“building confidence and security in the use of ICT”. To stress the importance of a multi-stakeholder approach, ITU named its work in this domain the Partnerships for Global Cybersecurity initiative. The next meeting on WSS Action Line C5 takes place on 14–15 May 2007. It will assess progress achieved since the May 2006 meeting and develop future work programmes in areas relevant to addressing current and future threats.

The Plenipotentiary Conference in Antalya in November 2006 instructed ITU to focus on initiatives to assist developing economies in adopting the technology and processes needed to maintain cybersecurity. ITU’s Telecommunication Development Sector (ITU–D) conducts programmes and study group activities related to this mandate. The objectives of these initiatives include extending ICT applications and services and contributing to building security and trust in the use of ICT; increasing basic awareness and building human and institutional capacities; developing sound national policies and enforceable legislation; monitoring progress at national levels; expanding watch, warning and incident response capabilities, and coordinating peer-to-peer sharing of experience between developing and developed countries.

An important tool developed in ITU’s Telecommunication Standardization Sector (ITU–T) is its recently released ICT Security Standards Roadmap. It covers the work of not only ITU-T, but also of the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the Internet Engineering Task Force (IETF), and various consortia. The road map includes general guidance documents and management and security standards. It lists work in progress, as well as proposals for new tasks.

For more information on the ITU Cybersecurity Watch, please contact cybersecurity@itu.int

Developing an international road map for cybersecurity

Our societies are increasingly dependent on information and communication technologies (ICT) that are linked through modern communication networks. These networks are responsible for a growing share of national wealth, and they provide potential for greater prosperity. However, threats have emerged that can seriously damage vital networks. More and more, electronic networks are being used for criminal purposes, or for objectives that can harm the integrity of critical infrastructure and create barriers for extending the benefits of ICT. To address these threats and protect infrastructure, each country needs a comprehensive action plan that addresses technical, legal and policy issues, combined with regional and international cooperation.

What form should these national strategies take, and how can we develop an international road map to promote global cybersecurity? Countries hold various views on the exact nature and scope of cybersecurity, making any debate on this topic complicated. For example, various countries see cybersecurity primarily as:

- a technical, network or information technology issue,
- a developmental issue because ICT services need secure and reliable networks, or
- an economic issue relating to maintaining business continuity or economic advantage,
- a law and enforcement issue to deal with cybercrime, or
- a national security issue relating to critical information infrastructure protection (CIIP).

Any international road map for cybersecurity must address all these different national perspectives. And all stakeholder groups have a role to play in promoting a global culture of cybersecurity.

The role of government

National governments have the responsibility of ensuring that their citizens are protected, particularly as public policy on information and network security has a major impact on a country’s global competitiveness. The State has the central task of coordinating and implementing a national cybersecurity strategy. ITU Member States are at widely differing levels in the development and implementation of their national policies and strategies. Some have developed comprehensive plans, while others are just beginning to consider the issues. A useful set of national case studies can be found in the “International CIIP Handbook” published by the Centre for Security Studies, a research institute in Zurich, Switzerland.

ITU Secretary-General
Dr Hamadoun I. Touré
As threats to cybersecurity are constantly evolving, any national policy must be flexible and adaptive. Typically, implementing a national strategy requires coordinating the work of multiple authorities and government departments, who have various perspectives on the problem. For some countries, an important task is to evaluate national vulnerabilities and match this to the roles of different government institutions and their relevant responsibilities. In a number of least developed countries, building the required human and institutional capacities and putting in place the necessary infrastructure, legislation and policies are priorities.

Another task for governments is to create new (or adapt existing) legislation to criminalize the misuse of ICT, to curb abuses and to protect consumer rights. Governments, with other stakeholders, are also responsible for raising awareness through public education about security risks, targeted at individuals and businesses, especially small firms.

Today’s global ICT infrastructure means that attacks can be launched from anywhere in the world and affect any country across the globe. Your computer might even become part of these attacks without your knowledge. Today’s global ICT infrastructure means that attacks can be launched from anywhere in the world and affect any country across the globe. Your computer might even become part of these attacks without your knowledge.

To protect national infrastructure effectively, national strategies must be matched with an international approach. It is also essential to create frameworks for cooperation across national jurisdictions, with the sharing of skills, knowledge, and experience. The Council of Europe’s Convention on Cybercrime is one such framework. It requires signatories “to cooperate to the widest extent possible” and provide “mutual assistance” within a constantly available system. It also provides the possibility for extradition for serious offences in the area of cybersecurity. Legislation requires effective enforcement through direct bilateral cooperation between countries, as well as by such agencies as the International Criminal Police Organization (Interpol), which carries out a number of activities to help in the fight against cybercrime.

The role of the private sector
As hackers become more sophisticated, the time is shrinking between their discovering a vulnerability and developing a malicious code to exploit the weakness. Early warning and rapid response are key to protecting business assets, and in many countries, the private sector is typically the first to assess technological changes and threats. Also, through taking part in relevant forums or standards-development organizations, industry plays a critical role in agreeing technical standards to protect security.

What happened to the WorldPay system demonstrates the dramatic effects that insecure ICT systems can have on business and consumers. And because ICT infrastructure is, for the most part, owned and operated by the private sector, its involvement in promoting a national and global culture of cybersecurity is crucial. Since effective cybersecurity needs an in-depth understanding of the various aspects of ICT networks, the private sector’s expertise and involvement are paramount in the development and implementation of national cybersecurity strategies.

The role of individuals
In addition, it is important to educate individual users of ICT about the importance of cybersecurity, particularly given the open nature of the Internet and the need to implement security measures at the edges of the network on personal computers in the home. Unfortunately, users are often unaware of the various threats and how to keep their machines safe. At the same time, ICT systems are increasingly complex and people may have to maintain systems that they do not fully understand.

For example, surveys have shown that a large percentage of personal computers are infected with viruses that have been unwittingly installed by users. As one result, hundreds of thousands of these computers have become zombies controlled by criminal gangs to create robot networks, or “botnets”. These are used to send spam or launch denial of service attacks for blackmail purposes, as in the case of WorldPay.

Due to the interconnected nature of ICT, genuine security can only be promoted when every user is aware of the threats and dangers. Governments and businesses both must help people obtain information on how to protect themselves — and thus also the community at large.

ITU’s work on cybersecurity
Since cyberspace does not respect national borders, and because no country alone can solve the world’s cybersecurity problems, we must find new methods for regional and international cooperation. This would encourage such key activities as the development of international standards, the coordination of legal systems, the halting of cyber-attacks in progress, and providing assistance to developing countries. As a result, a unique forum of 181 Member States, private-sector members and other stakeholders, ITU has a clear role in promoting safety in cyberspace.

At the second phase of the World Summit on the Information Society (WSIS) in Tunis in 2005, ITU was named the facilitator and moderator for WSIS Action Line C5 on
As threats to cybersecurity are constantly evolving, any national policy must be flexible and adaptive. Typically, implementing a national strategy requires coordinating the work of multiple authorities and government departments, who have various perspectives on the problem. For some countries, an important task is to evaluate national vulnerabilities and match this to the roles of different government institutions and their relevant responsibilities. In a number of least developed countries, building the required human and institutional capacities and putting in place the necessary infrastructure, legislation and policies are priorities.

Another task for governments is to create new (or adapt existing) legislation to criminalize the misuse of ICT, to curb abuses and to protect consumer rights. Governments, with other stakeholders, are also responsible for raising awareness through public education about security roles, targeted at individuals and businesses, especially small firms.

Today’s global ICT infrastructure means that attacks can be launched from anywhere in the world and affect any country across the globe. Your computer might even become part of these attacks without your knowledge.

Today’s global ICT infrastructure means that attacks can be launched from anywhere in the world and affect any country across the globe. Your computer might even become part of these attacks without your knowledge.

The role of the private sector

As hackers become more sophisticated, the time is shrinking between their discovering a vulnerability and developing a malicious code to exploit the weakness. Early warning and rapid response are key to protecting business assets, and in many countries, the private sector is typically the first to assess technological changes and threats. Also, through taking part in relevant forums or standards-development organizations, industry plays a critical role in agreeing technical standards to protect security.

What happened to the WorldPay system demonstrates the dramatic effects that securing ICT systems can have on business and consumers. And because ICT infrastructure is, for the most part, owned and operated by the private sector, its involvement in promoting a national and global culture of cybersecurity is crucial. Since effective cybersecurity needs an in-depth understanding of the various aspects of ICT networks, the private sector’s expertise and involvement are paramount in the development and implementation of national cybersecurity strategies.

The role of individuals

In addition, it is important to educate individuals of ICT about the importance of cybersecurity, particularly given the open nature of the Internet and the need to implement security measures at the edges of the network on personal computers in the home. Unfortunately, users are often unaware of the various threats and how to keep their machines safe. At the same time, ICT systems are increasingly complex and people may have to maintain systems that they do not fully understand.

For example, surveys have shown that a large percentage of personal computers are infected with viruses that have been unwittingly installed by users. As one result, hundreds of thousands of these computers have become zombies controlled by criminal gangs to create botnet networks, or “botnets”. These are used to send spam or launch denial of service attacks for blackmail purposes, as in the case of WorldPay.

Due to the interconnected nature of ICT, genuine security can only be promoted when every user is aware of the threats and dangers. Governments and businesses both must help people obtain information on how to protect themselves — and thus also the community at large.

ITU’s work on cybersecurity

Since cyberspace does not respect national borders, and because no country alone can solve the world’s cybersecurity problems, we must find new methods for regional and international cooperation. This would encourage such key activities as the development of international standards, the coordination of legal systems, the halting of cyber-attacks in progress, and providing assistance to developing countries. As a result, the development of international standards, the coordination of legal systems, the halting of cyber-attacks in progress, and providing assistance to developing countries.

The future of cybersecurity

At the second phase of the World Summit on the Information Society (WSIS) in Tunis in 2005, ITU was named the facilitator and moderator for WSIS Action Line C5 on...
“building confidence and security in the use of ICT”. To stress the importance of a multi-stakeholder approach, ITU named its work in this domain the Partnerships for Global Cybersecurity initiative. The next meeting on WSS Action Line C5 takes place on 14–15 May 2007. It will assess progress achieved since the May 2006 meeting and develop future work programmes in areas relevant to addressing current and future threats.

The Plenipotentiary Conference in Antalya in November 2006 instructed ITU to focus on initiatives to assist developing economies in adopting the technology and processes needed to maintain cybersecurity. ITU’s Telecommunication Development Sector (ITU–D) conducts programmes and study group activities related to this mandate. The objectives of these initiatives include extending ICT applications and services and contributing to building security and trust in the use of ICT; increasing basic awareness and building human and institutional capacities; developing sound national policies and enforceable legislation; monitoring progress at national levels; expanding watch, warning and incident response capabilities, and coordinating peer-to-peer sharing of experience between developing and developed countries.

An important tool developed in ITU’s Telecommunication Standardization Sector (ITU–T) is its recently released ICT Security Standards Roadmap. It covers the work of not only ITU–T, but also of the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the Internet Engineering Task Force (IETF), and various consortia.

The road map includes general guidance documents and management and security standards. It lists work in progress, as well as tasks for new initiatives.

For more information on the ITU Cybersecurity Watch, please contact cybersecurity@itu.int

Our societies are increasingly dependent on information and communication technologies (ICT) that are linked through modern communication networks. These networks are responsible for a growing share of national wealth, and they provide potential for greater prosperity. However, threats have emerged that can seriously damage vital networks. More and more, electronic networks are being used for criminal purposes, or for objectives that can harm the integrity of critical infrastructure and create barriers for extending the benefits of ICT. To address these threats and protect infrastructure, each country needs a comprehensive and integrated approach to cybersecurity. This requires developing sound national policies and strategies, and coordinating and implementing a national cybersecurity action plan that addresses technical, legal and policy issues, combined with regional and international cooperation.

What form should these national strategies take, and how can we develop an international road map to promote global cybersecurity? Countries hold various views on the exact nature and scope of cybersecurity; making any debate on this topic complicated. For example, various countries see cybersecurity primarily as:

- a technical, network or information technology issue;
- a developmental issue because ICT services need secure and reliable networks, or
- an economic issue relating to maintaining business continuity or economic advantage;
- a law and enforcement issue to deal with cybercrime, or
- a national security issue relating to critical infrastructure protection (CIIP).

Any international road map for cybersecurity must address all these different national perspectives. And all stakeholder groups have a role to play in promoting a global culture of cybersecurity.

The role of government

National governments have the responsibility of ensuring that their citizens are protected, particularly as public policy on information and network security has a major impact on a country’s global competitiveness. The State has the central task of coordinating and implementing a national cybersecurity strategy.

ITU Member States are at widely differing levels in the development and implementation of their national policies and strategies. Some have developed comprehensive plans, while others are just beginning to consider the issues. A useful set of national case studies can be found in the “International CIIP Handbook” published by the Centre for Security Studies, a research institute in Zurich, Switzerland.