REMARKS AS FOR DELIVERY

Bruce W. McConnell
Senior Vice President
EastWest Institute

At the Open Group Trusted Technology Forum, Baltimore
July 20, 2015

The State of International Cooperation in Cyberspace

Thank you, Allen, and thank you in addition to my colleague Sally Long who suggested that you might be interested in my perspective today.

I understand that this is the gazillionth event produced by Maggie Roth and her team. Congratulations. Maggie tells me the key to success is that "the right people" come to this event – so, welcome!

I encourage you to continue this important work. Conferences such as this one are critical to making cyberspace a safe and secure place for people around the world to work and live.

I will be speaking for about **35** minutes, in order to leave more time for discussion. My plan is to wander around backstage – behind the scenes in the world of global cyberspace policy – and tell you some of my impressions about the backstory that shows up in the press – mostly as hype about how the world is coming to an end any day now. Well, it sells newspapers!

I am Bruce McConnell, Senior Vice President of the EastWest Institute in New York.

EWI was established 35 years ago when "East-West" meant the Soviet Union and the United States.

In its early years, EWI enabled quiet conversations between military and political forces from both sides – the Warsaw Pact and NATO – during the collapse of the Soviet Union, to assist in a peaceful transition and successful reunification of Germany.

Later, we worked in Eastern Europe to assist the new governments of the former Soviet Union in collaborating on economic reforms.

Today, we have a global program. For example, we are working with the Russians to reduce narcotics flows out of Afghanistan, and we are working with India, Pakistan, and their neighbors to promote commerce and trade in South West Asia.

In China, we host a party-to-party dialogue between the Chinese Communist Party and the U.S. Democratic and Republican parties. And we also host a military-to-military dialogue between retired senior generals from the China and the U.S.

Six years ago we began work in cyberspace security. I came to EWI two years ago from the U.S. Department of Homeland Security where I was in charge of cybersecurity for the U.S. critical infrastructure.

Cybersecurity is a global issue involving many countries. We work with the major cyber powers – the U.S., China, Russia, India, and Europe – and with global technology companies.

Every year, EastWest produces an annual invitation-only cyber cooperation Summit that brings together 300 people from over 40 countries to work together for two days to improve the level of cooperation around the world on key cyber issues. Last year the Summit was in Berlin, co-hosted by the German government. This year it is in New York.

The Summit is the annual capstone of ongong work that we sponsor using our tried and true methodology – convene, reframe, mobilize. We bring the right people together, we reframe the issues so that solutions can emerge, and then we organize support for the recommended solutions in capitals and corporate headquarters around the world.

Our work to date has shortened repair times for and increased the resilience of undersea cable infrastructure, reduced spam on a global basis, kick-started and advanced conversations about how the rules of international law apply to cyber weapons, and promoted international cooperation on cyber incident reponse.

We make progress using small groups of experts, which we call breakthrough groups, that meet through out the year in person and electronically.

Today I am going to focus on the situation of cooperation among nations and companies in global cyberspace. I will begin by paying particular attention to relationships between China and the U.S. I choose these two countries because together they make up more than half of the world's Internet users, and because the tensions between the two in cyberspace are at an unacceptable level.

The theme of this conference is "Boundaryless Informaiton Flows." The meeting materials explain. "Boundaryless does not mean there are no boundaries -- it means that boundaries are permeable to enable business." We face increasing challenges in making this happen between the U.S. and China.

The EastWest Institue works especially directly with China on cyber issues. For example, we have worked closely with the Internet Society of China to reduce the incidence of spam and malware that affect networks globally. We are cooperating with two different Chinese non-profits on cyber arms control and incident response. And, I am frequently in Beijing and Washington to discuss ways of improving the dialogue between the China and the U.S. on cyberspace issues.

We are at a historical low point in the relationship. There is an unprecedented lack of trust and a lack of mutual understanding. This is a serious situation, and one that must be rememdied.

Cyberspace is the source of great economic and social benefits, and a wonderful incubator of collaboration and innovation. Its peaceful operation is of great benefit to mankind.

As Chinese Foreign Minister WANG Yi said earlier this year at the National Peoples Congress, cyberspace should become a new frontier of our cooperation rather than a new source of friction.

We must break through this impasse. In order to address this problem, it is useful to ask, "How did we get here?"

There has been considerable friction between the two countries on cyber issues over the past ten years. The US complains about repeated breaches of the computer systems of US manufacturing companies and theft of their industrial secrets by attackers who appear, at least in the eyes of US authorities, to be based in China.

The Chinese are similarly unhappy about the surveillance activities of the government that were revealed by Edward Snowden.

So there is frustration on both sides.

On the US side, the frustration was that the Chinese government was unable or unwilling to do anything to stop these attacks from continuing.

This frustration led the US Justice Department to announce the indictment of five PLA officers for alleged theft of US industrial secrets.

The Chinese government responded by suspending the government-to-government cyber working group established by President XI and President Obama in Sunnylands, California. So now the two major powers are not using the major vehicle that was estabilshed for talking to each other about security issues in this very important area of human endeavor.

First, it is my personal view that the US should not have issued these indictments. They are unprecedented in international relations.

Second, even if the US believed it was necesssary to issue these indictments, the US did not warn the Chinese that it was going to take this action. The Chinese view is that the working group would have been a good place to bring this evidence to the table for investigation and discussion.

Third, there is no immediate practical effect of this US action. It is really a symbolic action. The issue deserves more serious treatment. And, we cannot make progress on this issue, or on any issue, if you are not talking.

On the bright side, I would note that the visit to the United States of President Xi Jinpeng in September is creating pressure on both sides for progress, so the situation is not hopeless.

Toward the end of my remarks today, I will suggest some areas where I think China and the US could work together to improve the overall stability and security of cyberspace.

To arrive at that place I want to address six general questions.

---

1. What are the biggest security problems in today's cyberspace?

This is an easy question, because it actually was answered – in part – by US Director of National Intelligence, General Clapper, on February 26, 2015.

In the annual "Worldwide Threat Assessment of the US Intelligence Community," he states that cyber threats to US national and economic security are increasing in frequency, scale, sophistication, and severity of impact. The ranges of cyber threat actors, methods of attack, targeted systems, and victims are also expanding. However the likelihood of a catastrophic attack from any particular actor is remote at this time.

The Assessment foresees an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security.

While I would agree with these statements, I do not think they go far enough.

There are more complicated security problems in cyberspace. Each of these problems undermines the stability and predictability of the infrastructure that all citizens around the world depend on for many critical goods and services.

I have listed four here, including the inability of countries to respond to incidents across borders, to cooperate effectively on cyber crimes, to create norms and rules of behavior in cyberspace, and even to agree on the way that the Internet will be governed and managed. I will discuss these issues in more detail in a few minutes.

But the bottom line is, as security professionals, we have a lot of work to do to secure cyberspace!

2. As the world's leading cyber power, how does America enhance her cybersecurity?

As you know, in the US we place a great deal of emphasis on the responsibility of the private sector. We involve government in the economic dynamics of the market only as a last resort. We prefer to allow market mechanisms to allocate the creation and distribution of goods and services to the greatest extent possible.

Historically, the US has followed this approach with respect to cybersecurity. For example, the US Department of Commerce last year released a Cybersecurity Framework, which explains to companies how they can better secure their systems.

As a general matter, the use of this Framework is voluntary, not mandatory.

Instead of requiring companies to comply with the Framework, the government is expecting that market mechanisms will encourage its adoption. And that is already happening.

Insurance companies are starting to use the Framework as a basis for evaluating the cybersecurity practices of companies and setting the price for the insurance based on the extent to which companies are complying with the Framework.

Similarly, large corporate customers of banks and stock exchanges are starting to require their banks and other financial service providers to explain their level of compliance with the Framework.

So, the voluntary approach is starting to work in the private sector.

However, in some critical areas of health and safety, such as the nuclear power industry, the government does set mandatory cybersecurity standards. So far, this is the exception, not the rule. But if the voluntary approach does not work, I would expect we will see a more regulatory approach over time.

As far as the cybersecurity of government systems, that is the responsibility of the Department of Homeland Security, except that the military is responsible for protecting its own systems.

As we all know, there is a long way to go to successfully defend commercial and government systems from attack. One change that we believe would be helpful would be if the core technology that security professionals are trying to defend was more secure to begin with!

Consistent with this market-based approach, one of the EWI breakthrough groups is working on increasing the availability of secure ICT products and services. (ICT = information and communications technologies.)

We are taking a two prong approach to improving the market signals that are sent to the providers of ICT products and services.

First, we are encouraging those providers to use recognized and proven international standards and best practices that improve product and service integrity.

Second, for the buyers of ICT, we are promoting the use of procurement practices that are founded on recognized and proven standards and best practices for secure ICT.

This breakthrough group is being co-chaired by senior security professionals from Microsoft, Huawei Technologies, and the Open Group – Sally Long continues to be a major force in this work.

---

3. Is there national sovereignty in cyberspace?

I just talked about what is happening in the U.S. and earlier we talked about the Chinese. Around the world, we are taking a national approach to improving cyberspace. But will that work?

One of the interesting things about ICT is that it is not very respectful of boundaries of any kind. Indeed, ICT leads to the erosion of boundaries inside organizations and between organizations.

Inside many organizations, people no longer follow the strict chain of command when communicating. They will communicate directly with their peers, or they will skip over several levels of middle managers and send emails directly to senior management.

This change in behavior is creating tension inside organizations because the old roles are not necessarily respected.

It also can make the organization much more nimble, more agile, and more creative.

This shift in organizational philosophy has driven the innovation that created Silicon Valley, and it is affecting the structure of warfighting doctrine in the US military.

This lack of respect for boundaries also applies between organizations, and, in particular, between nations.

Nations are struggling to maintain the old notion of national sovereignty in the face of technology that does not care about where it sends information.

It would be overly simplistic to say the US position on sovereignty in cyberspace is clear cut. In some areas, the US does exercise sovereignty – for example in the area of taxation of electronic commerce and in import and export controls of technology.

In other areas, such as the free flow of political opinion, the US is less interested in controlling what Americans can see on the Internet, with the exception of child pornography.

Other countries have different approaches. Many countries, including China, India, and Russia, see a threat to political stability coming from the Internet, and are working to limit the risk stemming from that threat. And in Europe, there is increasing attention to this problem – particularly the use of the Internet by terrorists.

In this way, the Internet has become a proxy, and a catalyst, for a larger global conversation and disagreement around political, cultural, and social values.

In other words, it is not the about the Internet, it's about the information. And here's a prime example.

Every June in Strasbourg, France, 300 police, prosecutors, judges, diplomats, attorneys, and engineers from around the world meet to find better ways to combat cyber-enabled crime. I call it "cyber-enabled" because there is really very little "cybercrime." Most cybercrimes are just regular crimes – theft, fraud, destruction of property -- committed with electronic tools over the Internet. It's still the safest way to rob a bank.

But this year, the talk had shifted to a new dimension, criminal speech. How to prevent terrorist recruitment and violence facilitated by the Internet is now Topic A among cyber cops, especially in Europe. In the shadow of Snowden's revelations, it's a tough conversation. How much should the police be allowed to watch the people? Where are the lines between political speech, incitement to violence, and propaganda? What responsibilities do powerful platforms like Facebook play?

Today, European legislatures are moving to pass invasive surveillance laws, which, history teaches, will be abused. It took the US over ten years to temper the most extreme provisions of the Patriot Act. Europe, the cradle of human rights, must now find its own middle ground, while staying true to its values.

To help make that happen – not just in Europe but around the world, EWI is collaborating with a Paris-based organization, the Internet Jurisdiction Project. Our breakthrough group on Managing Objectionable Content is focused on Internet activity is illegal in one country but not in another. For example, it is illegal in France to advertise Nazi paraphernalia over the Internet, but not in the U.S. As a result, normal criminal assistance procedures between countries do not apply. When a person in France sees that kind of content using an Internet platform owned by a U.S. company such as Yahoo or Facebook, this can leave the foreign cyber crime investigator out in the cold. So we are working on procedures to make it easier to enforce local laws where the content is delivered, no matter where the provider is based.

---

4. <u>What can we learn about security in cyberspace from security in the "real" physical world?</u>

So I want to step away from these tough policy issues for a few minutes and explore an area that I think can be helpful for anyone trying to explain cybersecurity to a non-technical person. And that is by using analogies to the physical world.

This question – the similarities and differences between cyberspace and the physical world – is very interesting to me.

I have been using an analogy lately to illustrate the similarities and differences between the two when talking to non-technical audiences. I wonder what you think of this.

I ask them to compare the security measures on a different network that they are familiar with – airline transportation – and security on the Internet.

I like this analogy because the size of the air transport industry and the size of the electronic data transport industry are roughly the same size. But the value of goods and services transported on the Internet is 100 times greater than the value transported on airplanes.

And yet the security of air transport is much greater.

To get on an airplane, you need to prove your identity, but on the Internet, you can be anyone from anywhere.

To operate an airplane you need a license, but anyone can operate a computer. Similarly, to sell an airplane, you need to put the equipment through rigorous testing and certification, unlike anything that is required for computers.

Then there is the International Civil Aviation Organization, which sets standards for, and conducts inspections of, air traffic control facilities around the world. Nothing like that here, yet.

Finally, it is illegal under international law to shoot down a commercial airplane, but there is no agreement about what kinds of offensive actions are legal in cyberspace.

Analogies like this can help analyze the problem and determine whether or not a different approach is needed than what we are doing today.

Another comparison can be made – this time between cyberspace and outer space.

In outer space, like in cyberspace, it is impossible for an outside party to determine what is a weapon. A communications satellite may appear to be a peaceful device, but it may also be used to disable communications between the satellites of an adversary.

Similarly, a peaceful satellite can be turned into a kinetic weapon simply by detonating it and creating space debris.

Because of this property of satellites, international negotiating teams have been unable to come to agreement about the definition of space weapons. And they will face a similar problem defining cyber weapons.

For that reason, the EastWest Institute advocates adopting limitations on targets and levels of effects from cyber attacks, rather than trying to control cyber weapons.

Last year we recommended that States agree not to attack civilian nuclear facilities. And this year we expect our breakthrough group on cyber armaments to expand that recommendation to include major attacks on stock exchanges, financial clearinghouses, and the core infrastructure of the Internet.

---

5. What are some productive and fruitful areas of cooperation among nations in cybersecurity and cyberspace relations?

So, with all these problems, where is there room for progress – between the US and China, and among nations generally.There is serious lack of trust and confidence, so we should work on improving that.

I would like to suggest three areas of work that might be helpful in this regard.

First, nations should find ways of cooperating during cyber incidents.

There is actually already a bright spot in the relationship in this area. In the case of the recent attacks on Sony Entertainment perpetrated by North Korea, some of the servers used to mount the attacks were based on Chinese territory.

Once the United States learned about the attacks, it contacted Chinese counterparts and provided information about the servers that had been compromised by the North Koreans.

The Chinese took action to mitigate the risk from those servers.

This kind of cooperation should be expanded and procedures should be developed in terms of what kind of information should be exchanged between countries seeking assistance in a cyber incident.

One of our breakthrough groups is working on developing a standard request form that will draw on the work being done under STYX and TAXII. This form, and the related protocols, would specify what data elements should be included in a CERT-to-CERT request and what kind of reponse should be expected.

The second area of work has to do with reducing the risk of cyber attacks on critical infrastructure.

The United Nations Group of Government Experts on Cyber Issues has been discussing the applicability of the Law of Armed Conflict in cyberspace. At their most recent meeting in New York last month, 20 governments agreed on a set of general principles. While the report has not yet been made public, we understand that the governments involved remain wide apart, but there is some progress.

I mentioned a few minutes ago the lack of rules of engagement when it comes to cyber attacks on critical infrastructure. I also mentioned that the EastWest Institute is proposing examples of targets and levels of effect that should not be allowed. In addition to this work, our breakthrough group is working with Chinese and Russian think tanks to analyze existing proposals, such as the NATO Tallinn Manual and the Shanghai Cooperation Organization's Code of Conduct, to see where there are similarities and differences that could advance the conversation. These efforts complement the official work being done under United Nations auspices.

A third area is in cyber-enabled crime.

We talked earlier about actions where there is no mutual criminality across borders. But as I mentioned earlier, most crime on the Internet is just regular crime – theft or fraud – that is illegal just about everywhere. Organized crime is increasingly using the Internet to fund its other activities such as drug, weapons, or human trafficking. Here we face a situaiton where we have a 21st century crime scene – volatile evidence and wily attackers who change their identities daily. And we have 19th century procedures, that require lengthy written documents to be exchanged in order to share investigative leads and evidence. Morevoer, Internet companies do not always make it easy for law endforcment to get in touch with them when they may have evidence in their servers. This needs to change.

Here we have a breakthrough group led by the FBI, the European Cyber Crime Center, and a major Internet Service Provider that is working on a standard form and other measures to streamline these cooperation requests. And we are developing recommended set of information that companies should make public to make it easier for law enforcement to connect with the people in the company who are responsible for these matters.

---

6. <u>What institutions are needed to make all this work?</u>

I want to conclude with some more philosophical remarks about the state of play in global goverance and our approach to a broad range of secuirty issues… The world is becoming smaller every day, and, as Adlai Stevenson said over 50 years ago, we can no longer afford to live as strangers.

For many in the world, including eight of the world's ten most-populous nations, the post-World War II institutions were formed without their real participation. These institutions, formed by the victorious Allied powers, have served humanity remarkably well for 70 years. But in their current form they are losing legitimacy, and the breakdown in respect for the rule of international law is a symptom of an accelerating global shift in concepts of power and order. As Chinese Premier Li Keqiang suggested in recent remarks in Beijing, reform is needed, and a greater voice must be given to the global South.

In the United States, our national government suffers from its own crisis of legitimacy, created primarily by our legislature, and its inability to accomplish the basic tasks of governance such as enacting budgets, and fed by an increasing partisanship and loss of a sense of common purpose. As the leader of the free world and founding partner of the existing world order, America today retains a diminishing claim to moral and political leadership on the global stage, even while it remains the most sought after destination for immigrants from the rest of the world.

This crisis of context is being accelerated by technology, with its explosion of transparency, its stimulation of expectations of participation, its power to flatten organizational management structures, and its ability to support collaboration across boundaries of all kinds.

This democratization of information access is a direct threat to authoritarian regimes, which work hard to control its impact. But it is also a threat to industrial-age structures of any scale, whether private or public.

A Chinese investment banker observed to me recently that the advent of smart phones has created 600 million citizen journalists, undercutting the role of the party cadres as information sources for the Center, and supporting President Xi's ambitious and impressive anti-corruption campaign. Another senior Chinese, a government researcher, opined that "the erosion of boundaries means the only remaining potential enemy of the State is the people."

Of course it is important to note that the Network can also be used to create a distributed control system that strengthens centralization of management. As the latest Russian military strategy states:

> Strengthening of centralization and automation of military forces and weaponry on the basis of transition from the old system of rigidly vertical command management system to global networked automated systems of management of military forces and arms.

The crisis of context goes beyond traditional security issues – both internal and external – that national and international institutions are finding difficult to address effectively. As Susan Rice commented last year in an address entitled *America's Future in Asia*, "many of Asia's most vexing security challenges are transnational security threats that transcend borders: climate change, piracy, infectious disease, transnational crime, cyber theft, and the modern-day slavery of human trafficking." For each of these a patchwork of formal and ad hoc arrangements is struggling to address the risks. Yet, these arrangements, which supplement the industrial age institutions, are key to the transition to a new order.

We need to continue to explore alternative institutions that can take the place of those that are proving incapable.

There is a role here for experimentation. For example, in April 2013 the government of Brazil hosted an international town-hall meeting – "NetMundial" – on the of cyberspace. The 1,480 participants from 97 nations, convened under the banner of "multistakeholderism," ranged from ambassadors to academicians, from Microsoft engineers to a Chilean non-profit promoting the right of digital access. As I wrote then:

> Multistakeholderism, like many young life forms, is an awkward and somewhat tentative thing. Seven languages spoken with consecutive translation, four sectors represented plus the remote hubs, representatives standing in line to make two-minute interventions, and the open observation of the small drafting groups produced a slow and only "rough" consensus. And, with no governmental representatives on the drafting groups, one had the unique experience of seeing Canadian, German and U.S. cyber ambassadors leaning in, straining to hear the deliberations.

Clearly such a mechanism is not ready to be applied to dangerous security or pressing economic problems. But then, neither was the League of Nations. It took one failure, and a second World War, before we came up with the current world order.

Today we face a major rebalancing of power relationships. The first, I have discussed in some detail, State-to-State relations and the need to recognize the rapidly emerging role of the global South. Let me briefly comment on two other rebalancings. The second is public-private. In cyberspace particularly, States are not the only major cyber powers – private companies, mostly US Internet and technology giants – have considerable power in cyberspace as well, more than many countries. This conflict needs to be resolved peacefully.

The third is the relationship between individuals and organizations, whether the State or large companies. There is a shift here that we do not yet understand, a shift accelerated by the technology we have been talking about this morning. This is the topic of another speech, another time. But it is not going away.

We have a long road ahead, and we must cover it quickly. With luck, diligence and goodwill, we will not require two world wars to cement the transition to a system that supports each stakeholder taking its common, yet differentiated, responsibility.

Conclusion.

In conclusion, I want to summarize briefly my point of view.

Cyberspace is a critical area of human endeavor. It underpins the global economy. It is therefore very important for it to be peaceful, stable, and predictable.

As a retired Chinese Major General told me, the current situation is like two people who are approaching each other on a road in the middle of the night. The people cannot see each other well, so each is concerned that the other may be a demon, not a person.

This General suggested that we need to turn on the lights. This means talking to each other – not remaining in our respective capitals and assuming the other side is a demon.

Therefore, all of us here today should take responsibility for working to improve the safety and stability of cyberspace, to make it an area of cooperation, not a source of friction.

Thank you for your attention this morning, and I look forward to the discussion.