



Affaires étrangères et
Commerce international Canada

Foreign Affairs and
International Trade Canada

“International Pathways to Cybersecurity”

Report of Consultation

The aims of the EastWest Institute’s consultation on cybersecurity at the European Parliament on February 17, 2010 in the seventh Worldwide Security Conference (WSC7) were to:

- articulate new goals for worldwide cybersecurity and the steps needed to achieve them
- to stimulate progressive improvement in the way global cybersecurity is reviewed, managed, and implemented
- bring together leading policy makers, specialists, business executives, community leaders and journalists from around the world for a debate on defining and understanding international cybersecurity approaches, concerns and solutions.

The invitation-only consultation was supplemented by public sessions at the World Customs Organization headquarters on 18 February and by bilateral and other private discussions throughout the week. The private consultation featured a five party multi-lateral interaction between China, Europe, India, Russia and the U.S., but was attended by a diverse set of broader international representatives.¹ The WSC7 gathering of experts is the first step in formulation of what eventually will be the "rules of the game that one day will take the form of obligations," according to John Mroz, President and CEO of the EastWest Institute. Below you will find a summary framed around EWI’s three principal goals of WSC7.

Main Conclusions

There was a clear agreement that Track 1 diplomacy on worldwide cybersecurity cooperation is not working well on the tactical level and practically non-existent on the strategic level. As one delegate put it: “We are quickly running out of time. Technology is developing at such a rapid pace that policymakers are playing a catch-up game. Politicians and technical experts are not

¹ Participants of the private consultation described their primary competence as: political or policy (40%), business (27%), technical (19%), legal (9%) and defense (5%).

talking to each other. In an environment where 80 per cent of public infrastructure is owned by the private sector, this is rather problematic.”

The majority of experts emphasized that there is an urgent need for Track 2 diplomacy to help kick-start international cooperation on cybersecurity.² An essential element will be trust building, which can only be achieved through a bottom-up approach, starting with cooperation on small technical issues and then moving to more controversial strategic problems. One delegate voiced his concern that it might already be too late for bottom-up approaches and that more top-down methods are needed. Nevertheless, as long as Track 1 diplomacy fails to deliver results, Track 2 initiatives will have to lay the groundwork for international cooperation.

Goal 1: Articulate new goals for worldwide cybersecurity and the steps needed to achieve them.

“Cyberspace today is like the Wild West. It does not enjoy the international community’s setting of basic agreements, rules and procedures,” said John Mroz at the beginning of the institute’s consultation on cybersecurity. Another high-level participant argued that the best weapon against the online thieves, spies and vandals who threaten global business and security would be international regulation of cyberspace. This is not happening at the moment. In the words of another delegate: “People have to realize the Internet is an integral part of every country, politically, socially and business-wise. Not to focus on cybersecurity is playing with fire.”

Underlining the urgency of the subject, conference delegates set out to define some of the key problems policy makers are facing in today’s cyberspace³:

1. There is a clear lack of a commonly agreed definition of what cybersecurity means. All states treat cybersecurity as a domestic issue and hence definitions and legal frameworks vary across nations, which makes international cooperation difficult.
2. Breakthrough solutions will require the effective integration of technical, business, legal, defense and international policy competencies on a level that has not happened so far.
3. Current diplomatic assets assigned to the problem are inadequate to the task and reflect a lack of political commitment at high levels.
4. The commercial drivers for building security into network equipment, networks and services are not adequate.⁴ This is the result of a lack of consumer awareness of the risk exposure they face and a lack of leadership and commitment from those in control. The interests of netizens, businesses and governments need to be effectively spelled out at an international level so that the required investments will be made to secure cyberspace.
5. States have the right to organize offensive and defensive assets for information operations of a strategic character to affect the strategic intentions of other states but international

² 81% of the participants indicated that “the current level of international cooperation in cyber space is far, far behind where it needs to be.”

³ 56% of participants felt that a major international cyberspace crisis was inevitable.

⁴ Only 13% of participants indicated that “the private sector is sufficiently motivated to make the necessary improvements for cybersecurity.” While 91% believe that the private sector organizations should sometimes be a leader in initiatives with government.

law does not adequately regulate these assets.⁵ There needs to be a clear definition what "cyber peace" means.

6. There are three levels of information warfare that need to be regulated: political, military strategic and military tactical. The last (meaning electronic warfare assets oriented to single enemy targets or groupings in a localized vicinity) is often overlooked.
7. Nations are thinking too parochially about their online security to collaborate on crafting global cyber ASPR.

Bottlenecks

After stating the problems, delegates embarked on defining nine areas of bottlenecks in the international cybersecurity debate. Education and terminology were identified as major blocks in raising cybersecurity awareness. "Plain language is vital," argued one delegate. "We use a lot of complex terminology where it's not needed. We don't encourage people to think enough." Another delegate pointed out that there is a need for an international dictionary on cybersecurity to facilitate international cooperation.

Listed below are nine areas that need to be addressed by the international private and public sectors in order to achieve international cooperation in cybersecurity:

- a. **Education and Awareness.** Awareness needs to reach "critical mass" in public perception in order for it to become a pragmatic item of private and public sector agendas.⁶
- b. **Terminology.** Defining and understanding various descriptions of the issues at hand, whether seen as Cybersecurity (U.S.), Information Security (Russia), or Internet Security (China).
- c. **Creation of a sense and system of responsibility.** Responsibility needs to be imbedded at three levels (a) individual and corporate end users; (b) creators of technology and media; (c) government.⁷
- d. **Understanding** the end user as well as growth of new media and technology.
- e. **Constant Battle between Security, Privacy and Freedom.** Such matters will not have a one-off solution. Decision makers will need to understand that in order to reach solutions some compromises need to be made and balances struck among these three important factors.^{8 9}
- f. **Lack of Legal Framework.** Lack of domestic legal frameworks will impede international legal cooperation.
- g. **Challenging Human Nature.** By nature we have consistently reacted to threats once they triggered specific actions. The decision-making and reaction mentality needs to keep changing where we pro-actively address vulnerabilities before they are exercised by threats.
- h. **Dismantle the perception of domestic boundaries.** Many treat cybersecurity as a domestic issue, failing to understand that cybersecurity is a challenge that

⁵ 38% of participants indicated that "offensive cyber weapons are a necessary deterrent." 42% of the participants felt their country was capable of waging cyber warfare; 47% felt their country was not (11% unsure).

⁶ 64% of participants indicated that consumers are unaware of the security risks when using information and communications technology.

⁷ Participant responses for the biggest problem area for cybersecurity: political/policy (36%), technical (27%), business and legal (16% each), and legal (5%).

⁸ 56% of participants indicated that that privacy is not sufficiently protected in their country.

⁹ 59% indicated that the protection of youth is worth the cost of some limitations of freedom of expression.

transcends all borders and requires strong international dialogue, trust and cooperation.

- i. **Economics.** While the above aspects are considered, it is important to take into account the economics behind achieving cybersecurity cooperation. Who will pay for security? Can incentives be created for corporations and individuals?

After identifying the problems as well as bottlenecks in international cyber cooperation, delegates delved into a more detailed analysis of some of the key cybersecurity issues in breakout groups. Those groups focused on international cooperation, cyber warfare, the possibility of an international cyber treaty, the setting up of an umbrella organization on cybersecurity and the problem of lack of definitions in cyberspace.

Cyber Warfare

Discussing the problems associated with cyber warfare, some delegates argued that there needs to be a clear definition what ‘cyber peace’ means, but it cannot mean absence of planning for information warfare. Unlike during the Cold War, co-existence does not automatically mean collaboration in cyberspace. Key issues that need to be resolved surrounding cyber warfare are *Ius ad Bellum*, *Ius in Bello*, the right to self-defense and a possible distinction between offensive and defensive operations in cyberspace. Participants argued that there is an urgent need to formulate an international strategy and response to cyber attacks that parallels the traditional laws governing the land, sea, and air.

There are three levels of information warfare that need to be regulated: political, military-strategic and military-tactical. The last (meaning electronic warfare assets oriented to single enemy targets or groupings in a localized vicinity) is often overlooked. If there were an ability to demonstrate a specific entity's or a foreign government's complicity in an attack, what are the options for response? ¹⁰ For example, as a participant pointed out, the United States has long declared that a physical attack on it is an act of war that will be met with retaliation. How should that same principle be contemplated in the context of Internet attacks in cyberspace? Should our cyber policies hold a hosting state responsible for attacks launched by its agents, sanctioned or not? Is the response to a cyber attack limited to the cyber world or are physical responses on the table? These questions need to be debated further.

Lack of Awareness and Definitions

There is a clear lack of a commonly agreed definition of what cybersecurity means. Internet security, cybersecurity, and network security should not be lumped together because each of these has its own particular meaning. All states treat cybersecurity as a domestic issue and hence definitions and legal frameworks vary across nations, which makes international cooperation difficult.

In addition, many users do not understand how exposed they are to technologies that may be vulnerable to attack. One participant cited the statistic that 87% of Americans recently surveyed

¹⁰ 55% of participants were most concerned about cyber attacks coming from non-government organizations (including terrorists and organized crime).

believe they have never used a cloud computing service, while at the same time 65% of the same population surveyed admits to regularly using web-based e-mail. Most users do not understand how susceptible cloud-based services are to attack, and consequently they do not take even the most fundamental steps to safeguard their systems and protect their data.

Consequently, there is a need for education awareness, capacity and trust building, as well as systematic training of key policy makers and the overall population, along with the development of proper legislation and cooperation in educating and standardizing cybersecurity concepts, according to some participants. There was also a call for separate metrics to be put in place to evaluate the progress of international standardization.

Cyber Treaty?

Some suggested the setting up of a legal framework (Cyber Convention) that will be more comprehensive than current international legislation such as the Council of Europe Convention on Cybercrime. There is, however, a need to find a consensus agreement on the definition of threats, before switching to global frameworks. There is also a need for education awareness, capacity and trust building, as well as systematic training of judges, development of proper legislation and introduction of a reciprocity clause smoothing international cooperation.

Many opposed a global convention, arguing that there are already sufficient legal instruments such as the Council of Europe Convention and the UN protocol on cybersecurity. Some participants argued that the convention of Europe is already outdated and that post 2001 technical changes have to be taken into account. For an international treaty on cybersecurity to succeed, the establishment of effective domestic legal frameworks is essential, not least in the area of enforcement.

Participants from India pointed out that New Delhi has introduced comprehensive cyber security legislation after the Mumbai terrorist attack in 2008. Originally, Indian IT law was specially designed to promote e-commerce, but this legislation (based on the Council of Europe Budapest Convention) has recently been extended to cyber crime and cyber terrorism. For example, cyber terrorism is punishable as a serious crime carrying a life sentence.

In the United States several bodies have already been working on cyber crime issues (e.g. American Bar Association-appointed special cyber persecutors). These bodies often rely on already existing provisions (consumer protection, network violations etc.), which are applied to cyber crimes in child pornography, and identity theft cases. However, formal U.S. participation in any new international treaty on cybercrime is certain to face major domestic political hurdles.

Regional Organizations Forum

Aside from their membership in the United Nations, most countries are also members of regional organizations. Based on the recommendation from the ITU High Level Expert Group (HLEG), participants discussed the establishment of a global conference for international or regional organizations and relevant private industries to discuss and jointly formulate policy on cybersecurity and cybercrime.

The purpose of such a forum would be to exchange information and reach a common understanding on principles and standards for the global combat against cyberthreats. Those threats include massive and coordinated cyber attacks against countries critical information infrastructure, and terrorist use of the Internet. The regional organizations may then be able to assist and draft guidelines for their member countries.

Several regional organizations have been identified, and at least 12 organizations (OSCE, NATO, etc.) are of relevance for reaching a common understanding and coordination on principles and standards for the global struggle against cyber crime. The strategy for solutions may unite the existing regional initiatives and bring the organizations together with the goal of proposing global solutions.

Goal 2: To stimulate progressive improvement in the way global cybersecurity is reviewed, managed, and implemented.

A number of delegates argued that complacency is a very big problem when it comes to raising awareness for cybersecurity: "Nations take for granted the Internet is going to be 'on' for the rest of our lives. It may not necessarily be so," one delegate pointed out. "Imagine the Internet being down for two to four weeks," another participant said. "This would 'rain disaster' on online businesses as well as transport, industry and governmental surveillance systems." In the words of another participant: "It may take a big shock of an event to wake people out of their complacency, something equal to a 9/11 in cyberspace." With those considerations in mind, delegates set out to formulate a set of recommendations to spur international cooperation in cyberspace.

Policy Recommendations

Participants emphasized that only cooperation among major powers will be able to establish international regimes and provide 'public goods' aimed at reducing the vulnerabilities of modern society to disruptions originating from cyberspace.

In order for 'cyber cooperation' to start between major powers and to deal with mutual suspicions, policy makers should initiate a bottom-up strategy for international cooperation, which emphasizes cooperation on the technical/tactical level and then move on to strategic issues in international cooperation on cybersecurity. For example, the United States, Russia and China have much to gain from cooperation in combating cybercrime, or protecting undersea cables, which are the underpinning of international information society.

Another field of cooperation could be 'authentication requirements' (electronic signatures), which should be put in place proportional to risks of individual networks and take into account the individual's right to privacy. Authentication requirements have been problematic for policy makers everywhere. Discovering the origins of cyber attacks is very difficult. Even if an IP address is obtained, there is no certainty that it was the true source of the attack or just a compromised computer (a zombie), or one link in a chain of computers. Single states and law enforcement agencies are often powerless in the face of these new transnational threats. In addition, there are serious concerns in many societies about allowing governments to require complete attribution, since this could be used to control political activism on the Internet.

Delegates said imaginative messages explaining the importance of online protection are needed, tailored to different age groups and audiences. They should be transmitted in a variety of ways ranging from TV advertising and school curriculums to YouTube, Second Life, social network sites and video games. Other recommendations included:

- Focus on problems where there is community of interest (technical issues, spam etc.) in order to find consensus and build trust.
- Create an umbrella organization (U-15) that integrates the 12 regional organizations around the world that deal with cybersecurity. Current institutions such as the United Nations and G-8 are seen as not committed enough or having too little influence to genuinely advance international cooperation in cybersecurity.
- Begin private-public dialogue in finding solutions. The Basel II model was cited and can serve as an example for the way ahead (voluntary rating system of best practices, rewards for institutions that implement standards that reduce risk).
- Pay attention to critical international infrastructure (e.g. underwater sea cables) whose oversight and vital dependencies go beyond that of an individual nation-state or existing intergovernmental organization. Such infrastructure should be identified as critical international infrastructure -- mutual cooperation among nation-state stakeholders should be developed to ensure its appropriate prioritization and protection.
- A new focus on Africa is necessary, since the lack of legislation and supervision on the African continent will pose an increasing security challenge to modern information society. New undersea capacity being landed in Africa at present is massive but it is largely unregulated.
- A coordination centre between information response teams of different countries should be established so it can act in case of a cyber catastrophe. An integrated information management approach at the global level is needed.
- Cyber technology can also be used in other ways, such as applications for humanitarian efforts and to find victims under debris. There should be a meeting of the minds on the international level to create a 'safety blanket' when a disaster happens. After the Mumbai attacks, twitter feeds were used and interpreted by intelligence agencies for rushing out forces or to bring relief to victims.
- Countries, especially in Asia, need to be more sensitized to the lack of a legal framework to regulate cyberspace and to combat cyber crimes. Asia is experiencing a proliferation of malware and spyware. More and more spam is sent from Asia because most countries lack legal provisions to regulate spam.

Goal 3: Bring together leading policy makers, specialists, business executives, community leaders and journalists from around the world for discussions to

define and understand international cybersecurity approaches, concerns and solutions.

The multilateral cybersecurity consultation sessions brought together policymakers, specialists, business executives, community leaders and journalists from five “titans”: China, Europe, India, Russia and the United States, as well as other international representatives. In an effort to stimulate progressive improvement in the way cybersecurity is managed and reviewed, recommendations generated from this conference (see list above) will be brought before relevant governments, international institutions and actors in leading business circles.

Two of the keynote addresses at EWI’s seventh annual Worldwide Security Conference were given by former U.S. Secretary of Homeland Security Michael Chertoff and Dell Services President Peter Altabef. Chertoff called for stronger public-private partnerships, increased awareness and greater international cooperation on cybersecurity, while Altabef emphasized governance, technology and education as the cornerstones of more effective cybersecurity solutions.

Keynote Speech: Michael Chertoff, former United States Secretary for Homeland Security

Michael Chertoff, former United States Secretary for Homeland Security argued that the cornerstone of our 21st century economy is the ability to employ computers to transact business and operate our infrastructure. The dependence on cyberspace means that the underlying infrastructure and networks must be reliable and resilient – in other words, secure from failure, compromise, data manipulation, and theft. Focusing on the United States, the key points of his address were:

a.) In the U.S. there are no well-defined responsibilities for maintaining common situational awareness of emerging critical operational developments in cyber space.

In order to build more effective capabilities to prevent, detect, respond to, and mitigate against cyber attacks, it is imperative that key stakeholders in the public and private sectors continually search for meaningful ways to work together and to draw on each other’s strengths.

b.) In a cyber crisis, the United States lacks an effective decision-making framework below the cabinet level for coordinating the government’s response and recovery from a devastating cyber event.

The United States, Michael Chertoff pointed out, must fully fund and complete the implementation of the U.S. Cybersecurity Initiative which addresses this issue, and which places responsibility for network defense not only on the government, but also on operators of critical cyber infrastructure in the private domain.

c.) There is no user friendly process to facilitate private-public sector collaboration in the United States to defend against cyber.

Chertoff pointed out that civilians are on the front lines because personal communications and network systems are the conduits for Internet warfare. This means that the responsibility

for cybersecurity must not only be a joint effort primarily involving our governments' national security and homeland security elements and private enterprise, but it must also be an individual responsibility to practice safe computing.

Keynote Speech: Dell Services President Peter Altabef

Dell Services President Peter Altabef, in his keynote speech on 18 February, argued that governance, technology and education are the cornerstones of more effective cybersecurity solutions. He pointed out that the Internet is fulfilling long-held hopes of humankind: Distance learning, telemedicine, e-commerce, virtual communities, and instant global communications are now established realities. The Internet also can dramatically improve productivity. As a result, information and communications technology is now embedded at the core of operations for governments, financial systems, industries and critical infrastructure. Parallel with these benefits, we have seen the emergence of more sinister aspects of technological progress. The malicious and criminal use of cyberspace today is stunning in its scope and innovation. In addition, Altabef argued that an often overlooked consideration is the risk that the increasing rates and scale of cyber attacks threaten to undermine essential trust -- trust among nations, commercial and non-commercial institutions, and individuals -- trust that is necessary for economies and societies to promote the common good. Altabef identified three key points that need to be considered when talking about cybersecurity, technological progress and international cooperation:

a.) Cyber threats emerge in tandem with cyber benefits.

The real leap forward with the Internet was liberating information from the constraints of volume and cost. Yet in the past two decades, some of the most brilliant minds in technology have fought each other to protect – or to attack -- cyberspace. Despite the rapid growth in cyber security, cyber criminals have become a permanent part of the Internet's ecosystem.

b.) Current cybersecurity solutions are essential and significant, but broader efforts are also necessary.

Three basic elements required for security are governance, technology and education. Governance ranges from regularly changing passwords on a personal account to intensely complex and multi-layered security defenses across large organizations.

Altabef pointed out that individuals must have opportunities to educate themselves about cybersecurity risks and how to deal with them. He further argued that moving forward, security must be designed into new software and hardware products from the earliest planning stages.

c.) Interconnectedness mandates multilateral coordination

Altabef pointed out that there are efforts to move in this direction, including multilateral cybersecurity initiatives within the UN, the OECD, the European Union and other entities. The challenges include finding an effective balance between security and civil liberties as well as the specific and sometimes conflicting interests of different governments and constituents. Despite sincere efforts, a cohesive and coordinated approach that reflects existing political structures has remained elusive at the regional – much less global – level.

Other delegates further emphasized the need for new paths in cybersecurity. "Every user of the internet has a vested interest in keeping it secure as failure to do so risks losing all benefit," argued one delegate. To that end, he wants to set up an industry initiative that works with governments to create a more secure Internet.

Another participant said that failure to regulate could perpetuate cyber "failed states." He cited impoverished countries where customers can purchase unregistered SIM cards with mobile Internet capability, giving them the ability to commit online crime such as identify theft against people in rich nations without fear of being traced.

Summing up the conference, there was a clear agreement that Track 1 diplomacy on worldwide cybersecurity cooperation is not working well and practically non-existent on the strategic level. The majority of experts stressed that there is an urgent need for Track 2 diplomacy to help kick-start international cooperation on cybersecurity. An essential element will be trust building, which can only be achieved through a bottom-up approach, starting with cooperation on small technical issues and then moving to more controversial strategic problems. One delegate voiced his concern that it might already be too late for bottom-up approaches and that more top-down methods are needed. Nevertheless, as long as Track 1 diplomacy fails to deliver results, Track 2 initiatives will have to lay the groundwork for international cooperation.