2017 Annual Security Review Conference
27-29 June 2017
Session 4

PC.NGO/5/17
27 June 2017

ENGLISH only

Transnational Security Governance and Cyberspace Security

Bruce McConnell, Global Vice President, EastWest Institute

June 2017

Four years ago US national security advisor Susan Rice observed that the world'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." Today, one could add migration, violent extremism, the safety of fissile nuclear materials, and overall information security to that list.

These issues share at least two characteristics: First they are accentuated in their severity by modern technology. The bad guys, both state and non-state actors, are well equipped with the latest computers, communications equipment, and weaponry, and their ability to use these tools is enhanced by their access to global networks.

Second, no international regimes or institutions have these transborder issues well in hand. Rather, global bodies like the World Health Organization or the International Telecommunication Union are generally struggling to remain relevant. The post-war structures that have kept peace for 70 years face a crisis of legitimacy as rising powers that were not present at Bretton Woods scorn the old order and create their own institutions and power centers.

The Cyber Arms Race and Information Warfare

Today we are focusing on security and cyberspace. Cyber-enabled attacks in the lead-up to the U.S. Presidential election roiled relationships in Washington and globally. The term cyber-enabled emphasizes a new characteristic of cyberspace -- it's no longer its own thing. It's part of everything. There is very little actual "cyber crime." Instead, we see a plethora of ordinary crimes and attacks: theft, fraud, trespassing and destruction of property that use cyber means.

From a geopolitical standpoint, this cyber-enablement has produced a runaway cyber arms race, led by the United States, Russia, China, Iran, Israel, and some European countries, with many others, including North Korea, following close behind. Over thirty countries have formed cyber offense units. Non-state actors such as organized criminal gangs and the Islamic State are also players.

The U.S. Democratic National Committee hacks and related incidents consist of burglary and publication of the fruits on Wikileaks. From a legal standpoint, while it is against U.S. law to enter a computer without authorization, these incidents may fall more into the shadow zone of espionage. As for the publication, the U.S. Supreme Court has generally protected media publication of accurate, stolen materials of public interest obtained by a third party.

What's new for Americans is the possibility that there is an "information war" between East and West. Indeed, some states do not use the term cybersecurity, preferring the broader term "information security."

The events around the U.S. election have evoked a global conversation around fake news, political trolling, social media bots, and the weaponization of intelligence.

On the other hand, we have recently seen additional evidence regarding Western cyber actions against North Korean missile systems and the CIA's capabilities. Even assuming the most benign motivations by all parties, these continuing, ungoverned state-on-state skirmishes in cyberspace increasingly undermine terrestrial security and stability.

In contrast to cyberspace, other international domains are governed by norms of behavior and international law. In the airspace it is illegal to shoot down a commercial aircraft. But in cyberspace, the way in which international law applies is still being debated.

In commercial aviation we have organizations like the private sector International Air Transport Association and the governmental International Commercial Aviation Organization that partner to maintain safety and security on a global basis. There are no comparable institutions for cyberspace.

Everyone in this room is painfully familiar with the provisions that keep that network secure: identity proofing of everyone who gets close to a passenger plane, licensing of pilots, filing of flight plans, certification of aircraft, etc. We have none of these things in cyberspace. Yet the financial value of the commercial transactions conducted over the Internet (and here I'm not even counting SWIFT and other special purpose networks) is actually 100 times greater on an annual basis than the value of goods transported in the air cargo system.

Progress is modest. A group of governmental cyber experts has worked at the United Nations for over 10 years to come up with an initial set of non-binding norms of behavior in cyberspace.

These include:

- Not allowing the use of information and communications technology, or ICT, to intentionally damage another country's critical infrastructure.
- Not allowing international cyber attacks to emanate from their territory.
- Responding to requests for assistance from another country that has been attacked by computers in the first country.
- Preventing the proliferation of malicious tools and techniques and the use of harmful hidden functions.
- Encouraging responsible reporting of ICT vulnerabilities and sharing associated information.
- Not harming the information systems of the authorized cybersecurity incident response teams.

In February 2017, the government of the Netherlands, with the support of Microsoft, the Internet Society, the EastWest Institute, and the Hague Centre for Strategic Studies, launched the Global Commission on the Stability of Cyberspace. The GCSC is chaired by Marina Kaljurand, former Estonian foreign minister, and co-chaired by Michael Chertoff, former US Secretary of Homeland Security and Latha Reddy, India's former deputy national security adviser. This multistakeholder commission will build on and extend existing efforts to develop and advocate for norms and polices to enhance international security and stability and guide responsible state and non-state behavior in cyberspace.

On the private sector side, global ICT companies are beginning to step up to the responsibility that comes with their great power in cyberspace. For example, Microsoft recently issued a set of norms of industry behavior that global ICT companies should follow in their business practices.
Examples of the kinds of norms that companies are considering include:

- Creating more secure products and services.
- Not enabling states to weaken the security of commercial, mass-market ICT products and services.
- Practicing responsible vulnerability disclosure.
- Collaborating to defend their customers against and recover from serious cyber attacks.
- Issuing updates to protect their customers no matter where the customer is located.

Clearly, the industry is at an immature stage. Its rapid growth in importance has outstripped systems of governance, including the first line of defense – the market. As a general matter, until very recently customers demanded two things from the firms that supply ICTs – price and features. The market has responded, giving us all manner of convenience and efficiency, in business and in our private lives. Finally, however, buyers are starting to recognize the criticality of ICT to their daily activities, and thus they demand, and may be willing to pay for, security.

Yet there is a gap between what they need and what they are able to command. To address this gap, we recently published a "Buyers Guide for Secure ICT."[1] This guide recommends questions that buyers can ask ICT suppliers to help them evaluate the security of the products and services that these suppliers deliver.

Despite best efforts, the reality of today's dynamic technological environment -- with product cycles of 18 months or less – continues to challenge policy development. Two developments are dramatically altering the security picture.

First, we are moving to the cloud. We store our information there on virtual machines operated by major providers like Amazon Web Services. While AWS and Microsoft's Azure provide much stronger cybersecurity and resilience than any single enterprise can field, they also create systemic risk, with large potential consequences from technology failures or attacks.

A second emerging source of risk is the Internet of Everything (IoE). In a few years there will be ten times as many devices -- Fitbits, heart monitors, automobiles, thermostats, machine tools and floodgates -- connected to the Internet than today's smartphones and computers. These devices, when combined

[1] "Purchasing Secure ICT Products and Services: A Buyers Guide," EastWest Institute, September 2016, https://www.eastwest.ngo/sites/default/files/EWI_BuyersGuide.pdf.

with 3-D printing, promise to disruptively transform manufacturing and transportation. They will also create a ubiquitous, global sensor network that will be communicating what is going on everywhere. And these sensors are shockingly insecure -- built with easy to guess passwords, transmitting their data unencrypted, and being essentially un-patchable.

The conventional wisdom is that the IoE represents a massive increase in the attack surface. But at EWI, we are exploring two questions. First, why do we assume the bad guys will own the sensor network? Why not have the good guys own it and use the knowledge of what is happening on the Internet to increase security -- for example, by isolating problems and fixing them before they can spread? Second, we ask, how will the IoE shift the balance between endpoint and network security, and what are the societal implications of that shift?

There is much to be done in cyberspace to make it, and the information we all rely on, trustworthy and secure. I will be happy to get into some of those issues during the discussion. The question becomes, what institutional constructs are needed to ensure that work gets done?

Sovereignty and its Alternatives

One of the existing constructs that no longer serves us in the networked age is sovereignty, at least as defined by the Treaty of Westphalia that ended the Thirty Years War, in 1648. We need new forms and combinations of local and global leadership and participation. Since Westphalia, sovereignty has been focused primarily on protecting territory from outside forces. Today, we stand in a time of transition, balancing this traditional emphasis with a newer one based on states' responsibility to citizens for what happens *within* their borders.

It is not that borders do not exist, but borders matter differently than they have before. Take cyberspace, for example. It is impossible to define in what country the domain citibank.com actually resides, not to mention where the tens of thousands of cyber attacks each day on that domain come from. This ambiguity makes it difficult for individual states to enforce the law in cyberspace. We need networked responses to networked threats.

One example of the creation of a new form of governance relevant to cyberspace was last year's transfer of Internet traffic routing management from U.S. control to an international, multi-party, multi-sector governance community. The result is a complex structure that only a geek could love. But, it is also a real-time experiment in so-called multi-stakeholder governance, and well worth watching.

For the shorter-term, however, as states turn inward and transnational challenges multiply, we face an urgent need for institutions that can act globally in an agile manner, or at least with more agility than governments. Currently, the only existing organizations that can approach that agility are large, global corporations. Admittedly, they are not ideal—they have conflicts of interest based on their focus on returning shareholder value.

Of course, states have conflicts of interest as well when it comes to global issues, rooted as they are in territory. Nevertheless, companies, such as Coca-Cola, are increasingly investing in the future. Coke needs clean water resources in Africa—it will not be in business there in 20 years if there is not clean water. Microsoft practices and advocates for responsible behavior by large technology companies to reduce conflict and increase stability in cyberspace.

Power in the 21st Century

These challenges and responses relate directly to the nature of power in the 21st century. We are living in the networked age. The value of networks increases as more people become members. In my view, we are reaching a critical mass of interconnectedness in the developed world, and the rest of the world will be there in the next 10 years. But critical mass for what effects?

Not even the most civic-minded would advocate for direct democracy by everyday citizens on the complex questions that face our planet and our societies. That is why we have professional politicians and expert agencies, at least on a good day. What we do need, however, are ways to help those officials get to more nuanced answers. This is already happening on the local level in Europe and the U.S. where experts brief randomly selected civic councils to help them come up with advice for elected officials on a broad range of issues, from refugee assimilation to sustainability planning.

For these kinds of conversations to happen globally, we need to harness the technology that is increasingly connecting us. How can corporations help? Could firms host objective global forums that deal with some of the issues that will affect their bottom line and the rest of us with them? Perhaps some of the lessons learned from the trend to open, collaborative innovation networks—as practiced by DuPont, BT and other firms—may apply here.

National Security and Global Security

While global security issues are becoming salient for the long-term, in the short-term, national security "stories" dominate national security policy. I use the term "stories" to distinguish rhetoric from actuality—both in terms of action and in terms of effectiveness. The increasing attractiveness to mainstream politicians and electorates of fear-based, nationalistic narratives does not always translate into action—and when it does, such actions do not always improve national security. For example, Xi Jinping's government discriminates against U.S. technology companies in rhetoric, but the implementation is much more measured. And as far as the effects, banning world-class technology does little to improve global confidence in the Chinese banking sector.

The principal reason for this trend is that our planet is shrinking—people everywhere are feeling increasingly impinged by alien cultures, values and populations. Certainly, this is understandable in Europe given the weak economy and the rapid influx of hard-to assimilate refugees. But even when there are not a lot of new people coming, digital information from around the world affronts and disrupts our attention. And so in democracies, many people find the echo chamber of like-minded voices or the seductive addition to a constant feed of electronic news more comfortable. The networked age is not easy to live in. Meanwhile, dictators—like cult leaders—always shield their subjects, and themselves, from diverse viewpoints.

Nationalist isolationism does not do well against threats that cut across borders, like migration and terrorism. ISIS is a global threat network, as we have seen this year in Paris and London. Networked threats require networked responses. Until we get this right, humanity will continue to lose ground against the forces of atavism, cynicism and hopelessness. We cannot let this happen on our collective watch.