World Summit on the Information Society (WSIS) Forum 2016
International Telecommunication Union (ITU)

May 5, 2016

"Action Line C5 (Building Confidence and Security in the Use of ICTs) - National Cybersecurity Strategies for Sustainable Development"

Event Synopsis: *Building and ensuring trust in cyberspace is top of mind for global leaders, and reinforcing collaboration among the various stakeholders is key to achieving all of the seventeen Sustainable Development Goals (SDGs) set by the United Nations in September 2015. In particular, universal and affordable access to ICTs was recognized as pivotal for bringing the 2030 Sustainable Development Agenda forward. Increased ICT uptake and Internet connectivity, however, is not sufficient, let alone sustainable, if the underlying infrastructure and the devices connected to it are not safe and secure.*

The WSIS Outcome Review Process, which culminated in the adoption of the "Outcome document of the High-Level meeting of the UN General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society" in December 2015, reiterated the importance of Building Confidence and Security in the use of ICTs. It further recognized the challenges that countries, in particular developing countries, face in building confidence and security and called for renewed focus in capacity building and awareness raising among users of ICTs, particularly among the poorest and most vulnerable.

This session brought together various stakeholders to discuss how comprehensive national cybersecurity strategies at an early connectivity stage are an essential first step for a successful transition to a safe and sustainable digital ecosystem, and what the role of the different players within a country should and can be in that process.

Formal remarks as given by Melissa Hathaway, Potomac Institute for Policy Studies

"I am very honored to be here today and I would like to thank the ITU for inviting me to this important discussion.

Developing comprehensive national cybersecurity strategies is really about aligning agendas and aligning a country's economic vision with its national security imperatives. Countries' development initiatives and many of the digital agendas that these nations are currently pursuing are founded on bringing about high-speed communications to every citizen and to every last mile in order to be that platform for commerce, to generate and drive innovation, to enable new forms of communications and education for citizens, and overall drive economic health and well-being. Countries are connecting each and every part of their society, whether it is their transportation system, electric grid, agriculture systems, etc. to the Internet in order to enable and drive that productivity, efficiency, as hopefully GDP growth along with the modernization of their core society.

Those digital agendas are generally being pursued differently and separately from the countries' cybersecurity agendas, and they are not in aligned. And therefore then, **no**

country is cyber ready. Indeed, one part is being pursued for economic growth and well-being, and a second part for security and necessary resilience. When thinking about what is important for national cybersecurity strategies and sustainable development, it is important to **align the two agendas**.

If you look at many countries around the world, most of them are pursuing a digital agenda as the primary initiative and a cybersecurity agenda as a second, third, or not even on the agenda.

So, how do we align those agendas around the economics? Countries ought to realize that they will be unable to achieve the growth that they hope for unless security and resilience are built in.

At present, it is estimated that there is a $3.6 trillion opportunity in the marketplace for embedding ICTs into core infrastructures and driving communication to the last mile. In the next four years, as countries pursue the Internet of Things (IoT), it is expected that there will be a $19 trillion opportunity globally. And then, over the course of the next 10 years, countries will see at least a $32 trillion opportunity as they modernize all their core infrastructures and drive their digital agenda.

But who, and how many among those countries driving digital agendas, are actually measuring the losses they are experiencing from cybercrime, fraud, intellectual property theft, business disruption, and even property destruction? The ITU Secretary General mentioned this morning the losses from stolen records. However, it is not just the loss of personal identifiable information or the losses from fragile banking systems that are easily hijacked, or the disruption of power grids that we witnessed in Ukraine—all of these events have overall costs to countries and are eroding the trust in ICT, eroding GDP value, and eroding development agendas. Some countries are actually starting to measure this. The Netherlands, for example, has measured that they are losing at least 2% of their GDP to intellectual property theft and fraud. The United States has measured that it is losing at least 1% of its GDP to intellectual property theft alone.

I would argue that all countries around the world are losing a minimum of 1% of their GDP to *cyber insecurity,* and the more connected a country is without building the security and resiliency in, the more a country has to lose. And over the course of the next 10 years, as countries connect more essential services and critical infrastructure to the Internet and embed ICT in, they will also have to align their digital agenda with their security agenda. Only then will they will actually be able to realize the development agenda that we all hope for. To reach that goal, I have developed a Cyber Readiness Index (CRI)—a comprehensive, comparative, experience-based methodology to help national leaders chart a path toward a safer, more resilient digital future—and am now partnering with the ITU to drive those efforts.

The CRI 2.0 studies 125 countries, and we are currently in the process of publishing detailed country studies. The CRI underscores that the digital agenda is not aligned with the security and cybersecurity agendas anywhere around the world, and I expect that you will see that gap emerge even further as countries become more connected. The CRI 2.0 is based on seven essential elements, each of them connected to economics:

1. A **National Cybersecurity Strategy** that aligns the digital agenda with the national security agenda, or at least a digital agenda with security and resiliency at its core. Within that, it has to be measured within GDP—it has to exemplify how it is enabling the GDP growth and then measure the GDP losses associated with cyber insecurity, fragmentation, or fragility of core infrastructure.
2. **Incident Response** capabilities, so that if a country experiences an incident—like the one recently experienced by Qatar and its National Bank, or the United States and its government system, or Ukraine and its core electric grid—it can rely on its national incident response capabilities to respond to the incident and restore government or business continuity. A country should also rely on partnerships with industry, since industry is designed to operate and restore those critical infrastructure.
3. **E-crime and Law Enforcement**—as countries experience more crime and fraud and their critical infrastructure becomes more infected with botnets and the like, to what extent are they encouraging law enforcement to develop capability? To what extent are they developing e-crime laws? And at what point are Internet Service Providers (ISPs) and telecommunication systems going to be accountable for the infected infrastructures in their respective countries, and be required to clean it up so that those infected infrastructure can't cause crime against core businesses and core economic systems?
4. **Information Sharing**—governments and industry alike have exquisite information about what is going on in cyberspace. Bi-directional information sharing systems ought to become a reality. However, if government continues to classify all of its information, then it cannot be shared. And if all of industry information is proprietary then it cannot be shared either. 'All boats will not rise if the future of the IoT unless we start sharing that information and threat information.'
5. **Investment in Cyber R&D**—many countries are already pursuing innovation and research agendas because they see the market value of pursuing innovation to address cyber insecurity. Those countries that are pursuing research and development initiatives are finding that, when government and industry partner, they are going to learn more, and produce more, and ultimately capture more of the market share.
6. **Diplomacy and Trade**—cybersecurity and cyber insecurity are core to the trade and economic agendas. Cybersecurity is coming about in all trade negotiations. But how many of countries' trade negotiators actually understand that the free flow of capital, services, data, and goods is all dependent on the Internet? Few.

So, when countries start to look at trade negotiations, they should look at what the security and economic opportunity components of those negotiations are, and make sure that they represent both sides of the deal, so that they don't negotiate one over the other or subordinate one to the other.

7. **Defense and Crisis Response**—in the event of a national crisis, has that country developed a national capability, wherever it may sit in the government, to defend itself and to restore critical services and operations, outside of a one-off incident? These are emerging capabilities that many countries are starting to develop.

To conclude, when I think about what it takes for a national cybersecurity strategy and the future of sustainable development, it is not just the digital agenda; it is an overall balanced agenda that has security components, and security and resilience at its core.

* *

Questions on encryption and erosion of trust

In 1998, the United States took encryption off of the export control list in order to enable an e-commerce and global economy for trusted transactions. This decision was about enabling the technologies to enable trust and instill confidence into the platform. Over the course of the last 20 years, we have been very clever about how we could manipulate the technology. Citizens, corporations, and governments alike are all eroding the trust on the backbone of the Internet that we have all become dependent upon. Whether it is citizens taking it to the airwaves of the Internet to protest policies that they don't agree with, or to find a Zero-Day exploit to attack a particular infrastructure; or whether it is a corporation that chooses to steal the intellectual property to affect its competitors, or decides to expose governments' operations; or whether it is a government that does the same and the like against a corporation or citizen, the erosion of trust is now occurring at an exponential pace.

The CRI 2.0, which is available in all of the official UN languages, is about raising awareness and measuring the positive aspects of the Internet and of becoming connected and embedding ICTs in all parts of society, while also pushing countries to measure the losses due to cyber insecurity. When countries start to measure their insecurity, whether created by a backdoor in the technology or vulnerability in the system, and their losses, they cannot be ignored. Unfortunately, most of our countries and companies today are primarily driven by the economic opportunity and efficiency, the promise of GDP growth, profits, and margins. If they were to start treating this as a balance sheet, however, they would be measuring both the positive and the negative input. This would get the attention of ALL leaders; whether is the Situation Room at the White House or the Board Room at a corporation—they could not ignore it! It is key to communicate these issues in terms of both the positive and the negative aspects, but most of our countries right now are only looking through one set of lenses.