ICTs FOR SAFETY, SECURITY AND DISASTER RECOVERY

A PRESENTATION
BY
PAVAN DUGGAL
ADVOCATE, SUPREME COURT OF INDIA
PRESIDENT, CYBERLAWS.NET
HEAD, PAVAN DUGGAL ASSOCIATES
CONFERENCE DIRECTOR,
INTERNATIONAL CONFERENCE ON CYBERLAW, CYBERCRIME & CYBERSECURITY

ICTS FOR SAFETY, SECURITY AND DISASTER RECOVERY

- Information Communication Technology (ICT) is a crucial tool to support effective communication and decision-making under complex and uncertain environments of disasters by enhancing cognitive capacity of emergency managers.

- With the continuous influence and evolution of communication technologies, information sharing and decision-making has drastically changed and affects each phase of emergency management.

ICTS FOR SAFETY, SECURITY AND DISASTER RECOVERY

- Natural disasters are becoming more frequent, growing more severe and affecting more people than ever before. The reasons vary but include climate change, population growth and shifting habitation patterns.

- Developing the tools, processes and best practices to manage natural disasters more effectively is becoming an increasingly urgent global priority.

ICTS FOR SAFETY, SECURITY AND DISASTER RECOVERY

- Ongoing challenges in disaster management — such as cross-border issues when disasters affect more than one country, or the need to normalize data so that critical information can be quickly communicated, understood and acted upon — reinforce the need for such clarity and structure.

ICTS FOR SAFETY, SECURITY AND DISASTER RECOVERY

- Another challenge to the effectiveness of disaster management and recovery is sharing information across organizations hampered by a lack of interoperability.
- In a disaster management situation, information is widely distributed and owned by different organizations, critical data is maintained in disparate systems that often don't interoperate well, and there are no common standards to enable organizations to efficiently organize and share their resources during response operations.
- To complicate matters, disaster management teams may be dealing with a badly damaged infrastructure making information sharing nearly impossible.

ICTS FOR SAFETY, SECURITY AND DISASTER RECOVERY

- Another fundamental challenge is the need to automate manual records for disaster response and humanitarian assistance organizations, which is just as important as, if somewhat less glamorous than, other critical issues affecting their readiness.
- True interoperability is about connecting people, data and diverse processes and organizations, which requires not only flexible technology and accepted standards, but also the fewest possible bureaucratic and regulatory barriers.

ICTS FOR SAFETY, SECURITY AND DISASTER RECOVERY

- In many countries, the people and organizations that work in disaster management also have responsibilities related to national security. The processes and technology solutions they use for critical infrastructure protection can also be adapted for disaster management
- These responders increasingly rely on information and communications technology (ICT) systems that can streamline knowledge sharing, situational analysis and optimize collaboration among organizations.

ICTS FOR SAFETY, SECURITY AND DISASTER RECOVERY

- . Increasingly disaster management organizations look for applications that are industry-proven, robust, cost-effective, interoperable and, in some cases, able to operate with limited or intermittent connectivity and various levels of network capacity. When considering disaster management solutions, it's important to look for the following capabilities and benefits:

ICTS FOR SAFETY, SECURITY AND DISASTER RECOVERY

- ✓ Optimized situational awareness. Real-time communication, data management and data transmission deliver a full picture of the situation.
- ✓ Interoperable, collaborative environment. Responders save lives by improving information flow across all types of boundaries.

ICTS FOR SAFETY, SECURITY AND DISASTER RECOVERY

- ✓ Support for mobile, Web-based access across a range of devices. All components and people are connected in fixed and field locations.
- ✓ System security and reliability. A combination of powerful security and performance.
- ✓ Comprehensive system manageability. All facets of the solution are designed to work together.

ICTS FOR SAFETY, SECURITY AND DISASTER RECOVERY

- Change occurs rapidly in disaster management. Mandatory policies and procedures frequently require the modification of existing systems.
- The ability to rapidly adapt applications to keep pace with evolving situations benefits response organizations, and the people who depend on them, while preserving their IT investments.

ICTS FOR SAFETY, SECURITY AND DISASTER RECOVERY

- Disaster reconstruction has to start as soon as the initial disaster cleanup has taken place. This is a very complex endeavour, requiring a huge array of skill sets and a thorough knowledge of an ever-increasing variety of techniques and equipment.
- Thus, while the role of ICT in the long-term disaster recovery process is not as apparent as it is in disaster warning, there is no doubt that ICT is being used widely to expedite these activities.

OBJECTIVES OF ICT POLICY

- ICT evolution will take place with or without a systematic, comprehensive and articulated policy. However, the lack of a coherent policy is likely to contribute to the development (or prolonged existence) of ineffective infrastructure and a waste of resources.

ASPIRATIONS THAT ICT POLICIES SHOULD TRY TO MEET

- Providing citizens with a chance to access information,
- Increasing the benefits from information technology for the country,
- Providing information and communication facilities, services and management at a reasonable or reduced cost,
- Improving the quality of ICT services and products,
- Encouraging innovations in technology development and use of technology,

OBJECTIVES OF ICT POLICY

- Promoting information sharing, transparency and accountability and reducing bureaucracy within and between organizations, and towards the public at large,
- Attaining a specified minimum level of information technology resources for educational institutions and government agencies,
- Providing individuals and organizations with a minimum level of ICT knowledge, and the ability to keep it up to date, and
- Helping to understand information technology, its development and its cross-disciplinary
- impact.computers, satellites, broadband access, wireless access and the Internet.

SCOPE OF ICT POLICY

- As many countries are experiencing, an effective ICT Policy usually deals with the issues necessary to guarantee an efficient and effectively competitive communications (encompassing ICT) market so that the benefits created by an effective ICT Policy can then be beneficial and useful to other sectors. Fundamental issues include provision of access through competition, instituting incentives for foreign direct investments and building regulatory institutions that promote transparent and equitable entry to the ICT services.

MANAGING ICT SECURITY RISKS

- Recognition of the need to take security measures seriously can be seen in the increased use of firewalls to protect an organization's data and virtual private networks to control access to an organization's data or network.

- Individuals, businesses and public authorities all need to consider the impact electronic commerce has on the security of their personal details, electronic data and business infrastructure. Particularly in the financial sector ensuring the availability of information systems at all times is very important. Being unable to access a system could potentially lead to legal action as a result, for example, of financial losses where a payment was not processed within a particular time.

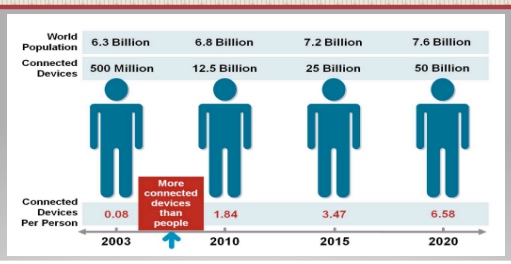
CYBER RESILIENCE

CYBER RESILIENCE

CYBER DISASTER MANAGEMENT

INTERNET OF THINGS

- Internet of Things is going to be come huge, with almost 50 billion devices being connected to the Internet by 2020, as per figures. So issues pertaining to IOT and privacy, IOT and cyber security, IOT and data protection will assume more significance.



ICTS FOR SAFETY, SECURITY AND DISASTER RECOVERY

- Since the end of the 1990s, when the debate about the impact of information and communication technologies on international security was first raised on the international agenda, the number of Internet users has grown over a thousand-fold from just 3 million in 1990 to over 3.2 billion in 2015 and is expected to reach 4.7 billion by 2025.

ICTS FOR SAFETY, SECURITY AND DISASTER RECOVERY

- Most of this growth will continue to come from developing countries, including countries in Asia and Africa. The number of mobile devices is already higher than the world's population. Digital environment and threat landscape are changing too: state and non-state actors increasingly exploit vulnerabilities in cyberspace to gain advantage over their competitors and adversaries.

ICTS FOR SAFETY, SECURITY AND DISASTER RECOVERY

- As recent events and predictions for the future show, now is the time to fill capability gaps with regard to cybersecurity and resilience at the highest level of any organization. The rapid pace of innovation and network connectivity will only increase in the coming years, making board-level action on this topic absolutely urgent.

ICTS FOR SAFETY, SECURITY AND DISASTER RECOVERY

- In the next few years, billions of new devices will connect to the internet as well as to corporate and government networks. These networked devices bring with them the threat of new risks to the enterprise and, more importantly, to networked systems that affect millions of lives.

ICTS FOR SAFETY, SECURITY AND DISASTER RECOVERY

- In the next few years, billions of new devices will connect to the internet as well as to corporate and government networks. These networked devices bring with them the threat of new risks to the enterprise and, more importantly, to networked systems that affect millions of lives.

ISSUES

- As Internet-based platforms and infrastructure continue to grow in importance for the delivery of basic services and become part of critical national infrastructure, the risk of conflict resulting from misunderstandings or misperceptions between countries becomes more acute.
- To reduce the possibility of such a scenario materialising, the international community has engaged in several regional or global processes focused on clarifying how the existing international law applies to cyberspace, development of norms of responsible state behaviour, and development of confidence-building measures (CBMs).

ISSUES

- The difficulties with attribution of attacks give states the ability to deny responsibility, as has been the case for the North Korean government which has consistently denied any involvement in the cyber attacks on Sony Pictures Entertainment.
- The challenges related to attribution are even more daunting if one takes into account the possible consequences of an erroneous attribution and a relatively easy access to instruments for conducting cyber attacks by cyber criminals and hackers.

STEPS/RECOMMENDATIONS/ MEASURES

- Confidence-building measures are one of the key mechanisms in the international community's toolbox aiming at preventing or reducing the risk of a conflict by eliminating the causes of mistrust, misunderstanding and miscalculation between states.

STEPS/RECOMMENDATIONS/ MEASURES

- Cyber security is insufficient if the challenges of digitalization are to be effectively met. Protection is important, but organizations must also develop strategies to ensure durable networks and take advantage of the opportunities that digitalization can bring. While there are many broader definitions of cybersecurity, there is a difference between cybersecurity and the more strategic, long-term thinking cyber resilience should evoke.

INTERNATIONAL COOPERATION

- In the field of cybercrime international coordination and cooperation is vital. Cybercrimes are not limited to national boundaries and the detecting and prosecuting of these activities will likewise necessarily cross these boundaries.
- Cybercriminals may choose to route their communications through several jurisdictions in order to try to avoid detection and likewise the evidence of their crimes may be located across a variety of jurisdictions.

INTERNATIONAL COOPERATION

- The Council of Europe has drafted a Council of Europe Convention on Cybercrime which since 2001 has been signed by 38 out of 47 members of the Council of Europe; although Azerbaijan, as the only SPECA member country who is also a member of the Council of Europe, has not yet signed. Canada, Costa Rica, Japan, Mexico, South Africa and the United States are also signatories to the Convention. The Convention addresses issues of substantive and procedural criminal law, which Member States are obliged to take measures to implement in national law, as well as issues of international cooperation. In terms of offences, Section 1 of the Convention distinguishes four categories of offence:

THE ROAD TO RECOVERY

- The private sector, public sector and nongovernmental organization community must work together to deploy technology solutions in the most effective manner, and to ensure that solutions are appropriate, sustainable and designed to achieve the best possible results.

THE ROAD TO RECOVERY

- Moreover, technology can be a powerful force that opens exciting opportunities for organizations to better achieve their missions and accelerate their impact.