber-related resumes to interested parties. NSCI is a small, veteran-owned business headquartered in Virginia.

That's Where the Money Is

When asked why he robbed banks, Willie Sutton is reported to have said, "Because that's where the money is." If he were alive today, it's unlikely he'd bother with the risk involved in the classic "stickup" with his Thompson submachine gun. He'd probably take a safer route – theft via the internet – although with Willie's flair for the dramatic and penchant for notoriety, he may not like cyber criminal anonymity.

With the explosive growth of cyberspace in conducting business of all types, it should come as no surprise to anyone that network attacks are also growing exponentially. Why? Because to paraphrase Willie Sutton, that's where the money, intellectual property, national secrets, and even our individual identities are. So how are we doing in protecting these valuable resources? This paper examines the world's most lucrative targets – the top ten countries in terms of total users of the internet – focusing primarily on their economies, industrial capabilities, politics, or other factors that might make them prime targets of cyber attacks. Most of these countries also rank among the top ten economies of the world and possess military and technological capabilities that would further place them in the top ten in those categories.

So let's first take a tour through the top ten, starting from #10 Korea (37.5 million internet users) and working our way to China at the top (360 million users). We'll follow that with a few notes on the countries that are the league leaders as the witting or unwitting hosts of cyber attacks, sometimes involuntarily providing "safe harbor" or as a source of botnets for hackers, cyber criminals, or other nefarious enterprises from other countries. In addition, we provide some information on the cyber capabilities of these 10 countries from the excellent resource *Cyber Commander's Handbook* published in January 2010 by Technolytics. We also provide a discussion of some of the recent dialogue regarding international agreements in cyber, and our opinion of whether the nations of the world should finally get serious about entering into such agreements.

#10 – The Republic of Korea

South Korea, the world's 25th most populous country, ranks tenth in terms of total internet users. It also can claim the distinction as the most "wired" nation on earth, with over 77% of the population using the internet. With the fifteenth-largest economy, South Korea last year surpassed the United Kingdom, Russia, and Canada to become the world's eighth-largest exporter and the seventh-largest trading partner of the United States. It is also now the eighth-largest trading partner of the European Union, exporting primarily electronics, automobiles, ships, petrochemicals, and robotics around the world. Cheap, high-speed broadband service has provided South Korea's citizens with easy access to the internet, resulting in a 97% growth in the number of internet users over the past decade. However, it has also prompted an outbreak in online gaming and social networking that have become so prevalent that many of South Korea's citizens have been diagnosed as "addicted." The government has thus engaged in the creation of internet-addiction counseling centers, hospital treatment programs, and even "boot camp" facilities, complete with military-style obstacle courses, in an effort to fight this phenomenon. [1]

[1] http://www.technolytics.com/CyberWarfare.asp

General (Ret) Ron Keys, RK Solutions;
Jim Ed Crouch, NSCI
May 17, 2010

At the same time, South Korea's military networks encounter an ever-growing number of cyber attacks, with an average of 95,000 cases of hacking attempts and viruses reported each day. The majority of these are believed to originate in either North Korea or China. In 2009, the South Korean military signed a memorandum of understanding to work with the U.S. on information assurance and computer network defense. The agreement is intended to enhance cyber defense capabilities and improve interoperability between the two nations after Seoul assumes wartime operational control of its troops from the U.S. in 2012.[2]

With its economy, manufacturing, growing export business, and dependence on the internet, there is much to protect in South Korea.

#9 – France

With an economy that ranks sixth in the world, France combines both private enterprise and government ownership and control. Although government involvement has declined in recent years, it is still heavily engaged in the railway, electricity, aircraft, nuclear power and telecommunications sectors.

France's population ranks 20th in the world, but it is ninth in numbers of total internet users, the result of over a 400% increase since the year 2000. This growth has brought nearly 70% of the French population with access to the internet.

According to the World Trade Organization, France was the world's sixth-largest exporter and the fourth-largest importer of manufactured goods in 2009. As a result of large investments in nuclear technology, France has in operation 59 nuclear plants that generate almost 80% of the country's electricity.

France's major military industries produce a variety of major weapons systems, including aircraft, ships, tanks, and missiles. Although France has withdrawn from the Eurofighter project, it is actively investing in other European joint aircraft and ship programs. It continues its long tradition as a major arms seller, making most of its manufacturing designs available for the export market.

France's GDP declined by 2.1% last year, and the tax burden remains one of the highest in Europe. The government budget deficit more than doubled between 2008 and 2009, to over 8% of GDP, with unemployment approaching 10%. An initiative that reduced the standard work week to 35 hours was intended to solve unemployment but has proved unsuccessful at doing so. Minimum wage laws providing relatively generous compensation seem to have contributed to the high and continuing unemployment numbers.

In spite of these factors, and perhaps in some cases because of them, France's industrial base and infrastructure still offer a lucrative target for would-be hackers and cyber spies.

#8 – Russia

Russia has undergone significant changes in recent years, moving from a centrally-planned economy to one that is more market-based and globally-integrated. Reforms in the 1990s privatized most industry, with notable exceptions in the energy and defense-related sectors. [3]

Ranking ninth in population and fourteenth in GDP, the country is eighth in number of internet users, the result of 1,300 percent growth since 2009. However, of Russia's 140 million residents, only 32% are users of the internet.

Russia's ongoing experiment with quasi-capitalism is an interesting case. As state-owned firms moved to the private sector, their ownership was passed to those with political connections, leaving the nation's wealth highly concentrated among a new "ruling class." Property rights are not yet fully incorporated, and the government still interferes in the marketplace. Fertile with natural resources, Russia is the world's largest exporter of natural gas

[2] http://www.koreatimes.co.kr/www/news/nation/2009/11/205_47544.html
[3] https://www.cia.gov/library/publications/the-world-factbook/geos/rs.html

General (Ret) Ron Keys, RK Solutions;
Jim Ed Crouch, NSCI
May 17, 2010

and second-largest exporter of oil. This reliance on commodity exports makes Russia vulnerable to boom and bust cycles that follow the highly volatile swings in global commodity prices. The government since 2007 has embarked on an ambitious program to reduce this dependency and build up the country's high technology sectors, but with few results so far. The Russian economy was one of the hardest hit by the 2008-09 global economic crisis as oil prices plummeted and the foreign credits that Russian banks and firms relied on dried up. [4]

Long-term challenges include a shrinking workforce, a high level of corruption, and poor infrastructure in need of large capital investment. [5]

Although Russia continues to transition towards a capitalist economy, the inability of technology-trained individuals to find legitimate work has resulted in their recruitment by organizations engaging in cyber crime. In spite of the significant image problem this has created, the government hasn't appeared interested in fixing it as long as the cyber criminals maintain a hands-off approach to Russian assets. This has become more problematic as Russia at the same time has insisted on the development of international treaties on cyberspace while in the main acting as a witting host to a variety of miscreants. The Russian Association of Electronic Communications, established in 2006 to speed Russia's integration into the global internet economy, may be gaining momentum in fighting this problem – not by law enforcement, but by initiating a Russian version of Silicon Valley near Moscow that is expected to create thousands of jobs over the next five years. However, in the absence of a crackdown on cyber crime, it seems unlikely that the legitimate jobs created can provide the necessary incentives for the criminals to change occupations.

The preponderance of media reporting on cyber incidents from Russia in recent years has centered around Russia-as-attacker versus Russia-as-target. Notable among these have been the 2007 and 2008 Distributed Denial of Service (DDoS) attacks against Estonia and Georgia, both of which were very effective in disrupting network operations in those countries. The attacks against Estonia caused across-the-board upheaval for the better part of three weeks. Despite the complaints and finger-pointing, there is still plausible deniability of a State sponsored attack.

#7 – United Kingdom

The U.K. is the world's sixth-largest economy, although it ranks only 22nd in population. With a declining industrial base, the U.K.'s service sector is now responsible for 73% of the GDP. This sector is dominated by financial services, primarily in banking and insurance. London is the world's largest financial center and a major hub for international business and commerce. It has the largest concentration of foreign bank branches in the world. Many multinational companies that are not primarily UK-based have chosen London as their most important foreign headquarters location. The Scottish capital, Edinburgh, has one of the principal financial centers of Europe and is the headquarters of the Royal Bank of Scotland Group, one of the world's largest banks.

Over 46 million Britons, or 76% of the population, are connected to the internet following an impressive 200-plus percent rate of growth during the last decade.

With an economy so heavily dependent on banking, financial services, and international business and commerce, the U.K. remains a prime target in the cyber battlespace.

#6 – Germany

In spite of a scarcity of raw materials, Germany has the fourth-largest economy in the world behind the United States, China, and Japan. However, exports and imports suffered their biggest drop since 1950 last year, causing Germany to be overtaken by China as the world's leader in exported goods.

[4] https://www.cia.gov/library/publications/the-world-factbook/geos/rs.html
[5] Ibid

The nation's GDP is composed of approximately 70% from the services sector and 29% from industry. Germany leads the world in solar power and wind turbine technologies, and is most famous for high-quality automobiles such as Mercedes Benz, BMW, Porsche, Audi, and Volkswagen.

Its population of 82 million places Germany fourteenth in the world, with 54 million (65%) of its citizens being reported as users of the internet.

As in much of western Europe, German birth rates have been in decline for several years. In 2009, the rate was only 1.36, well below the level considered sustainable. If present trends continue, forecasts indicate that by 2030 as much as 28 percent of Germany's population will be elderly, and the ratio of workers to retirees will be reduced to 1:1. With large welfare programs typical of most European countries, this could create huge financial problems for Germany in the future.

Experts have been monitoring Chinese cyber espionage against Germany since the 1990s. A counterespionage official with Germany's domestic intelligence agency said the country has verified "many hundreds of attacks per year," and that others had likely gone undetected.[6] This relatively low number leads us to believe that Germany either has a different definition of the word "attack," has limited capabilities for detection, or has few resources of interest to China.

Nevertheless, in August, 2009, attacks reported to be sponsored by the Chinese military targeted the computers of many of Germany's top officials. In a remarkable coincidence, the reports surfaced just as Germany's Chancellor Angela Merkel began a week-long diplomatic mission to China.[7]

#5 – Brazil

Brazil is the world's fifth-largest country and has the eighth-leading economy. It has large and developed agricultural, mining, manufacturing and service sectors, as well as a large labor pool.

Brazil's major export products include aircraft, electrical equipment, automobiles, ethanol, textiles, footwear, iron ore, steel, coffee, orange juice, soybeans and corned beef. The country has been expanding its presence in international financial and commodities markets, and is one of a group of four emerging economies – along with Russia, India, and China – that have formed a loose alliance with a name, BRIC, that is an acronym derived from the first letters of their country names. Some experts predict that the four BRIC countries could, by the year 2050, emerge as the top four economies in the world. In fact, recognizing this possibility, leaders of the four have engaged in summits in an attempt to formalize the relationship. With a population approaching 200 million, Brazil is the fifth-largest country, and has the ninth-ranked economy. The last 10 years saw a staggering 1,250% increase in internet use, bringing the total number of Brazilians being "wired" to 34%.

#4 – India

India's diverse economy – the twelfth-largest in the world – consists of small farming operations, modern agriculture, a wide range of modern industries, and a multitude of services. A move towards a market economy and reduced controls on foreign trade and investment began in the early 1990s and has served to accelerate growth, which has averaged more than 7% since 1997. With vast human and natural resources and a huge knowledge base, India is expected to be among the leading economies of the world within the next decade.

Slightly more than half of the work force is in agriculture, but services are the major source of economic growth, accounting for more than half of India's output. Major industries include telecommunications, textiles, chemicals, food processing, steel, transportation equipment, cement, mining, petroleum, machinery, information technology-

[6] http://www.habledash.com/index.php?option=com_content&view=article&id=91:the-cyber-wars-are-already-worldwide-on-web&catid=47:newsflash&Itemid=65
[7] www.securityfocus.com/brief/639

enabled services and software. The country's workforce totals half a billion people. India has capitalized on its large numbers of well-educated people, skilled in the English language, to become a major exporter of software services and software workers. It has proposed limited privatization of government-owned industries, in part to offset its current deficit. India's long-term challenges include inadequate physical and social infrastructure, limited employment opportunities, and insufficient basic and higher education opportunities. In the long run, however, the huge and growing population is the fundamental social, economic, and environmental problem.

Of India's 1.1 billion people, only seven percent have access to the internet. That seven percent nonetheless translates into 81 million people, many very highly skilled.

Trade between China and India has grown rapidly in the last ten years. China has already become India's biggest trading partner. Common economic interests are driving the two countries into closer political cooperation both bilaterally and internationally, putting aside their decades-long disputes over the border and the Tibetan question.

Notwithstanding this easing of tensions, India has been a target of cyber hacks and espionage from China since 2007. Of course, who hasn't?

#3 – Japan

Forced to virtually disarm – and freeing up money for other priorities – in the aftermath of World War II, Japan developed a technologically-advanced economy through a cooperative effort between the government and industry. With an outstanding work ethic and technical savvy, Japan's citizens created an economy that grew at a breakneck pace through the next four decades. Investing heavily in real estate ventures around the globe, Japan's bubble finally burst in the 1980s. This has been followed by two decades of stagnation or negative growth. To appreciate the magnitude of this problem, consider this: the Nikkei 225 average peaked at nearly 39,000 at the end of 1989; twenty years later it stood at 11,000, a drop of almost 75%.[8] In spite of this, Japan, ranked tenth in population, still stands at fourth in exports, and second in GDP worldwide.

To address its problems, the Japanese government has intervened with huge infrastructure investments. This has propped up the economy but has massively increased the national debt.

Debate continues on the role and effects of government intervention and funding to stimulate consumption. The debt, estimated to have reached 192% of GDP in 2009, and an aging and shrinking population caused by a 1.29 rate of fertility in 2009, are two major long-run problems.

In spite of the gloomy economic picture, Japan's citizens remain among the world's most prosperous.

Of its 127 million people, over 75% are connected to the internet, a two-fold increase during the past decade. According to the national police agency, Japan's internet crime statistics took a big jump in 2009, led by ID theft, database attacks, child pornography posts, and copyright violations. Police made arrests or took other action in 6,690 cases, up 5.8 percent from the previous year and the highest figure since data was first compiled in 2000. The number has more than doubled in four years.[9]

#2 – United States

The U.S. economy is, of course, the world's largest – by a long shot. Historically, it has maintained a stable overall GDP growth rate, a low unemployment rate, and high levels of research and capital investment funded by both national and, increasingly, by foreign investors. In 2006, consumer spending made up 70 percent of the United States Gross Domestic Product. Like other developed countries, the United States is faced with retiring baby boomers who have already begun withdrawing from their Social Security accounts; however, the American

[8] http://news.bbc.co.uk/2/hi/8471888.stm
[9] http://www.physorg.com/news186931900.html

population is young and growing (2.05 fertility rate combined with a very high immigration rate) when compared to Europe or Japan. The United States public debt is in excess of $12 trillion and continues to grow at a rate of about $3.83 billion each day. It remains to be seen whether Washington's actions over the past two years will result in a recovery or a national bankruptcy. Of the nation's 307 million people, 74% are users of the internet, a 138% increase since the year 2000. Because of the U.S. position as the world's lone superpower, cyber attacks from all points of the globe are so commonplace that they're hardly newsworthy anymore. For example, Politico recently reported that "Congress and other government agencies are under a cyber attack an average of 1.8 billion times a month. In 2008, security events caused by vectors including worms, Trojan horses and spybots averaged 8 million hits per month. That number skyrocketed to 1.6 billion in 2009 and climbed to 1.8 billion this year, according to Senate Sergeant-at-Arms Terrance Gainer. " [10] This stunningly-high number is probably more suggestive of the need for standardization in our definitions of what constitutes an attack, a probe, or a ping, than it is the amount of intellectual property resident on Capitol Hill.

#1 – China

In the 1980s, the government of China arrived at a startling revelation: a market-oriented economy seems to work better than government ownership and control. With the economic reforms implemented since then, the country has experienced significant growth in consumption, investment, and standards of living. With private companies now playing a major role, China's economy is now the third-largest in the world. According to China's official statistics, the poverty rate fell from 53% in 1981 to 2.5% in 2005. Similar success stories can be found in the infant mortality and maternal mortality rates. Further, the number of citizens having access to a simple telephone rose more than 94-fold during that 24-year period. The number of internet users now totals approximately 300 million. Although this number is a mere 27% of China's population, it represents one-fifth of the total number of internet users worldwide.

These reforms have been a two-edged sword from the Chinese government's perspective. Although not the only national government to have these concerns about its own citizens, the Chinese government is fearful of internet activity that threatens to undermine state control. Internet service providers hoping to do business in China are required to sign an agreement whereby they pledge to disallow the dissemination of information that may "...jeopardize state security and disrupt social stability, contravene laws and regulations and spread superstition and obscenity."[11]

Illustrative of the government's reluctance to abandon its totalitarian instincts is the recent dustup with Google over censorship issues and cyber attacks targeting human rights groups and foreign businesses operating in China. Internet experts and Google officials believe the Chinese government installed malware on users' computers to gain access to the targeted individuals' Google e-mail (Gmail) accounts.

China has committed significant military resources to cyber warfare, with Chinese hackers routinely targeting networks in countries such as the U.S., U.K., Germany, and India. Accusations of attacks by China have become so prevalent that if you can't claim membership in the "targeted-by-China" club, you must be a real sad sack of a country.

The Best Defense is a Good Offense

The data and descriptions for the tables below was taken from the *Cyber Commander's Handbook* published by Technolytics in January 2010. The ratings used by Technolytics range from 1 (Low) to 3 (Moderate) to 5 (High). For our purposes, we have included only the 10 countries listed above, plus North Korea. For a complete country listing, we recommend purchasing the book – an excellent resource.

[10] http://www.politico.com/news/stories/0310/33987.html#ixzz0lMRt0xj6
[11] http://dfn.org/voices/china/selfdiscipline.htm

Cyber Military Capabilities (2009)	Cyber Capabilities Intent	Offensive Capabilities Rating	Cyber Intelligence Capabilities	Overall Cyber Rating
China	4.2	3.8	4.0	4.0
United States	4.2	3.8	4.0	4.0
Russia	4.3	3.5	3.8	3.9
India	4.0	3.5	3.5	3.7
North Korea	4.2	3.4	3.3	3.6
Japan	3.9	3.3	3.5	3.6
South Korea	3.5	3.0	3.2	3.2
United Kingdom	3.2	3.0	3.0	3.1
Germany	2.5	2.5	2.4	2.5
Brazil	2.1	2.5	2.1	2.2
France	2.0	2.1	2.2	2.1

Table 1: Country Cyber Capabilities Ratings[12]

Cyber Capabilities Intent: Represents commitment or reason to acquire capabilities to carry out actions.

Offensive Cyber Capabilities: The ability to achieve a specified objective in the cyber domain through offensive (generally thought of as "attacking") actions. This includes four major components: force structure, technical superiority, readiness, and sustainability.

Cyber Intelligence Rating: The adaptability of current intelligence collection capabilities to adapt to the new cyber domain or the ability to change the current collection capacity in order to generate insight into the cyber domain .

Overall Cyber Capabilities Rating: The summation of the above three areas that represents the estimated overall cyber capabilities.

Who… Me?

During the third quarter of 2009, China must have fallen asleep; it dropped to fourth place among the world's cyber attackers for the July-September period. Jumping into the lead for the quarter was Russia with more than 13% of the total attacks launched. According to Massachusetts-based Akamai Technologies, an internet content delivery service, the remainder of the top four were Brazil (8.6%), the U.S. (6.9%) and China (6.5%).

Akamai reported discoveries of attacks either from or through 207 different countries during the quarter. Rounding out the top ten were Italy, Taiwan, Germany, Argentina, India and Romania. The top ten were involved in some way in 61% of all attacks.

In January, 2010, Symantec conducted a telephone survey of 2,100 businesses and government agencies in 27 countries and found that "100 percent of them had experienced cyber losses of some type in the past year. Seventy-five percent of organizations said they were hit by a cyber attack in the past year and 36 percent of those rate the attacks as either 'somewhat' or 'highly effective'." [13]

The report went on to say:

[12] Cyber Commander's Handbook; pp 10-13; technolytics; January 2010
[13] http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=sesreport2010&om_ext_cid=biz_socmed_twitter_2010Feb_ESR report

[General (Ret) Ron Keys](), RK Solutions;
[Jim Ed Crouch](), NSCI
May 17, 2010

> *"The top three reported losses were theft of intellectual property, theft of customer credit card information or other financial information that resulted in monetary loss in 92 percent of instances. The top three costs, according to the survey conducted for Symantec (NASDAQ: SYMC) by Applied Research, were productivity, revenue, and loss of customer trust.*
>
> *"The study found that 42 percent of enterprises acknowledge that cyber risk is their top priority and concern -- more than terrorism, natural disasters, and garden-variety theft combined... Even with this increased attention on safeguarding critical data and systems, enterprises continue to report massive cyber attacks that compromise not only customer confidence but, potentially, their ability to remain in business."* [14]

Of course, everyone is happy to discuss their "victim" status, but are naturally unwilling to admit to cyber activity themselves, whether "active defense" or offensive. Moreover, countries on the receiving end of cyber attacks are reluctant to reveal the source – unless that source happens to be China or Russia – even when they're able to determine it. Attribution techniques continue to improve every day, but it is not always wise to reveal too much about how – or even whether – attribution has been determined. Often the methods and sources used in determining attribution constitute intelligence too valuable to risk revealing to adversaries, and there is always an advantage in knowing more than your adversary thinks you know about the who, what, where, and how of an attack. There is always a next time.

All Hat, No Cattle

Countless studies during the past few years have been commissioned from around the world to study and make recommendations for a way ahead for cybersecurity. Virtually all reach the same conclusions: top-down leadership, public/private partnerships, international cooperation, standardized laws, a central governing body, and increased public awareness, education, and responsibility, among others. Although the global community is making progress in some of these areas, most efforts seem to have stalled on the international, bilateral, and multi-lateral agreement fronts.

In 2001 the Council of Europe adopted a "Convention on Cyber Crime," commonly referred to as the Budapest Convention. Provisions of this agreement standardize national laws regarding "illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighboring rights."[15] Since its original adoption, 46 countries have signed on, with an additional 120 countries using it as a model for their own legislation.

The United Nations recently began discussions on a Russian proposal for a new treaty dealing with cybercrime. Originally proposed and rejected in 2005, this document has the support of China and other developing countries, but is being resisted by the U.S. and U.K., who believe the new proposal will impede progress made towards Budapest-based legislation around the world.

According to a report in the *Pittsburgh Post-Gazette*, the U.S. recently sent a delegation to a Russian-sponsored internet security conference in Garmisch, Germany. At the conference, the two countries agreed to renew bilateral discussions regarding cybercrime, computer security, and law enforcement in the cyber arena. As the newspaper reported, "The United States has succeeded in creating a global 24-hour, seven-day network of law enforcement agencies in 50 nations, which have agreed to collect and share data in response to computer attacks and intrusions. While officials from both nations said that law enforcement cooperation had improved, the

[14] Ibid
[15] http://en.wikipedia.org/wiki/Convention_on_Cybercrime

Russians have still refused to sign the European Cybercrime Treaty, which is strongly backed by the United States." [16]

The report went on to say, "At the same time, for the past 13 years the Russians have also been trying to "interest the United States in a cyberspace treaty in which nations would agree not to develop offensive cyberweapons or to conduct attacks on computer networks.[17] The United States has repeatedly declined to enter into negotiations, arguing instead that improved law enforcement cooperation between different countries was all that was necessary to combat both cybercrime and cyberterrorism."[18]

Also contained in the *Post-Gazette* account was a discussion of further disagreements between the U.S. and Russia that point to the difficulty of reaching any meaningful international agreements:

> *"...Gen. Vladislav P. Sherstyuk, Russia's undersecretary of the security council of the Russian Federation and the former leader of the Russian equivalent of the National Security Agency, criticized the treaty, saying that a single provision effectively violated Russia's sovereignty by permitting foreign law enforcement direct access to the Russian Internet.*
>
> *"He also restated Russian concerns about the absence of an international treaty limiting the military uses of the Internet. 'Cyberattacks are left out of international military law,' he said. 'Information technology can be used as a tool to undermine national peace and security.'*
>
> *"The Americans have accused the Russians of turning a blind eye to cybercriminals who have operated with relative impunity from their country. In response, the Russians have criticized what they see as the United States' 'hegemony' over the Internet and privately expressed concerns that the United States has retained a 'red button' — the power to shut off the Internet for specific countries."* [19]

In spite of these disagreements, conference participants expressed optimism about the progress made. As we publish this paper, the United States and Russia are engaged in a U.S.-Russia Information and Communication Technology (ICT) Roundtable.[20]

The Way Ahead

So where should the U.S. go from here? Does the U.S. proceed full speed ahead as signatories to international agreements, or does the U.S. continue to discuss the need and work around the edges while quietly stiff-arming sweeping accords with other nations. While we wholeheartedly support increased engagement and collaboration with international partners, our vote is for the latter.

It is likely that the United States enjoys a technological edge in its cyber capabilities – both offensive and defensive. That may explain why China – and not the U.S. – is implicated in so many attacks against a wide variety of countries. Perhaps the U.S. has a better ability to penetrate networks without leaving behind as much evidence. Why should the U.S. give up this edge or unnecessarily tie its own hands? [21]

In addition, with anonymity/attribution still a principal characteristic of cyber aggression, treaty compliance will be difficult to enforce. Can signatories to an agreement depend solely and safely on trust to ensure compliance?

---

[16] http://www.post-gazette.com/pg/10106/1050953-115.stm
[17] Which of course would be like trying to put the Nuclear Genie back in the bottle… only cyberspace is a much cheaper and ubiquitous Genie.
[18] http://www.post-gazette.com/pg/10106/1050953-115.stm
[19] http://www.post-gazette.com/pg/10106/1050953-115.stm
[20] http://fcw.com/articles/2010/05/11/web-u.s.-russia-it-talks.aspx
[21] For an expanded perspective on why the U.S. should be cautious about entering into international cyber agreements, see the article by Kathryn Stephens and Larry McKee, "Cyber Espionage: Is the United States getting more than it's giving?" .

General (Ret) Ron Keys, RK Solutions;
Jim Ed Crouch, NSCI
May 17, 2010

What foundation exists for this trust? Moreover, what about the basic necessity of agreement on terms such as cyber crime, cyber attack and cyber exploitation that would be a part of any such accord.

In spite of these concerns, however, a case can be made for continued work toward international standards, especially in the area of cybercrime. Nations should cooperate on identification, arrest, and prosecution of cybercriminals. It may not be easy to reach consensus on everything that constitutes a cyber crime, but there should be common agreement on the most obvious. For example, some of the U.S.'s closest allies have placed restrictions on so-called "hate speech" – something that most Americans would consider a violation of the First Amendment. But there's no reason why the U.S. and others shouldn't be able to reach agreement on some activities – theft of financial resources or intellectual property and trafficking in child pornography, for example – that constitute criminal activity. Rather than rejecting all international agreements outright, the U.S. and international partners should be able to find common ground on these and other issues while continuing to work at resolving the larger differences – the "one bite at a time" way to eat the elephant.

Other areas for international cooperation include education, training, and information sharing. It seems nearly everyone in the international cyber community recognizes that increased situational awareness is critical to getting in front of cyber actors with aggressive intent. The U.S. should encourage sharing vulnerability discoveries and defenses against new malware and viruses. In addition, the U.S. should encourage providing assistance to other countries in determining attribution following a cyberspace criminal activity.

In short, the U.S. should be collaborating with other nations with the intent of achieving agreement on defining common cyberspace terms and on what constitutes normative behavior regarding such areas as nation-state liability and accountability for cyber criminal activity.

Increased mutual understanding regarding international views of cyberspace will help to better define ideas such as "use of force" and "armed attack" in the context of cyberspace. Both formal and informal relationships between the U.S. and other nations should be encouraged, in both the public and private sectors. U.S. leadership with the international cyber community will help to build the confidence and trust necessary to enhance transparency and cooperation.

Although we do not advocate for a full-speed-ahead approach to signing international agreements, we remain strongly in favor of individual nations doing everything possible – bilateral agreements with like-minded countries, and other actions on the low-hanging fruit from the endless list of recommendations produced from the multiple studies conducted over the past few years – to defend their sovereign rights, manage risks, and ultimately protect personal freedoms, financial prosperity, and national security in cyberspace.