Internet Governance Forum
Hyderabad, India
Dimensions of cyber-security and cyber-crime
4 December 2008

Note: The following is the output of the real-time captioning taken during Third Meeting of the IGF, in Hyderabad, India. Although it is largely accurate, in some cases it may be incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the session, but should not be treated as an authoritative record.

>>MARKUS KUMMER: Good morning, ladies and gentlemen. We start now with the panel session on the dimensions of cybersecurity.
But before we start, I would like to urge you to make sure that you hand over your headsets after the session when you go out.
Yesterday, I think there were about 80 headsets missing after the session. Now, we don't suspect anybody of trying to steal the
headsets, but it's also important to hand them back so that they can be recharged.
If we lose 80 headsets after each session, we will not be able to hand them out anymore, and you will not be able to listen to our interpreters.
So please make sure you hand them in after the session.
But let's now move to this panel session. And I pass the microphone to our chairman, Mr. R. Chandrashekhar. He is Special Secretary
in the Ministry of Communications and Information Technology of the government of India.
Please, sir.

>>R. CHANDRASHEKHAR: Thank you, Mr. Markus. Good morning and welcome to the first session on the second day.
I think this is an important, really important, session. We are all aware of how much of Internet has grown and how much the
convenience and benefit of Internet have come to mean for not just civil society, but for researchers, for governments, for commerce,
for the economy in general. So much so that all of these areas are now quite dependent on the Internet.
But this heavy dependence has also brought in its wake some unwelcome attention, creating problems, people who would like to create
problems for this infrastructure which forms the basis of activity in all these key areas of daily life. And it's also not just drawn
attention from people who would like to create problems in the working of the Internet, but this medium itself, the sheer
convenience and benefit, in fact, is available not just for those who want to do good, but equally for those who want to perform acts
which are illegitimate and illegal in any civilized society.
Crime and criminality in any developed society is dealt with through the force of law. But legislative measures are bogged down
by the problems of jurisdiction, geographical boundaries, and also by slow adaptability in a fast-changing technological environment.
And in India, for example, we have been trying to make some changes which Mr. Rai will talk about. And these limitations also imply
that there are a lot of other things which need to be done. And there are a vast number of stakeholders involved at various levels,
and perhaps a lot needs to be done at each of these levels.
We have this morning a panel which collectively represents many of the different stakeholders, many of the people who are involved

in actually managing the Internet at various levels. And the emergence of these threats and the use of the Internet for illegitimate purposes, both of which need to be dealt with, can perhaps be addressed through this panel to raise the issues,
to bring out clearly what are the kind of issues, what are the dimensions of the threat, what are the implications for all the
diverse stakeholders involved, and what are the possible actions which need to be taken both individually and collectively to meet
these threats going forward, especially when we are now talking about trying to reach not just the next billion, but even the last
billion. These issues become even more important. And I think without further ado, we have an exciting panel here, and,
hopefully, from the interventions of each of the panelists, the main issues would be brought out. Hopefully, we will have a
little time left for some questions and answers at the end of the session. And then in-depth discussions at the various workshops which would follow.
So I would like to now turn to the panelists one by one. And would you like to --

>>BERTRAND DE LA CHAPELLE: Maybe we can introduce them as they speak.

>>R. CHANDRASHEKHAR: What we would do is, as each panelist comes up to speak, the panelist would be introduced. And I would
request the moderator to do the honors.
So let's now turn to the first panelist. And I would request you to introduce the first panelist.

>>BERTRAND DE LA CHAPELLE: Thank you very much, Mr. Chair.
It's a great pleasure to be here.
I wanted to make just three quick comments on the methodology. This is a mapping exercise. It is obvious that in an hour and
a half, we will not be able to address in depth, and let alone solve, the questions that we're addressing here. And there will
be an afternoon session, as you know, that will allow further questions. The purpose of this panel today is to present you with a
certain number of perspectives on those questions of cybercrime and cybersecurity. And we hope that the views that will be
presented will help you understand the various dimensions of cybercrime and cybersecurity.
I will turn now to the first speaker, who is Michael Lewis, who is the deputy director of the Q-CERT, the CERT in Qatar, and also
connected to Carnegie-Mellon University.
Michael, can I ask you -- I'm sorry, you are there -- can I ask you to give us a presentation rapidly, and particularly address
the notion of cybersecurity networks.

>>MICHAEL LEWIS: Yes. I'm happy to do so. Thank you, and good morning.
In the interests of time, I'll move fairly quickly. I do have some slides, and I don't expect -- that is, I won't read the slides
to you. I'll just hit the highlights and then you can read them at your leisure later.
I think we all can agree that cybercrime is a growth industry. Yes, that is, users are increasing, the devices, the number of
devices, the range of devices are increasing.
The vulnerabilities associated with these devices are increasing. The exploits based on these vulnerabilities are

increasing,
and now I think a more recent twist that we recognize, the financial incentives and the interest to -- for criminals and for
terrorist has also increased. So this shouldn't be very controversial. But it is worthwhile for us to note that we inherit legacy systems. With those systems come old exploits. Even if we did everything perfectly well starting from today, we would
have to deal with persistent threats over the course of the next couple of generations.
Now, again I'll make the point that it's now fairly easy for someone to become a cybercriminal at many levels. It's easy to get
involved. The rewards are quite high. It's very difficult for law enforcement to move against it. And, really, the innovation
is happening more on the criminal side. As a computer scientist, I'm really impressed by what's happening with some things such
as botnets and these distributed command and control systems. So it's not looking good in this regard.
Now, we should start -- with so much controversy, we should recognize that the Internet is good, but it wasn't really designed
for security. And there is a great deal of dissension about what we mean by security. And I reference here the parable of the
three blind men and the elephant. But in this regard, it's better for us to be proactive than reactive. But because we live in
interesting times, we should prepare for the worst. Incidents happen, they happen all the time. In fact, I presume everyone in
here at one time or another has lost or thought they lost a USB drive. How would you approach your data if you assumed in every
instance that it would be lost or that every message that you sent in clear text would become public?
So everyone at every level is doing something already. But it's better to do it better and in accordance with the growing body
of experience and best practices.
There are some people who have done some very good work. And we should learn from this. And, in particular, we should try to
use relevant and useful standards and policy and adapt them. I think a one-size-fits-all strategy isn't effective. We should
recognize regional, local, cultural issues that may influence the implementation of a security strategy.
And I think it's important for us to develop systems and implement systems that complement and don't compete with each other,
that mutually reinforce. I've come to call this broadly a cybersecurity network. Bertrand mentioned this previously. And many
of the panelists talk about trust, relationships of trust. So I'll give you a couple of examples.
In particular, maybe the question to ask is, when something goes wrong, who do you call?
At any level?
What happens in a crisis? Would someone recognize it when it happens? Do they know what to do? When to do it? And in some
cases, whether or not law enforcement should be involved, and if so, how to engage with law enforcement.
Are the relevant roles defined? There are a number of issues of authority and responsibility and liability that don't really
get raised until there's a crisis. And I would propose that that's precisely the wrong time to try to resolve those issues.
The trusted relations also should be developed in advance. You don't want to think about who to call or work your way through
your box full of business cards of people that you've met at conferences when time matters.
And, again, I think this -- I've mentioned many times that it should be done at all levels, because security, as we know, there's
no silver bullet. It's a question of defense in depth. It needs to be handled from the highest of levels to the more -- the most
mundane and tedious of levels. One possibility, a component of cybersecurity is to address this idea of a computer

security
incident response team. This can exist, again, within an organization, within a sector, at a regional level, a national level.
And they ideally will be more proactive than reactive. But by the very nature of the term, you'll notice they emerged from a
reactive framework. I'll give some credit to Carnegie-Mellon. I'm also employed by Carnegie-Mellon. They were the founder of
the original CERT.
Now, a couple of diagrams to get away from the text. Frontline incident response. Within an organization, when something goes
wrong, there should be somebody inside who handles that. If people go outside the normal channels, then they may violate internal
policies on handling information or on privacy. So it's really quite important to have something inside.
And so the green boxes are people, and that box in the middle could be any entity inside the organization that has the responsibility and is charged with maintaining the system and responding. And this response needs to be formalized. In many
cases, people do these things, they do them perhaps in an ad hoc manner. But it's not as comprehensive as it could be. And maybe
the message of the day is that security is a constant, evolving situation. The threats evolve. The responses evolve. And the organizational approach should also evolve.
Now, within organizations, it's nice to have coordinated and formalized response. But this should also be true at a national
level. And this is the part that I think is often missing. Out of hundreds of CSIRTs in the world, there are a handful that
actually are CSIRTs with national responsibility. If something goes wrong, if there's an attack on systems in my country, coming
from another country, and I can trace this back, whom do I contact in the source country? This often isn't very well defined.
Over time, it should become more defined. And one way, one mechanism to do this is through the formulation of national CSIRTs.
But they are one player amongst many. And I make the point in this slide that a national CSIRT is a necessary but not sufficient
component of any national strategy. You'll notice there are multiple CSIRTs here, in banks, education, ministries. And there
are ought to be a mechanism where they can report and consult with the national center and the national center can push information
to them, simple things, alerts and notices, or notifications of seminars or workshops. But these channels need to exist in
advance. The points of contact need to be established. Secure methods for communication need to be established and tested on
a regular basis, such that they exist in a crisis.
Now, putting this together, this isn't a beautiful diagram, but it tries to capture that at least at a national level, the cybersecurity network has multiple constituencies: End users, organizational response centers, the national center. Notice
that circle in the middle is a region center. You need to work with your neighbors, your trade partners, and the like. And then off to the left, you'll notice law enforcement. There could be engagement with law enforcement at any level. And then
off to the right, we talk about external organizations, such as FIRST, the Forum for Incident Response and Security Teams,
which is, I think, in my estimation, probably the premier organization for this type activity, and organizations such as the
ITU, which has done some very nice work, in particular, the ITU-D initiative, question 22/1 on national frameworks for
cybersecurity.

The point is, they should be consulted and your work could be aligned with them.
Now, I'll move quickly through the rest.
The coordination of this approach, there are ought to be a strategy, there ought to be a program for incident management.
You need to know who your friends are, constituents, and counterparts. And you need to establish these relations. And then
test the system. Conduct regular targeted events. Build the skills and share the experiences.
Now, this slide, this next one, simply demonstrates a particular incident, genericized, it was a DDOS attack on an organization in my domain. And my point here is, anybody something happens, it ought to be reviewed and let it see fresh
air and strong light.
Most of the time when incidents happen, people hide them. That's a bad approach. You can have a program which handles
such things discretely and provides good advice, sound advice. The goal would be early detection, improved response, shortened time frame of the duration of the situation. And at every level, you'd like to try to reduce the impact and improve
from event to event. And perhaps this will lead to recognizing categories of incidents, what should be done and when, provide
people with the right authority. Excuse me. And recognize if there are liability issues. And in some cases, in the response
to the incident, the mitigation of the damage may actually interfere with the follow-up analysis. So the team needs to be
trained in analysis techniques which are forensically safe. You don't want to do the analysis on the original equipment. You might want to do this on images of that equipment such that you don't inadvertently step on your own toes in the follow-up.
Now, the observation at the bottom here has to do with the question that you ought to do this in advance, when you have the
time to do it and the consideration to do it, not when time is of the essence.
I'll also make the observation that you should align -- whoops -- you should align with partners. OWASP, the Open Web
Application Security Group, or the Antiphishing Working Group -- notice here, because I'm in Qatar, we talk about the GCC
and the Arab League, the modern version of law enforcement. Our national ISP, QTEL, I mentioned first. I want to give some
mention to the ITU as well.
So there really needs to be in that circle -- there's a national network inside the country. But there are also external partners, so that this cybersecurity network needs to be broad and deep.
And then a few questions that I'll leave for the afternoon discussion. But there are a number of things we want to think
about: How much security do we actually want or need? What kind of security do we really desire? Are we sometimes
conflating safety with security?
If we implement controls, how do we do it without damaging the actual benefits of the Internet and much of what made it
what it is today?
Should there be anonymity? And if so, how much and when? Who holds the data? Under what guidelines? And then one that seems
to be coming back quite a bit lately is this issue of protecting vulnerable communities, in particular, children. What should
we do there? A full range from awareness to tools.
I leave with you those questions such that in the afternoon session we might come back and touch them in more detail.
Thank you for your time.

>>BERTRAND DE LA CHAPELLE: Thank you very much, Michael, for presenting the first element regarding the cybersecurity network and insisting on the notion of readiness and the preexistence of relationships between the different actors so that monitoring on a regular basis, prevention, and reinforcement of the system of response can be done in times of quiet times, to be ready when the system is submitted to an attack.

I will now turn to Marc Goodman, who is director of international cooperation, the center of policy and international cooperation and also responsible for the international multilateral partnership against cyber threat.

Marc, can you, in particular, highlight the distinctions between handling cybercrime as opposed to handling crime in the traditional environment, what law enforcement actors, you've also been working with Interpol in the past. And if you can relate it to your personal experience, that would be great. Thank you.

>>MARC GOODMAN: Thank you very much, Bertrand.

I have some slides that I brought along with me to sort of illustrate these problems. And I'm happy to show them to you now.

From my perspective, hopefully, today, I can share with you where law enforcement is on these topics.

One of the biggest questions up-front is a definitional one, what is a cybercrime, what's cyber terrorism, what's a cyber threat? And why should we care about any of these? I won't spend our time here looking at these definitions. Just to say that there are many definitions out there. We are reaching some agreement, and the work continues.

The first point I would like to make is the fact that traditional crime has moved online. So any crime that you can think of in the real world, whether it be money laundering, sexual exploitation of children, gambling, intellectual property theft, identity theft, extortion, threats, illegal drugs, prostitution, all of these are occurring in cyberspace with great success, I'm saddened to say.

So what we had is criminals taking good advantage of technology and just improving their operations.

The next form of cybercrime that we have seen are sort of the new crimes. These are the crimes that could not exist were it not for computers and computer networks.

So prior to computers or, perhaps, telephone networks, there was no hacking; right? That's a relatively new phenomenon.

Some of our other speakers, Michael spoke about denial of service attacks. Viruses. Now we are seeing increased sophistication of phishing, botnet armies, terrorist use of the Internet, and an area I am interested in, crime in virtual world, which is sort of Web 2.0, 3.0 forms of criminality.

Whatever we do, I can tell you the criminals are several steps ahead of us or next to us.

Another form of Internet threat or technical threat to consider on both the national and the local level are critical infrastructure threats. Michael talked about the increasing amount of networking of technologies, and what we have seen is that, increasingly, government systems, whether they be air traffic control, banking, energy, national security, all of these are connected to networks.

And so if those networks become penetrated, there are threats that need to be considered. And I just want to say that these are not theoretical threats. There was a famous case in Queensland, Australia where a former employee hacked into the water sewage system in one of the states in Australia and was able to release raw sewage throughout Australia. Many of you will be familiar with the Estonia attacks of recent time. And in Massachusetts, about ten years ago, somebody got control

of the
air traffic control tower in a small airport in Massachusetts and were able to disable the runway landing lights, all remotely
via a network connection.
So these threats are quite real.
One of the latest ones, and perhaps very relevant today as we have our conference here, is terrorist use of the Internet. And this is everything from publication of ideologies online, propaganda, the raising of funds, recruiting new members,
intimidation campaigns. We have all seen these terrible videos online of beheadings. The terrorists are taking full advantage
of the technology that's out there and using it for operational planning to make their terrorist attacks more efficient, sadly.
And so this is something that we need to be aware of.
Of course, each of these technologies has a positive use as well. But they are being used for negatives and for criminal activity.
I want to make a point that Internet crime, cybercrime, these types of crimes are new from our former forms of crime in that
they are truly international. If we have a criminal that intrudes into a bank in Manila, the police in the Philippines will go ahead and begin their investigation. They may find out that the origin of the attack was in Buenos Aires. They then talk
to police in Brazil who find out the attack came from Seoul only to go ahead and ultimately address the perpetrator in Canada.
This is something new.
Previously, if a murder, if a homicide took place in the streets of Paris, what did we know? Well, we knew the dead person was
in Paris. We knew also that the perpetrator of the crime had to be in Paris. It was all quite simple as we look back.
Now the question is where is the crime scene and who is in charge? And law enforcement is spending a lot of time trying to
work out these issues.
So there are several challenges. One of them is, as I just mentioned, the relevance of geographic distance. These investigations can be very expensive. They require a lot of resources. They need to be done in real time, otherwise the
evidence can go away. The anonymity of the Internet makes things difficult. Jurisdiction is hard, legal is hard, and the technology is always changing.
So just because you knew how to do a forensic analysis of a Windows 95 machine, that won't help you with vista, per se.
And so you have to stay on top of it.
The legal issues are somewhat of a challenge because many have no laws against cybercrime. So even if India has a very
strong cybercrime law, if they are attacked from a country who has no cybercrime law, due to international treaties, mutual
legal assistance, et cetera, dual criminality, it will be almost impossible extradite the perpetrator and bring them to justice. So it's important that we work together closely.
I am here today on behalf of an organization called IMPACT. I won't give you a commercial for them. Just to say there
is a booth out there in the cybercafe and I welcome you to stop by where I can answer more of these questions.
In conclusion, there are more than 200 countries connected to the Internet. Cybercrime is a global issue.
It may be great that 50 or 75 or even 100 countries have rules and regulations, policies and procedures concerning cybercrime.
But if 150 countries more don't, then we have a problem.
And so we need to work with our partners in the developing world to help ensure that we can have cybersecurity, cyber peace,
and cyber trust around the world. Otherwise, what we will end up developing are what we call cyber havens. We have already

seen this with money laundering. Money launderers tend to go to certain countries because it's easy for them to launder money there.
Unless we can truly make a strong international architecture in which we can have an Internet that is built upon peace, trust, security
and the avoidance of crime and harming other people, then we won't succeed. We all have to sink or swim together and cooperation and coordination
are key.
And I thank you all very much for your kind attention.

>>BERTRAND DE LA CHAPELLE: Thank you, Marc.
We wanted to have the two presentations with slides to launch the discussion.
It is a way to share with you and to make you understand the perspectives of people who are actively working on a daily basis
in those fields, from the law enforcement cooperation perspective and from the security and enhancement of the resilience and
capacity of response side.
Now we'll try to get into other dimensions without slides, but to explore additional perspectives. The things that we have
seen are that readiness is important, that there are a large number of actors, that implementation takes time to prepare, and that the methodology is evolving.
This notion that a lot of actors are involved, I would like to ask Patrik Fältström to explore further.
Patrik Fältström is from Cisco, and as a provider of equipment and a very well-known security specialist, he is in contact
with a great diversity of actors.
And during the preparation, one question emerged. Like we had with Michael, who are you going to call? What you would
call the "Ghostbusters" approach: Who are you going to call?
The other question is who is responsible and who is responsible for what?
And there's another point I would like you to maybe make a comment on, is collection of data is necessary, and there is a lot of
data that is available on the activities of people. And the collection of data is necessary for forensics and for inquiries. But it also brings new challenges in terms of dissemination and access to data.
If you could also address this point.
So the responsibilities and data.

>>PATRIK FÄLTSTRÖM: Yes, thank you very much, Bertrand.
So as you heard before in the two previous presentations there are a large number of organizations involved, and a pretty
complicated network of organizations. But it's even more complicated than that, because in the first presentation, we actually
saw something that looked like a diagram. You had a national CERT and everything is fine, and if you just fill out the names
of the organizations, the boxes, you just follow that scheme and you are done.
It is not that easy, unfortunately.
And there are a couple of reasons for that. And one of the reasons is, of course, that the world has changed quite a lot.
If we look at the service voice, you just lift the receiver of a telephone and you make the phone call, if you look 30 years
back, in each country more or less you had an incumbent. And that incumbent was responsible for the functionality of that
service. And they kept track of who was calling who, they sent out the bills. If things didn't work, you called them. If it was the case the police needed the information, they knew how to talk to.
But today, it is even more complicated. We introduced competition, we introduced now portability so it might be

hard to even
know who the phone number belongs to. It's even the case that you have more and more virtual telephone companies or voice over
IP providers that act over national boundaries. So the question is, then, which -- if that organization that is covering multiple
countries, like many ISPs do, if they want to talk to a CERT, should they pick one of the national CERTs or the one where the crime
is or their favored ones? It depends, I think is the correct answer here.
It is also the case that when we are acting against some incident, as we heard, it's pretty important that we do some prevention
methods. People install various different kinds of anti-virus software in the computers. You have firewalls. You put in
mashers to trace where traffic is passing, to detect what is happening. You install security systems on the doors.
So that's a prevention thing. But even though you have created this barrier that is going to protect you, of course something might happen.
And during an incident, then you would like to act. Like we saw the diagram with the arrows across the world. So you need to
be able to know, should I talk to the law enforcement? Who can help with these hard decisions?
But then after everything is resolved, unfortunately, it might be the case that some disaster happened as well, but regardless,
you would like to collect some statistics, collect data, draw conclusions of what's happening so you have a feedback loop afterwards,
after the action where you collect information what actually happened.
And that feedback and the statistics is, in turn, of course, supposed to help to increase the prevention methods that you are
implementing.
So in reality, you have a circle of action, feedback, reaction, and prevention, which goes around and around and around.
So the important thing is to think about the security, not only as Marc said to do it beforehand, but also to update your prevention mechanism according to what happened, according to recent incidents. Both in your organization but also in other
organizations. And how can you get to know what you should do? Well, you talk to the organizations that are the good ones,
you've got statistic and feedback, which might be different organizations than being the one that held during the attack,
which are different organizations than the one that helped with the prevention.
So we have multiple organizations depending on where in this cycle you are at the moment that you want to talk, to but you
also have different organizations depending upon what kind of problem it is.
Because I just gave an example with a voice application, but on the Internet, of course, we can run many different applications
and services on top of an Internet access.
So it ends up being pretty complicated to know who you are going to talk to, just simply like I've got a DDOS attack against me.
Who am I supposed to talk? Who knows where that flow is coming from?
That can be really difficult to know.
Even if you know the IP address for some weird reason where the attack is coming from, who knows where that IP address is?
That's a complicated question that I work quite a lot with the police in Sweden to try to figure out what is the best way of
sorting that, to resolve the issue of finding where an IP address is. Because the ISP may not know where geographically the end
of the IP address is.
It's the one owning the fiber of the copper pair that knows where the IP address is or even the cell phone provider that

can
do triangulation of the radio.
So even for one sort of simple thing like an IP address, and about the data that you asked me, Bertrand, it is pretty -- there
are multiple providers involved in collecting information, even within the same geographical area. And then on top of that we have
the multiple dimensions across the world that you just heard about.
So this is extremely complicated.
But it's not only that. It's also the case, of course, that if you are an enterprise or if it is the case that you have a network,
and all of us have at home, if we connect computers or networks to the Internet, what we connect ends up being a part of the
Internet. And this is also a change in the thinking of the world compared to in the old days when we connected a phone to the
phone network. In Sweden, at least, it was the case that we could even only buy phones from the incumbent. They approved the
phones. It was their phone jack. They had complete control over the whole system.
Today, when I connect something to the Internet, my things ends up being part of the Internet.
So personally, I am a little bit irritated on all the pictures in gross which is here is my computer, here is my network, and
over there is the Internet. The Internet includes my stuff.
And because my stuff ends up being a part of the Internet, I am also responsible for that piece of the Internet.
So we have a shared responsibility. And because of that, it is even more important that we talk with each other.
So who should you talk to? Well, the thing is you should talk to the one you trust, and you should talk to the ones that
actually help you.
Which means that this is to a certain degree competition and market economy regarding services.
There are multiple CERTs out in the world, and, yes, we at Cisco has one. Many of the manufacturers have CERTs, just like
countries, just like organizations that you saw before, and each one of those give different kind of service. Some of them
are better during the actual action during an incident, some are better regarding the statistics collection, and you talk to
the one that gives you help.
You give information to someone if it is the case that you trust them that they are only going to use the information, what
they are telling you what they are going to use it for, and specifically you are giving information to them if you get more
data and information back than what you give them. Basically, it helps you to talk with them.
If you have a country and you have three or four Internet service providers in the country, I claim that a CERT will not be
created in that country as long as the ISPs can talk to each other. It must be easier for each one of the ISPs to talk to the
CERT than to talk to all the other ISPs.
So to a certain degree the CERT is really a coordination center that makes it easier for organizations to, first of all,
exchange this information and create this feedback loop. But also, all of this trust normally starts by having individuals
trust each other. That needs to grow into having organizations trust each other. And when organizations trust each other and
when you start to pass data back and forth -- I am trying to grow into, to move into your question here, Bertrand -- then you need
to create a legal framework. You need to set up NDAs between the organizations, you need to have a formal structure. But that is
built according to a bottom-up process.
Trying to tell someone that you as an organization, you must give your information about all the security incidents and
everything

that has happened to this other organization, being told that is a little bit uncomfortable.
It's much better if you start with the bottom-up process, start to understand that you should give out the information, that it helps.
So all of these organizations work together in an ecosystem where you have multiple processes going on and multiple CERTs, and
certainly they are overlapping, but all of them are solving a problem. If they don't solve a problem, they will go away because
people will not share information with them.
So now when the information is shared, it could be both tracking, for example, phone calls and IP addresses, which is as part
of the prevention methods. It could also be during an incident or after an incident happened that you collect statistics.
Is it dangerous to exchange information? Well, I think what Bertrand and I talked about yesterday is that the answer is, for
that as well, it depends. It depends very much on who is asking, what query is allowed to the data, and when you ask, do
you get -- what information do you get out? Just because of the authentication authorization to the database, it might be
the case that different parties querying get, even though they issue the same query, get different data back.
So, for example, an IP address by itself might not be dangerous at all. But the IP address and a usage pattern or traffic
flow or the connection to a customer, that might be privacy information, and most certainly is under some legislations.
So the collection of data by itself doesn't have to be dangerous.
But it is the usage and how it's queried and what it can be used for which is the problem.
And that's why after a while of this informal network of individuals, you need NDAs and the formal structures. But once again,
built in a bottom-up process. There are multiple of these, and specifically I see different organizations, depending on at what
part of this feedback circle we are working.
Thank you.

>>BERTRAND DE LA CHAPELLE: Thank you very much, Patrik.
I think you used an expression which is it's extremely complicated. It can also be said that it should be naturally complex,
as it adapts to a network which is, itself, a complex system in terms of the theory of complex systems.
The reason why I mention this is because Patrik was alluding to the past situation. And maybe some unconscious desire to
return to a situation where things are simple, or simpler. And I think the main challenge for all of us -- and it is exemplified
by the comments -- is that we have to handle a huge network of actors. And the interactions between those actors at different
stages of the loop that was described.
I wanted also to make a bridge between what Patrik has said and what Michael said earlier regarding filling the boxes.
I think Patrik and -- sorry, Michael, you can make just one brief comment to explain how long it takes sometimes to establish a
CERT, to say it's not something that comes from the top only but it's built from the interaction.

>>MICHAEL LEWIS: I think Patrik's point is valid. It looks easy but it's not. There are only perhaps two dozen or two and a
half dozen of these national CSIRTs in the world and I don't think any of them have it just right.
The project I am on now in Qatar was designed by Carnegie-Mellon based on its 20 years of experience and the best practices of
the community. And even with a master plan that had a lot of good advice, we have been at it for three and a half

years and we
are not there yet.
So I do think this is not an overnight success and as was noted earlier, it needs to evolve of.
It also needs to include private sector partners. I think that was implied but not made specific enough, and I'm glad Patrik
has referenced there.

>>BERTRAND DE LA CHAPELLE: Thank you, and it's basically also taking different formats in different countries and the different
actors have different structures.
I would like now to give the floor to Jayantha Fernando who is the director and legal advisor of the ICT agency in Sri Lanka.
He helped establish the national Sri Lankan CERT and also helped develop the legislation on cybercrime in Sri Lanka. And we thought
it was interesting to have the experience that he could bring. And if I may ask Jayantha to deal with both those elements,
particularly how you establish the CERTs, including the cost dimension, which I found interesting when we prepared. And the second
element is what methodology did you use to develop the national cybersecurity framework and did you use any inter reference.

>>JAYANTHA FERNANDO: Thank you, Bertrand.
Before I deal with the specific issues, asked a question of me from Bertrand, let me spell out some of the challenges that we
all encounter from the governmental perspective.
The transition from paper-based environment to a paperless and a network environment has created great opportunities for governments,
businesses and users.
The opportunities we all know go with challenges. This is true in a network environment as well.
That brings us to this morning's discussion which has become a global challenge for governments, businesses, and for individual users.
We are here to discuss dimensions of cybersecurity and cybercrime. Many of the speakers in this panel have dealt with these
challenges and given us an overview of cybersecurity and cybercrime.
The purpose of my intervention here is to address some of the policy and enforcement challenges from a governmental perspective
and share some of the policy trends and approaches to legislation and the institutional models, such as the establishment of CERT,
which might help in the discussion in the afternoon.
So are we really losing the battle against cybercrime, is the question.
Well, the policy challenges we encounter on a day-to-day basis may give that impression to all of us.
On the one hand, law enforcement reform cannot keep pace with the developments in technology.
Therefore, the law enforcement processes are often behind technology. And this is a global phenomenon.
Interestingly, from a legal perspective, some have sought to define cybersecurity, and the definition in the Cybersecurity
Information Act is an interesting example. However, no consensus has been reached in respect of a definition on cybercrime.
And cybercrime broadly used with categories of human behavior where the confidentiality, integrity, and availability of a
computer or computer system is affected. And where the systems are used as a tool for the commission of other traditional
offenses, like cheating, criminal misappropriation, criminal theft, fraud, et cetera.

So many of our speakers have dealt with that issue earlier.
Battling cybercrime also poses enforcement and policy challenges. And that's the substance of what I have been asked to
intervene on.
Any criminal investigation interferes with the rights of others where the person is the subject of an investigation, how they
are related to the party. In a democratic society, such interference must be justifiable and proportionate to the needs of the
society sought to be protected.
However, the growth of network-based crime has raised difficult issues in respect of the appropriate balance between the needs
of those investigating and prosecuting such crime, and the rights of users and -- of such networks.
In addition, there are the rights of and interests of the network providers, the intermediaries that build and/or operate the
network and services through which data is communicated. These challenges require parties to the enforcement process -- namely,
investigators, prosecutors, and judges -- to work in a coordinated manner.
This necessary coordination is also challenging for governments because of the lack of expertise to often deal with cybercrime.
As such, governments have been compelled to rely on expertise from outside governments, such as from academia and business.
This is the experience in Sri Lanka as well.
The Computer Crime Act number 24 of 2007 in Sri Lanka, which was brought into operation on the 15th of July this year, responded
to these enforcement challenges by providing for an independent group of experts to assist the law enforcement agencies in the
investigation of cybercrime.
These designated experts are fully empowered and given protection under the legislation.
However, safeguards have also been built to protect the business as well as the computer systems they use which are subject
matter of investigations.
This is to provide the comfort measures required for businesses and individuals to report cybercrime. So for instance, as
Patrik pointed out, some of the confidentiality measures that he spoke of earlier have been built into our legislation, and those
obligations have been enforced on experts together with provisions to ensure that business continuity is not hampered during
investigations as much as possible.
Governments can no longer rely on traditional government expertise to address cyber threats and forensic issues.
As such, new institutional models may have to be created based on hybrid frameworks.
The Sri Lankan experience may be an interesting regional example in this regard.
In mid June 2006, the Sri Lanka CERT was created to address cybersecurity incidents, and this was established as a government-owned
company as a subsidy of I.T. Agency of Sri Lanka, with support from the World Bank, and runs on a private sector driven model with
highly skilled incident handlers with pay commensurate with those in the private sector.
The board of the CERT consists of a range of stakeholders such as enforcement authorities bankers, private sector and academia.
These efforts have resulted in the establishment of other technical CERTs, like the one established by the Sri Lanka's foremost
technical university, University of (saying name), as a project of the Sri Lanka domain name registry.
In conclusion, I have to say this, we have encountered persistent problems in relation to capacity building, and this is another
area where governments have to rely on international expertise and private sector support.

I would like to say that the battle against cybercrime will not be lost if there is increased international cooperation.
Cybercrime by nature is multi-jurisdictional, as pointed out by many other speakers, and not confined to one country.
As such, governments cannot enforce cybercrime in isolation. That's reality.
This has created increasing pressures on governments, including those from the least developed segments to harmonize legislation or
at least harmonize enforcement processes.
Harmonization has increasingly become a precondition for international cooperation.
In harmonization, governments have to rely on international best practices. And one successful harmonization approach that
Sri Lanka relied on is the approach adopted by the Council of Europe I mentioned on cybercrime. And that is one approach that we
looked at and we adopted.
And we look forward to acceding to that convention in the near future.
I take the opportunity to call upon greater collaboration between governments, international organizations, businesses, and
other stakeholders to address the growing threats associated with cybercrime.
And I thank you for this opportunity to intervene from a government perspective. Thank you.
[Applause]

>>BERTRAND DE LA CHAPELLE: Thank you, Jayantha, for the insistence on a certain number of points. We will have the opportunity
to come back to the use of reference frameworks and how a typical -- a particular convention was used for your country to establish
the different building blocks and the balance between the different elements. Because you were also alluding to the proportionality
of the means and the tools. And I think we've heard the word "trust" a lot. And the interesting thing is, there's a challenge
also to establish trust in the actors who are in charge of security and combating cybercrime.
And I would like to now turn to Dr. Gulshan Rai, who is the director general of the -- at the Ministry of Communications and
Information Technology in India, and also the -- responsible for the Indian CERT, to ask him a question about what specific types
of problems are encountered in a country -- did I say China? Sorry -- in India -- what specific types of problems are encountered
in India. And, in particular, we were alluding during the preparation to one tension between the time that is required in terms
of reactions and the processes that are needed to guarantee a certain number of rights in the persecution and search.

>>GULSHAN RAI: Thank you. Mr. Chairman, Mr. Markus, dignitaries and delegates and friends, it's, indeed, a pleasure to make
a contribution on this forum on the very important subject of global threats and challenges to cybersecurity.
The information technology infrastructure in India today is a vast fabric of computers from supercomputers to hand-held devices
and interconnecting networks, enabling high-speed communications, information access, advanced computation technologies,
transactions, and automated processes.
People in India see and use the components of the I.T. infrastructure, mainly desktop computers connected to the Internet, that
enables e-mail, instant messages, exchange, and downloading of sound and image, online shopping, information searches, interactive
games, and even telephony.
We also work with information technologies that drive day-to-day operations in industry and government and are

relied upon by
organizations large and small for a range of functions, including design, manufacturing, inventory control, (inaudible) information
storage and retrieval, education, training, and research and development. In fact, economists credit successful applications of
information technologies throughout our economy for the spectacular gains in productivity over the last five years in the country.
Economic potential is increasingly linked to the utilization of the information infrastructure.
Today, the computing systems control the management of power plants, air traffic control systems, food and energy distribution,
and the financial systems, to name only some. Banks, for example, rely on extensive distribution -- distributed communication
network, and information services, both for customer interactions and interbank operations. The reliance of these sensitive
physical installations and processes on the I.T. infrastructure makes that infrastructure extra critical and in the nation's interest to safeguard.
Now, this revolution in proliferation of information technology in every sector of society has also increased the potential of
those who could harm, giving them the capability to do so from afar, while armed with only a computer and the knowledge needed
to identify and exploit vulnerabilities. Today it is possible for a malicious agent to penetrate millions of computers around
the world in a matter of minutes, exploiting these machines to attack the nation's critical information infrastructure, (inaudible)
system or state valuable data. The threat clearly is growing. Most indicators and studies of the frequency impact, scope, and
cost of cybersecurity incidents among both organizations and individual point to increasing levels and varieties of attacks.
The number compromised systems are increasing. These compromised hosts are used as a threat form for launching further attacks,
particularly distributed denial of service attacks or injecting bots or the malicious codes over there.
The CERT in India has also reported about 800 new electronic vulnerabilities during the 2007 in the country, which is more than
a 24 increase in 2001. The total number of attacks, including viruses and worms, cyber frauds in operations, are rising by about
50% annually, with many types of attacks doubling in numbers.
The story about spam is also -- is similar. (inaudible) which we are observing about the spam in India is more or less in line
with what pattern we observe, somewhere around 80% of the spams in e-mail traffic. In a survey conducted by the CERT, as well
as Price Waterhouse, shows that 50% of the organizations providing one or other type of services experienced compromised systems
in 2006 or 2007, which is almost double than the figure of what we observed in 2000.
The numbers of phishing cases are on the increase among the Indian banks. 78 cases of phishing are being reported on an average
per day. Most of the phishing cases are hosted outside, are hosted in one country, registered in another country, and where we
find problem in disabling them.
The most disturbing fact is that there has been increase in the number of cases of cyber incidents pertaining to domain name
registry. The registrars, the address, and the I.P. address, as well as the address of the registrants are found to be fake.
Involving cybersecurity, it requires a strategy involving people, process, and technology. We are working with the public and
the private sector and other organizations to train our manpower. We are also sending our people abroad for getting

trained
in implementations of best security practices, particularly in the context of information, national information infrastructure.
India was the 12th country in the year 2000 to enact Information Technology Act 2000, a legal frame towards the issues in -- to
address the issues in cyberspace. The legal framework was based on the technology and practices being followed and available at
that point of time. The act provided the evidentiary value to the electronic document and for certain other -- and included
certain other computer offenses.
Over a period of time, not many offenses and contraventions have emerged. Due to (inaudible) and innovation in technology,
these informations and offenses need to be addressed for safer working in cyberspace.
We are in the process of amending of a legal framework to address issues posed by these new technologies and the new crimes which
are being observed in cyberspace. We are amending the -- our Information Technology Act 2000. And we have introduced the bill in
the Indian information to the amendment 2006, which is now pending before the parliament.
The amendments deal with data security, data privacy, identity theft, cyber terrorism. For the first time, we have tried to
define the cyber terrorism, child pornography, spam, phishing, and online frauds.
The body will have to implement best security practices to secure data collected by them while providing services. Any leakage
of data on their account will result in compensation commensurate to the damages suffered by the victim.
The service providers will also have to preserve traffic data for a period which can be specified in consultation with the
industry. The amended legal framework will be in line with all the provisions of the European convention, cyber convention.
The national CERT is in position, and the national CERT is a part of all the member communities, namely, the first forum response
team, the Asia-Pacific CERT, and we have relationships with many of the CERTs. We are, in cooperation with the first of the
Asia-Pacific CERT, getting out the mock trials our studies provide us in the country in a regular manner.
We have also set up a garment industry initiative, a company has been set up, namely, data Security Council of India, to work
with the industry to create awareness and, in short, compliance to the best practices among the information technology-enabled
services and I.T. organizations in the country. The challenge is huge for us to train our police and judicial officer to collect
analysis, to collect, analyze potential evidence. And we are very actively working in this direction, with the help of -- in
a public-private partnership.
Today, over a billion users worldwide connects this Internet. Over the next year, over the next five to six years, a more billion
new users will join existing users on the Net. With the growth of Internet, the growth of the users, Internet will dramatically
expand reach and scope.
Addressing the requirement to secure cyberspace within the country, as well as globally, for the longer term requires collaboration
and cooperation among the countries, both for taking research, to explore science and develop the technologies necessary to design
security into computing and networking systems and software from the ground up.
There are several areas relating to cybersecurity in which there may be conflicting interest and needs, and such areas will need

to be addressed as a part of a comprehensive approach to the cybersecurity. It's more a global phenomenon. For example, as a part
of (inaudible) attacks or to track down cybercriminals, it may be necessary to know the origin of data packets on the Internet.
But such knowledge may be perceived by some to conflict with an individual right to privacy or anonymity.
To cite another example, while some nations are perceived as necessary (inaudible) of data, may be perceived by others as
unwanted censorship. Such issues involves ethics, law, and social -- society, questions, as much as they do technology. And
these nontechnology issues make the cybersecurity problem even more challenging.
There's a need to exchange information without any hindrances among the nations and among the organizations to track down the
criminals. Global alliances and exchange of information have to be established while attaining safety, security, and stability
of the Internet.
The CERTs are cooperating very well around the globe. They are cooperating each to disable some of the incidents or spams.
But when it comes to getting the hard data, they are -- these CERTs need to be given powers to handle so as to (inaudible).

>>BERTRAND DE LA CHAPELLE: Mister --

>>GULSHAN RAI: Such steps will be the true -- the society, the citizens, judges, academia and industry need to work together
toward a mechanism for effective collaboration and cooperation so as to work towards providing a safe and secure cyberspace to
our citizens. We commit ourselves and will collaborate with any agency in the world to work toward this.
I thank you very much for giving us the opportunity to interact and give our presentation. Thank you.
[Applause]

>>BERTRAND DE LA CHAPELLE: Thank you, Mr. Rai.
And you pointed to one element, which is the tension with other types of concerns, like privacy protection, protections of
various freedoms, and the constraint between the need to have the tools to react and the necessary protection of those rights.
I think Jayantha was alluding to it as well.
I wanted to make a clear point here.
The prospective that this panel -- perspective that and the construction of this panel has taken is to basically present the
perspective and the viewpoint from people who are working from the cybersecurity and cybercrime daily job and activities. You
know that immediately afterwards, there is another panel that is dealing with fostering security, privacy, and openness, which
is dealing a little bit more about not the balance, but the interaction and the interplay between those different dimensions.
But we thought it was useful to present you with a perspective that is not frequently visible in many of the fora that deal with that.
I would like now to give the floor to Alexander Ntoko, who is the head corporate strategy at the ITU, and also the focal
point on cybersecurity, and particularly the initiative that the ITU has launched, which is the Global Cybersecurity Agenda.

Alexander, can I ask you, in your presentation and comments, to give some elements on two points. The first thing is, what is
the consequence that the trans-border nature of the cybercrime and cybersecurity has on the necessity to organize the trans-border
cooperation and the harmonization, and particularly of the frameworks and the actors. And the second element is, how, given what
has been said before, is it possible to engage very broad diversity of actors? And in the case of ITU, actors who are not in the
current membership of the ITU, actors who are companies that are not the traditional interlocutors or actors from other organizations on a daily basis.
Thank you.

>>ALEXANDER NTOKO: Okay. Thank you, and good morning to everybody.
You have heard already about the threats and how complex they are, the need for collaboration, for cooperation.
You have also heard from my other colleagues how things are getting even more sophisticated.
One thing that I'm going to say is that we are dealing with a problem which is global. I'm not going to get into the specifics
of, you know, what types of attacks or threats exist, because this has already been covered. But the one thing which I think is
really important is that, one, we agree that we are all connected. Two, we need to somehow come to some kind of a common
understanding. You know, we live in a society. We need to have some basic rules about how we do things in this society.
What we have done in the ITU as a result of the World Summit on the Information Society, which has entrusted ITU to facilitate
and coordinate the global response, is to launch an initiative which we call the Global Cybersecurity Agenda. The agenda was
launched by the Secretary-General 17th of May last year. And what is unique about this is, it just addresses what Bertrand was
talking about. We said if we wanted to address this issue which involves so much stakeholders, many of whom are not participating
in ITU or not in ITU's own forum, we need to come up with a very broad group of experts representing all the stakeholder groups.
So we did set up an expert group, a high-level expert group of 101 also experts from all over the world, representing industry,
governments, international organizations, NGOs, academic and research institutions, because we wanted to see how these entities,
what they thought would be the way forward, what was their understanding of some of the threats and how can we, you know, try to
capture those common elements. Because the tricky thing with cybersecurity, cyber threats, cybercrime, is that it involves so many
actors. It involves almost everybody. Everybody who is connected to the Internet is an actor. You might not want to be one.
But if your computer is part of a botnet, you are part of whatever threat that computer is disseminating. So it is something
which needs, one, two types of approaches. We need to look at a top-down and a bottom-up approach. When I say "top-down," I mean
while we are working on connecting the individual, I don't know, businesses, governments, groups, or whatever, we have to also have
this view that this business, these companies, these organizations, are part of a global network, and how do they interoperate
with this -- the other elements of this global network.
What we came up with as a result of one year of, you know, work, you know, which the experts, you know, had

meetings and discussed
and tried to see how we can agree on something, the first thing was that we had to work on five main pillars. And I will explain a
little bit why this is very important.
We need to look at five areas of activities. We cannot address issues of cybersecurity by grouping people into categories and
saying, "This is something just for businesses. This is something just for governments. This is something just for civil society."
Because governments have roles to play in -- in some cases, in some of the technical activities, depending on what the government
is doing. Governments have a role to play also in areas like capacity-building. Civil society have roles to play in setting up
projects, in building capacity, in raising awareness.
So the way we are going to move forward is to create a framework or some what we call pillars, an area where people of common
interest can meet and work on solutions, regardless of the types of entities.
So we came up with five pillars which resulted from the work of the high-level expert group. One is legal measures. Many
colleagues have talked about legal issues, forensics, laws, the colleague here from Sri Lanka talked about what they have done
nationally in putting in place a law of cybersecurity and cybercrime.
The second pillar is technical and procedural measures.
Because -- which is why I think I'm quite happy with the mix in this panel, because we have somebody from Cisco who has talked
about those technical issues and how some of them can be addressed at the level of networks. So we need to have an area, a work
area, which we call technical and procedural measures.
We need to have organizational structures. Another presenter talked already about the CERTs, I think two or three people talked
already about the CERTs and how they are important.
We need to focus also on capacity-building, which is cross-cutting, you know. Everybody in every area, whether it be technical
or legal, you need to build capacity.
And the last or the fifth pillar is that of international cooperation. Because we are connected. And the one thing which we
need to really take account of is the fact that the criminals are very well connected and very well organized. And we cannot
continue to keep on addressing cybersecurity in silos, you know, because we are all connected. And that is the one thing which I
think one of the presenters talked a lot about the fact that, you know, you don't have a crime scene with a body and a weapon and
everything in the same location and jurisdiction. We have a very complex situation to manage. And the criminals and those who
perpetrate some of the cyber threats are one step ahead of us, because they are quite organized. And I think being organized,
having a bottom-up and top-down approach, bottom-up, because we have to build these sets at the national level or regional level,
we have to build capacity in countries, in schools, we need to set up networks which are secure. But then we also have to know
that these networks need to be connected to a global infrastructure where, you know, the strength of this overall infrastructure
is the weakest link.
So we need to look at how we can better organize ourselves and how we can be proactive, which is the second key point that I am

going to make.
We have in the past, you know, been involved mostly, like, firefighters, you know, you wait for the building to burn down, and
then you try to turn off the fire. And I think we have to change that approach. We need to be proactive. We need to put in place
systems that will -- like we -- you know, I think it was in December 2004 -- I might be wrong -- where we had the tsunami in Asia that
killed so many people. And some are saying that if some of these people just knew that, you know, these waves were coming, maybe
we could have saved a certain number of lives.
We have to do the same thing in cybersecurity. We have to put in place early warning systems, systems that will try to inform
people of where the threats are.
But what is tricky here is that it is not like a wave coming from the ocean and we know where it is heading and it has a clearly
defined destination.
A computer located in Sri Lanka is as close to an attacker, like any other computer. So it is not the same thing as us seeing
the wave going through, you know, regions, well-defined geographical areas and coming. But we still have the capability to be able
to raise awareness on certain threats before they get to the victims.
We have, as a result of one year of working within this expert group, we got to a point where we said we need to stop talking, we
need to now start acting. Because also one thing which is important is, there are real issues. People are losing money. There are
crimes being committed against children. We have people who have, you know, created business models around committing crimes on
the Internet. Marc talked about some crimes which are really new as a result of information and communication technologies which did
not exist.
So we need to really try to see how we make sure that we can get this information out about the threats, because some of you might
remember, I think it was the ILOVEYOU virus or something which came out a number of years back. This was an e-mail virus. And one
of the things that we noticed was that for people to be aware that there is this kind of a threat, in many cases, it is already --
you must already have opened the e-mail. Everybody is looking for love, and you see "I love you," you know, you click on it. But I
think we need early warning systems. We need systems which will be able to, you know, inform people about threats. And just
developing a little bit on that, one of the things that we did, we signed an agreement with impact. Marc talked a little bit about
impact. We signed this agreement where we are working with quite a number of global security companies who are working together
for the first time, aggregating some of the feeds and trying to put together information which would be relevant to keep layers
in cybersecurity so that they are aware of the threats. Because that will be already something -- I think it will be a major victory
on our part if we can get away a little bit from this firefighting and trying to be more proactive, trying to be more preventive,
and trying to detect threats before they actually get to us.
Those of you who have the time, you can get a demonstration at the ITU Impact booth at the village, the IGF Village, that's what
it's called.

The last thing which I would talk about has to do with -- I think Bertrand talked about the need for, you know, harmonization,
framework for harmonization. And, you know, the cross-border nature of cybersecurity and cyber threats.
We cannot all agree at a global level, even amongst businesses, if we take just the business community and say, "Let us agree on
what we should or should not do." It is not going to be that easy. Because some businesses might say, "Well, we think that a
certain degree of unsolicited communication is necessary for us to expose our products and services." Some might say, "Well, we
think that this is spam."
But I think we have to identify those common areas where it is easy for us to come to an agreement. And one of the things that
we have done in the ITU is, we have -- we thought about the issues, the crimes, the threats, and we said, "Well, if we focus on
protecting children, we think it would be difficult for anybody to, you know, resist doing that. And we believe that if we start
with one area where there is a common understanding that there is a need for something to be done, we can use that and build on
other areas.
So the child protection is an initiative that was launched to try to see, you know, working with a number of stakeholders.
And, of course, we are really, as everybody knows, we have this strong description of an intergovernmental organization, which
we are. But we don't only work -- we don't work only with governments. When we deal with things like cybersecurity, I have been
myself to nearly 100 countries, and over my nearly 19 years in the ITU, I have been with a number of entities, NGOs working on
trying to secure, you know, a telecenter which maybe is involved in or has some security problems or people are using them to try
to launch attacks in developing countries. We work with industry, of course, which are also our members.
But the key message, I think, which I -- I'm trying to convey here is that when we are dealing with cybersecurity, cybercrime,
describe threats, we need to work on the basis of what we call those five pillars that I mentioned, because you create a common
environment where all interested stakeholders, irrespective of which entity type they are, can come together and work.
So to conclude, basically, we have three things that I think we should do, because we need to start -- or we have already
started -- some of our colleagues have mentioned some of the solutions on how they are putting things into place. But I think
we have to intensify our efforts, because the criminals, those who are committing these offenses, are using technologies for
purposes that they were not intended for seem to be one step ahead of us. And we need to catch up. We need to look at how we look
at this problem as a global problem while acting local with all the relevant stakeholders.
That's what I mean by top-down and bottom-up at the same time.
We need to be proactive. We cannot sit and wait for the threats to hit us. We are all aware of how global early warning systems
are being used in a number of domains.
The third thing is, we have to be organized. We have to be much better organized. And this organization has to do with cooperation.
It is a win-win situation for everybody if we all work together.
So I think for now, I'll stop my remarks at that, and thank you all for listening.
[Applause]

>>BERTRAND DE LA CHAPELLE: Thank you, Alexander.
We are reaching the end of this panel.
Once again, the architecture of the day is not to have the discussion on the panel right now, but to use the three hours of
discussion this afternoon to address the broad range of issues, including the ones that will be discussed in the next panel now,
which will provide a different angle on the same kind of problem.
I just wanted, before giving back the floor to the Secretariat and our, now, chair, just wanted to highlight one word here.
And maybe, sorry, before we close, if there are any questions, we can take four or five comments to feed into the afternoon.
If there are people who want comments, you can go to the microphone that is here, the microphone in the middle. And please
make either just a comment, a remark, or a theme to be discussed further in the afternoon. We have three hours in the afternoon.
But go ahead.
(no audio).

>>BERTRAND DE LA CHAPELLE: The mic is not working. Is the mic working?
>> Can we please have someone helping the person with the microphone? Do we have any sound engineers in the room?

>>BERTRAND DE LA CHAPELLE: We have the pleasure of a distinguished UK parliamentarian with us.

>>ALUN MICHAEL: Is that working -- yes.
It's all or nothing.
Alun Michael, a member of the U.K. Parliament.
I attended WSIS as a Minister responsible for I.T, but before that I had some time as a policeman. And it's a point I want to make
about the context of our discussion.
Can I congratulate you on the expert panel that we have had and the very complementary nature of all the contributions that
have been made.
My point is about how we deal with crime.
Law enforcement and, indeed, law doesn't deal with all activities that are criminal.
That's true in the real world. Most serious crime, some less serious crime is dealt with by law enforcement. But most success
in the big challenge, which is to cut, reduce, prevent crime comes from a partnership approach to crime reduction.
In the UK we have set up local crime reduction partnerships that's dealt effectively with violent crime reduction down to litter
and parking fines.
My point is that it's true also of the Internet-related crime.
We promised in IGF 2007 in Rio that we would set up a U.K. IGF and that we would look at developing a crime reduction -- Internet
crime reduction partnership.
We have made a lot of progress, and I know other countries are taking that approach.
I have no disagreement with anything that I have heard from the panel, but I think one of the big questions for us is how the IGF,
in future years, can increasingly be the point where we bring together the experience of trying to cut crime, Internet-related crime,

at a national level and, indeed, at a subnational level because I believe in the long-term future, the IGF has a big place in that
activity. The reduction, the protection against crime, implementing the work that's been described by the expert panel.
And I hope this afternoon we can explore some of those issues.
Thank you very much.

>>BERTRAND DE LA CHAPELLE: Thank you very much.
We are now at the end of the panel, so if there are just comments and suggestions for this afternoon.
>> Yes, thank you. My name is Jean-Jacques.
Yes, the panel this morning is excellent but I do have a number of concerns that are still lingering.
Everyone has talked about international cooperation, but we all know very well that in the cybercrime area, the weakest links
are the developing countries, and they make the entire chain very fragile.
So you want to have alert centers.
Let's ask the developing countries, then, at the same time as they are becoming equipped to join the modern society, you want
to ask them to have super armies that are more expensive than the networks that they are setting up?
So you are beginning to understand the difficulties for developing countries to have to face down the challenge of resources
to be able to develop, but, on the other hand, to build up these super armies to combat cybercrime.
I would like to discuss this this afternoon.

>>BERTRAND DE LA CHAPELLE: Yes, exactly. That's what it boils down to. The cost of security.
Any other suggestions?
Two comments.
Please formulate your point as a topic or a theme for the discussion this afternoon.
We will have three hours for this this afternoon.

>> I am from McAfee, developers of security software for computing and for network security.
My question is, we have all these products and multiple companies that are building security software and products around
the world for various situations.
From a private product developer perspective, what kind of participation can we have in the IGF? And maybe like a consortium
of software developers to standardize on logging forensics and basically evidence building.
It's just a question, because I'm not sure what we can do as much as we are very keen to participate.

>>BERTRAND DE LA CHAPELLE: Thank you.
Another comment.
We take two final comments, and then we'll close the panel.

>> I'm Henry De Souza from India.
As we try to reach out or provide access to a billion people or the last billion, many of them will be children and young
people, and a large section of them will be from Asia.
At a time when there is so much hatred and hate campaigns and violence spread through the net, should we not network with the
educational departments and other stakeholders so that we are able to sensitize the young minds, impressional minds through the

hazards that are coming to us through the net?
Thank you.

>>BERTRAND DE LA CHAPELLE: Thank you.
And the last suggestion for this afternoon.
Thank you.

>> I am Manuel B. from ANACOM Portugal. I congratulate you for the panel you have presented today. I would like to highlight
also some work done by other organizations, like OECD, on this material. And I think it would be important to have them present
their point of view this afternoon.
And I would like to issue a question on how you sustain and build knowledge on security.
Not from an individual perspective, but by teamwork.
Thank you.

>>BERTRAND DE LA CHAPELLE: Thank you.
I think the point about interaction with other organizations is key.
I will end up my very pleasant role as the moderator of this panel now with one word that emerged through the discussion and I am
very happy it did, which is the word trust. It turns out it means three things concurrently.
One is the trust in relations between the people who handle cybersecurity issues. The second is trust as a goal, that we want to
have a network that people do trust. And the third element that was basically alluded to and that we can discuss in the future is
how we can, as citizens as well, trust the procedures that are put in place to handle cybersecurity and cybercrime threats.
With this, I hand it over to either Markus or our chair, depending on whether there are announcements to do.
Mr. Chandrashekhar.

>>R. CHANDRASHEKHAR: Thank you, Bertrand.
In conclusion, I would like to, first of all, compliment all the panelists on having brought out so very clearly and explicitly
the many kinds of threats that are facing not only the Internet community but, in fact, the Internet itself.
And also, I think a repeated point which is brought out by everybody is the chilling fact that those who are out to cause these
problems are quite often a step or two ahead of those who are engaged in solving the problems.
And also the fact that all of us are a part of the Internet. We are not an extension of it, we are not an attachment to it.
We are part of the Internet. And we could actually wittingly and unwittingly be a part of the problem as well.
But we most definitely need to be a part of the solution to these problems.
I think what came out very clearly in the various presentations, which I don't need to repeat, are some of the possible actions
that can be and, in fact, are being taken in some countries, and also some of the limitations of these actions.
I think that was also very clear from the presentations.
Equally, who are the players and who are the entities who might take some of these actions and who need to do certain things?
But notwithstanding all of that, the fact remains that there are still a number of open questions on how exactly this collaboration
between all the entities that are involved in being a part of the solution and how exactly the trust that was repeated in recurring

theme could actually be built up in a workable and pragmatic manner to solve the problem of cybersecurity that is still out there.
Of course, as was mentioned, there are later sessions and workshops which are precisely meant to enable everybody to delve deeper
into some of these issues as well as some of the remedies which were suggested. And more particularly, to address some of the open
questions that have been flagged and that remain.
So with that, I think I would perhaps like to conclude this session and thank the panelists and also the very able moderation
by Mr. Bertrand.
And Markus, if you would like to make any announcements before we conclude.
Thank you very much.

>>MARKUS KUMMER: Thank you, Mr. Chairman. My thanks go also to the all the panelists.
Just to say we are again now going to make a flying handover to the next panel. So please remain in the room. And while I ask
our panelists here to rejoin their seats in the hall, I'm at the same time asking the next panel to come up here on the podium,
and we will rearrange the podium.
Thank you.
[Applause]