Internet Society™

Cybersecurity: Speech Given at the Embassy of the Kingdom of the Netherlands in Washington D.C.

Thanks Martijn for that introduction, and thanks to Ambassador Jones-Bos and to the Netherlands Office for Science and Technology for inviting me to speak.

Good evening. Since so many of you have spent today talking about how you might collaborate on cybersecurity, and about specific technical projects you may be working on, I thought I'd take a step back and provide a perspective on why cybersecurity is such a huge issue, why the stakes are so high and the answers so difficult.

Today, more than two billion people around the world are online. That's two billion people who are relying on the Internet to be a trusted place to get and share information. Some subset of those two billion are using the Internet to buy real or digital goods, collaborate with business partners, and handle the tasks of everyday life, like paying their bills.

Yet many people still worry about the security of their online transactions and whether their privacy is being protected. The endless stream of news stories about cyber attacks contributes to these concerns.

Tonight, I'll lay out pieces of the cybersecurity puzzle, and put them in context of the Internet's fundamental principles. I'll end by offering a framework for policymaking that I believe will be useful in preserving those principles.

I'll start with a basic question. What is cybersecurity?

If you ask a friend or neighbor, you'll get one answer—maybe having to do with concerns over their credit card data being stolen or having gone too far in a Facebook posting that could be read by a prospective employer. If you ask parents, they will tell you they worry about what a child might be looking at, or the possibility that the child is the victim of cyber-bullying or on the receiving end of "sext" messages.

This is a view of the end user, but it’s just one perspective.

For businesses, cybersecurity has other implications— companies all need to safeguard customer information, protect commercial data, or prevent intrusions and damage to their corporate networks. Yet the business perspective of cybersecurity is far from uniform; companies vary widely in their specific needs, expectations, and sophistication. A small business may not be concerned about the same things that General Electric is concerned about, and the auto industry may not have the same cybersecurity requirements as a health care provider that relies on e-health records.

And then there is the government perspective, which has to take into account the concerns of citizens and businesses while also dealing with any national security threats that an Internet attack might pose. With many government services and national physical infrastructures increasingly tied to the Internet, the disruptive potential of a cyber attack is significant. The Minister reminded us of this, this morning, with his recounting of the details of last summer's Diginotar crisis in the Netherlands.

Governments' approaches to cybersecurity, like industries, aren't always the same. Among other things, they vary with the country's geographic location and economic development.

For example there are differences between developed and developing countries in how they address cybersecurity. Those of us who live in developed countries have gotten used to inexpensive bandwidth and relatively easy access to security software. Doesn't mean we always take advantage of it, but it's there.

In many developing nations, unlimited access for a set fee isn't a given. Users often pay more as their use goes up, so things like spam imposes costs on people who can least afford it. Neither, in some cases, can they afford to download regular antivirus updates. In places where electricity is unreliable, an attempt to download new software can turn into a costly failure if the power shuts off.

There are other important differences in emerging economies. People access the Internet through wireless services, and Internet users in these countries are much more likely to get on the Internet at a cybercafé or community access points like libraries. These modes of access are extremely important for people who might otherwise never be able to get online.

But these modes of connecting have certain risks. Cybercafes can be especially problematic, because of the possibility that private information will be available to other users who sit down a few minutes later at the same computer. In Uganda, criminals took advantage of this, methodically recording online banking transactions made at cybercafés.

For all of these reasons, a developing country is likely to have a different set of priorities when it comes to the Internet, than a developed nation like the U.S. or the Netherlands. While the U.S. or Netherlands might be most focused on securing advanced computing infrastructure or funding cybersecurity R&D, a developing nation might well be more concerned with developing the technical and policy capacity to deal with online fraud. Many developing countries lack the basic legislative frameworks to address cybercrime, particularly when the crime may not even originate in their countries.

Which of these concerns should be the priority when it comes to our cybersecurity efforts and cybersecurity policy in general? For that matter, how do the diverse concerns of government match up against the security needs of citizens and businesses? I'm not sure that anyone can answer that question, and I certainly wouldn't want to have to prioritize among these stakeholders. They all have legitimate interests, and in many cases, the interests, though specific to them, are also intertwined.

It is the legitimate claims of all of these stakeholder groups that explains why it is so difficult to reach consensus on how to define or address cybersecurity. That doesn’t mean we should throw up our arms in frustration. It just means we have to be smart about how we proceed.

Any framework for tackling cybersecurity needs to work back from an understanding of the different ways in which the Internet is valuable to its different stakeholders.

To practically everyone, the Internet has value as a communications tool and as an engine of economic growth. It also has value as an enabler of social and even political change. What are the principles of the Internet, the building blocks, that give it this flexibility and that we should be sure preserve as we try to develop the right cybersecurity policies?

There are some basic characteristics about the Internet that really matter:

The first is the Internet's **global reach and integrity**. As an Internet user, I have to feel confident that all of the endpoints are connected--that when I type in www.rabobank.com, that's actually the site I go to, and not somewhere else. It's a little like the seal on a bottle of Tylenol, which reassures me that there has been no tampering with what's inside. This integrity is partly a result of a technical specification called DNSSEC, which has been in the news a bit lately because of the impact that the SOPA legislation would have had on DNSSEC. I'll come back to SOPA in a few minutes.

The second core Internet principle is something we at the Internet Society call **permission-less innovation.** Said another way, this is the ability of anyone to create a new service on the Internet without having to get approval from a governing body. Without thinking about this too long, any of us could come up with a long list of online services that might not exist if scientists and entrepreneurs needed to vet their ideas with, say, their local phone company, their national government or the United Nations.

If Tim Berners-Lee had to ask for permission, would the World-Wide Web exist? Would the idea of a Web "spider" have been rejected, cutting off the development of Internet search services such as Google? Would Facebook have 850 million users and be headed for an IPO that could value it at $100 billion? How about Wikipedia and Twitter and Web mapping software and downloadable music and hundreds of other things we take for granted in our daily lives?

A third thing we must preserve is the **accessibility of the Internet**. This goes farther than people's being able to consume whatever legal content they want; it extends to their ability to contribute content, add a server, or attach a new network, as long as they follow the Internet's technical standards.

And the fourth thing to safeguard is the Internet's **spirit of collaboration**. In addressing Internet security issues, we must find a way to get all stakeholders involved, from users, to those of you in the Internet research community, to commercial companies, to policymakers. Solutions developed in isolation either don't solve the problem or cause more harm than good. In some cases they can create significant problems that undermine the stability of the Internet.

The last few months have furnished some clear examples of badly designed policy "solutions" that would impact these core Internet principles. Take SOPA, or the Stop Online Piracy Act, in the United States. SOPA took aim at a legitimate problem of the Internet—

the theft of copyrighted material and trafficking in counterfeit goods. In practice, users who tried to access a site considered illegal under SOPA would have been redirected to a U.S. government Web page—perhaps one run by the Department of Homeland Security – or would not have reached any site at all. This policy would have compromised the implementation of the DNS security protocol, DNSSEC that I alluded to before. The policy would require ISPs to essentially hijack legitimate queries from users and redirect them to a site they didn't ask for. It would cause people to constantly wonder if the website they were directed to was the same as the one they requested. This would have huge implications for Internet security.

The other thing about SOPA is that it would have forced ISPs to block entire domains. Since a single domain can house many unrelated sites, this policy would have impacted all sorts of non-infringing sites. It was, in the end, legislation that would have done far more harm than good, and the Internet community, including my organization and I'm sure many of you here, voiced its disapproval. We were happy when Congress shelved the plan.

Now, we have to turn our attention to the equally controversial ACTA, or anti-counterfeit trade agreement. ACTA is an international treaty whose basic purpose is to provide an international framework and standards for the enforcement of Intellectual Property online and to address the sale of counterfeiting goods via the Internet. As we did with SOPA, the Internet Society has gone on record criticizing ACTA, in particular for the secretive way in which this international accord was developed, with only two of the 11 negotiating texts made public.

Like SOPA though, the most effective pushback appears to be happening at a grass-roots level, with protests in many parts of central and Eastern Europe. ACTA would allow countries to block traffic or content and would give them considerable latitude in defining acts of infringement. The ambiguity of the treaty's language raises the specter of findings of infringement or counterfeiting being used as a pretext for limiting Internet freedom. The protestors have done a good job of making their voices heard: Germany, Poland, Bulgaria, Slovakia, and the Czech Republic have all backed off their pledge to adopt the treaty—at least for now. The Netherlands did the same last week.

It's encouraging to see governments getting the message and reconsidering policies that would undermine the Internet's principles. But it would be unrealistic to expect that all governments are going learn these lessons and stop trying to control this medium.

Five months ago, China, Russia, Tajikistan and Uzbekistan approached the U.N. with a proposal for an International Code of Conduct for Information Security. The proposal included a line about “curbing the dissemination of information" that undermines other countries' "political, economic and social stability, as well as their spiritual and cultural environments.”

From the perspective of most of us in this room, that's obviously too sweeping a guideline; it goes against the grain of the Internet. But it is part of the international context for addressing cybersecurity's challenges. We can't pretend it isn't out there.

Happily, there are goals related to cybersecurity that many countries already agree on.

An Internet security breach, after all, isn’t like a territorial crime, where the consequences are generally limited to the geographic area where it happens. Internet security problems have the potential to spread quickly and widely, something we first learned back in the late 1980s, with the release of the Morris worm that infected 6,000 defense, university and research computers. That was front-page news, at the time.

There have been similar incidents in recent years, some reported and some not, that have caused policymakers everywhere to pay closer attention to network security and look for ways to cooperate across borders.

In particular, many governments are looking to protect vulnerable groups, including children, from online threats and to find ways to empower them to protect themselves. Governments are eager to learn from the best cybersecurity practices of others. And no government should want a cyber criminal who launches an attack from their country to have a safe haven.

Interpol has done some great work in tracking down online criminals. And there are other mechanisms that countries have that reflect their common interests in ensuring the Internet's safety. For instance, there are computer emergency readiness teams—CERT, for short—all over the world, coordinating their countries' efforts and sharing information when there are security incidents.

Last year, when the White House released a document called the International Strategy for Cyberspace, it talked about the importance of getting international research communities “to take on next-generation challenges to cybersecurity.”

The White House position paper also cited the “immediate and long-term benefit” of helping developing nations shore up their own cybersecurity capabilities.

Cooperation between developing and developed nations is already happening.

I was in Trinidad & Tobago last week, meeting with the Caribbean Telecom Union. This is the organization responsible for working with ICT Ministries all over the Caribbean to help them implement Internet-related policies. They have a small staff—four or five people—-highly qualified-and their priority this year is squarely on cybersecurity.

Many Caribbean countries do not have the resources, technical expertise or capacity at the individual government level to forge cybersecurity policy on their own. Yet they don't want technology to pass them by. They want to be a part of the global information economy, but they know that this future depends on their ability to implement some level of cybersecurity. As a result, they are looking for private sector input and advice. They are eager to learn from governments like the U.S. and the Netherlands about what's working and what isn't. They are reaching out to the technical community for technical solutions. Their approach is practical.

There are numerous other examples of international, multistakeholder cooperation on cybersecurity issues that are taking place within the OECD, APEC, the Internet Governance Forum, and the Organization of American States, just to name a few.

So when I talk about information sharing and international cooperation, it isn't just a fancy construct. It's real; it's happening now.

I'd like to close by discussing, more tactically, what we should be doing about cybersecurity. How should we approach it at a policy level?

First, international cooperation -to the extent possible – is essential. The reason for this is clear. If an attack hits a retail company in London, and the perpetrator is in Sarajevo, the malware may have traversed computers in three or four other countries en route to its destination. That's a situation that requires cross-border cooperation.

Cross-border cooperation is also valuable in situations that aren't as high pressure, for instance in avoiding duplication of effort in the development of security technologies or protocols. The Internet Engineering Task Force is a good example of collaborative technical standards development that is open to participation by any expert from around the world. The discussions that happened earlier today among you are another example of positive cooperation that should serve as a catalyst for further innovation.

Second, any policies we come up with should be based on open technical standards. The Internet wouldn't have had the explosive success it has had if the software that has driven its growth weren't easily adaptable for other purposes on the network. Security solutions that are developed within expert communities—again, the IETF is an example—are more likely to be effective and scalable, and consistent with the Internet's basic principals.

Third, the policies we come up with should be flexible enough to evolve over time. We know that the technology is going to change—that's a given. The solutions need to be responsive to new challenges. We don't want to develop a policy in 2012 that is outdated in 2013.

Fourth, the policies need to be developed using a multi-stakeholder model. That means that effective policies can't be unilaterally created by government. They can't reflect a back-room deal worked out by industry leaders. They can't just be the brainchildren of engineers. All of these stakeholders must work together.

Within this policy framework, we should not overlook a few critical values, namely basic privacy protections and freedom of speech.

Privacy protection begins with better awareness and understanding by users of how their information will be collected, used and stored by those they interact with online. I consider myself an experienced online user, yet I struggle to understand the legalese in most online privacy agreements and often don't take the time to read them. If we want people to use the medium, they have to trust it. To trust it they need some basic understandings about what will happen to their personal information and confidence that their expectations will be met.

Freedom of speech is also fundamental to the Internet for reasons that most of us in this room, coming from countries with long traditions of free personal expression, take for granted. People need to be able to share ideas and information and communicate freely; this is what makes the Internet powerful and allows people to innovate. If you institute a cybersecurity policy that disregards freedom of expression, you threaten one of the main things that make the Internet valuable.

The bottom line is that the policies we put in place should not undo the good thing we've got. There's a temptation, in many situations relating to cybersecurity, to be reactive, especially if something has happened that has jeopardized the welfare of a child or compromised financial data, or resulted in major infrastructure damage. We have to remember that it isn't the Internet that does bad things, any more than it is the post office that does bad things or the telecommunications network or transportation system. People sometimes use these mechanisms to do bad things, but it's still people doing them. We shouldn't attack the medium in an effort to deter the crime.

There is one other thing I'd like to add, which is always crucial to the development of good policy. And that is the willingness of those who are developing policy to truly listen to those affected by their decisions.

One of the remarkable things about the Internet is how quickly it allows people to rally around a good idea, or discredit a bad one. Would it be a good idea to develop a cybersecurity technology or policy approach that choked off permission-less innovation? What if cyber policies resulted in an Internet that was carved up along national boundaries?

We could create those things, but they would leave us with a radically diminished platform, one that far fewer people would want to use. I'm not even sure it would be the Internet.

And that, we must not allow.

Thanks for listening—and for being part of this crucial effort, at such an important time
-Sally Wentworth, Dutch Embassy, Feb. 21 2012