



WORLDWIDE CYBERSECURITY INITIATIVE

TOP 5 BREAKTHROUGH GROUPS

EXECUTIVE SUMMARY

20 September 2010

P R E F A C E

In May of 2010, the EastWest Institute (EWI), with the technical co-sponsorship of the IEEE, convened over 400 stakeholders and subject matter experts from more than 40 countries for the first Worldwide Cybersecurity Summit in Dallas. Their focus was on solving critical international policy roadblocks that are major impediments to cyberspace safety, stability and security. The attached 5 areas were prioritized amongst more than 25 that were discussed in the Summit's working program. Prioritization was based on the degrees to which: the matter is international, the problem is policy-related, progress is stalled or non-existent, a solution would bring benefit, the subject is being neglected, the needed technologies are mature and business support is feasible. Each of these is being actively worked among international communities of interest with the aim of progressing through the stages of dialogue and understanding to consensus and action.

In parallel to these 5 breakthrough efforts, are (a) several breakthrough efforts related to the 12 recommendations of the Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) report; and (b) other subjects being carried on from Dallas, such as international cooperation for protecting youth in cyberspace, harmonized international legal frameworks and the use of information and communications technology (ICT) in international emergency response to catastrophes.

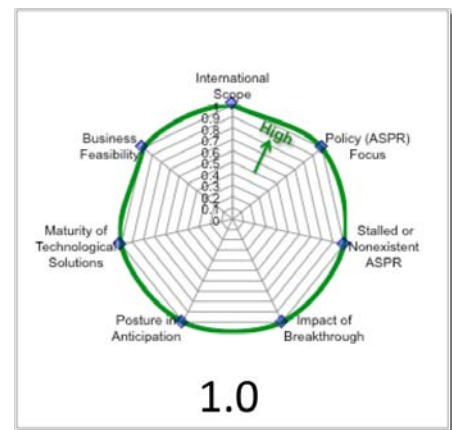
International Priority Communications (IPC) Policy

Despite international technical standards having been developed, the world lacks an international priority communications capability because policies do not exist to guide their implementation. As a result, the world's government and private sector decision makers have less than acceptable probability of completing critical communications during an international crisis. What could be a 90% blocking rate for all calls on public networks during a crisis could be addressed with proven technical solutions so that 90% of essential calls are completed.

The Institute has raised awareness of this under discussed vulnerability, is currently convening world-class experts and stakeholders to work out policy solutions, and will champion the mobilization of resources to implement an international priority communications capability.

More background

Next generation networks are increasingly exposed to the potential for massive congestion that would impair services, including the most important communications. This increased exposure is introduced primarily by emerging bandwidth-intense applications such as imaging, video and gaming. Historic experiences have demonstrated the enormous demand for communications in the midst of catastrophes (Australian wildfires, China's 2010 Qinghai and Sichuan earthquakes, Hurricane Katrina, July 7 London bombing, Mumbai terrorist attack, September 11 terrorist attacks, Thailand Tsunami, etc.). When implemented effectively, national-level priority communications have proved to be indispensable for government authorities and private sector emergency responders. All major catastrophes can benefit substantially from international assistance.



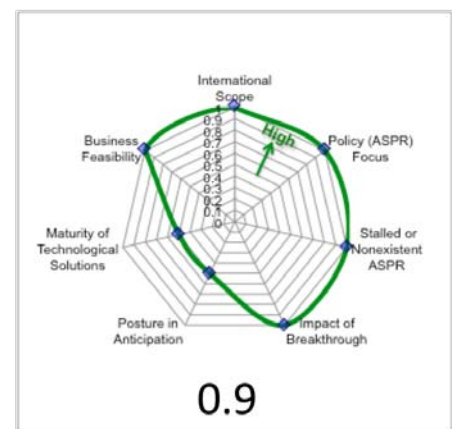
Cyber Conflict Policy and Rules of the Road

The most fundamental aspects of military conflict policies have yet to be developed for cyberspace. Such a state of affairs is an invitation for unnecessary escalation should an act of aggression be perceived.

The Institute has established Track II bi-laterals with key nation-states (e.g., China, Russia, U.S.) and is working through cooperative dialogue that begins with trust-building and moves into the most difficult subject matter requiring cooperation. EWI will continue to work with senior officials in governments as well as private sector stakeholders to develop the underpinnings for the much needed policy in this arena.

More background

The U.S. establishment of a Cyber Command in May of 2010 suffices as evidence that military conflict in cyberspace is a real and present danger. It is a huge concern because defense and civilian infrastructures are highly intertwined and exposed due to their utter dependence on information and communications technology (ICT), and because nation-states are investing in offensive capabilities. Policies are complicated because the identification of an attacker can be extremely difficult.



Trusted Cybersecurity Information Sharing

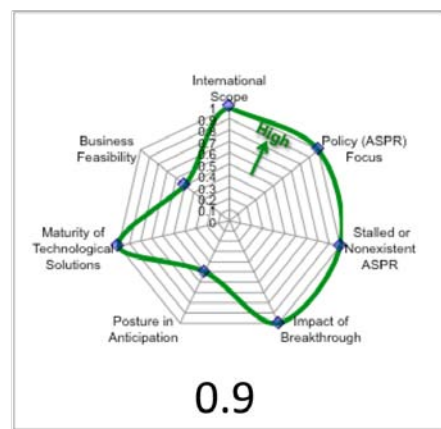
The best assessments of the frequency and damages of cybersecurity breaches are incomplete. No one knows how bad the impact really is, yet the trends – increased complexity, increased connectivity, and increased criticality – are all forces that will make the problem worse. At the same time, the most effective practices for promoting cybersecurity are shared to a limited degree. The establishment of a trusted environment for information sharing of cybersecurity compromises and best current practices is needed to make our shared cyberspace more safe, stable and secure.

The Institute is working with stakeholders to develop new models for trusted information sharing. A key part of this initiative is encouraging bold private sector leadership in its partnership with the government.

More background

Legitimate commercial and other interests impede transparency of cybersecurity breaches. Financial institutions and retail stores have reputations and customer’s interests to protect. Government and medical agencies have related concerns.

Information sharing communities have proven to be highly beneficial, when effectively implemented and nurtured. However, existing communities are fragmented and vary widely in the level of robust exchange. The value proposition for participants must be strong. Given the expertise and ownership of the private sector, its leadership will be essential.



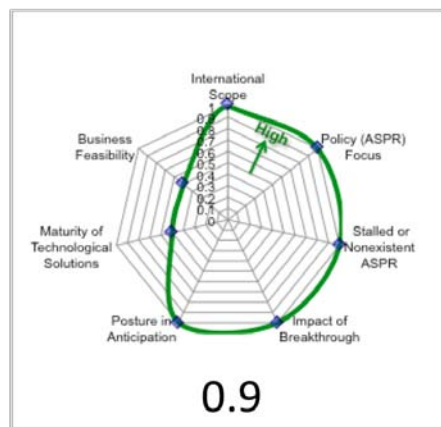
ICT Development Supply Chain Integrity

There are insufficient mechanisms to evaluate the trustworthiness of information and communications technology systems. The current situation has governments, businesses and individuals in profound dependence on countless systems without performing due diligence, relative to what is at stake. Government stakeholders indicate a willingness to utilize evaluation methods if they can be confirmed as being effective measures. The complex international nature of these supply chains requires an international approach.

The Institute has a special focus on the international policy aspect of this challenge, is convening leading technical experts and senior private sector leaders to develop consensus-based mechanisms and incentives, and will mobilize governments and other resources around the implementation of the guidance to be developed.

More background

The reliability and security of this technology is imperative for public safety, economic stability and national security. However, the hardware and software that make up the fabric of cyberspace is designed, developed and deployed with a highly complex integration of supply chains that span the globe. Such complexity is extremely difficult to control. In addition, the realities of competitive market pressures and business profit objectives inadvertently detract from reliability and security considerations. The infusion of mistrust amongst traditional and emerging competitors and adversaries further complicates the landscape.



Worldwide Cyber Response Coordination Capability

The world's capacity to swiftly and decisively respond to a major crisis in cyberspace is limited by the contour and level of cooperation among nation-states, as well as by the lack of anticipation and preparation for an event requiring multi-national cooperation. The impact should such weakness be exposed could easily include devastating, long-term economic instability and well as endangered public welfare and national security.

The Institute is convening government and private sector stakeholders to develop breakthrough measures toward building a broader and more robust international capability.

More background

The current capacity for emergency response is quite mature. There are over 50 national Computer Emergency Response Teams (CERTs) worldwide. In addition, each of the private sector's global equipment suppliers support cyberspace with around the clock technical support teams. However, the needed intensity of cooperation exceeds the threshold attained by business driven technical support centers and the national-level emergency response teams.

In addition to 24 x 7 points of contact, alternative *modes of contact* are needed, as the Internet and telephone communications may be impaired during a major international cyber crisis.

