ICTS FOR SAFETY AND SECURITY- LEGAL, POLICY & REGULATORY ISSUES

A PRESENTATION
BY
PAVAN DUGGAL
ADVOCATE, SUPREME COURT OF INDIA
CHAIRMAN, INTERNATIONAL COMMISSION ON CYBER SECURITY LAW
PRESIDENT, CYBERLAWS.NET

CYBER DISASTER MANAGEMENT

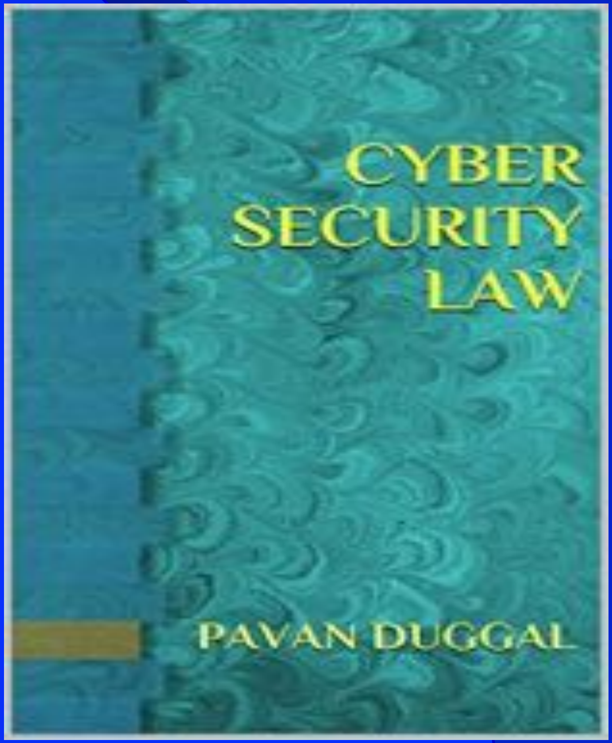
Safety issues with ICT

IMPORTANCE OF DISCIPLINE OF CYBER SECURITY LAW

- ❑ Given the significance of cyber security, it is but natural to expect that legalities and connected issues concerning ICT and cyber security will engage the attention of relevant stakeholders. Hence, Cyber Security Law as a subject assumes prominence. Cyber Security law is an important emerging discipline in the overall discipline of Cyberlaw.

DEFINITION OF CYBER SECURITY LAW

- *Cyber Security Law can be defined as "the new emerging legal discipline within the Cyberlaw umbrella, which deals with all the legal policy and regulatory issues pertaining to cyber security, its protection, preservation, maintenance and continued updation."*



CYBER SECURITY LAW

- All legalities pertaining to unauthorized intrusion into computer networks, computer resources and communication devices by various state and non-state actors having ramifications, not just on the security of the said resources, networks and communication system but also on electronic data resident therein, are covered within the broad umbrella of Cyber Security Law.

DEFINITION OF CYBER SECURITY LAW

- Cyber Security is today becoming extremely complicated and is directly connected with the national security of nations, apart from protecting sovereign interests of nations in cyberspace.

DEFINITION OF CYBER SECURITY LAW

- Cyber Security Law as a discipline, deals with the legal protection and preservation of Cyber Security of computer networks, computer resources, information infrastructure, Critical Information Infrastructure and other information resources which host, deal, handle, process all kinds of data, whether sensitive or non-sensitive, personal, non-personal or otherwise.

ICTS FOR SAFETY AND SECURITY

- 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 clarity on legal and policy issues connected therewith

ICTS FOR SAFETY AND SECURITY

- 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.
- Hence, legal issues based frameworks need to be implemented at the earliest.

ICTS FOR SAFETY AND SECURITY

- .
- 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 AND SECURITY

- ✓ 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 AND SECURITY

- ❑ 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.

NEED 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.

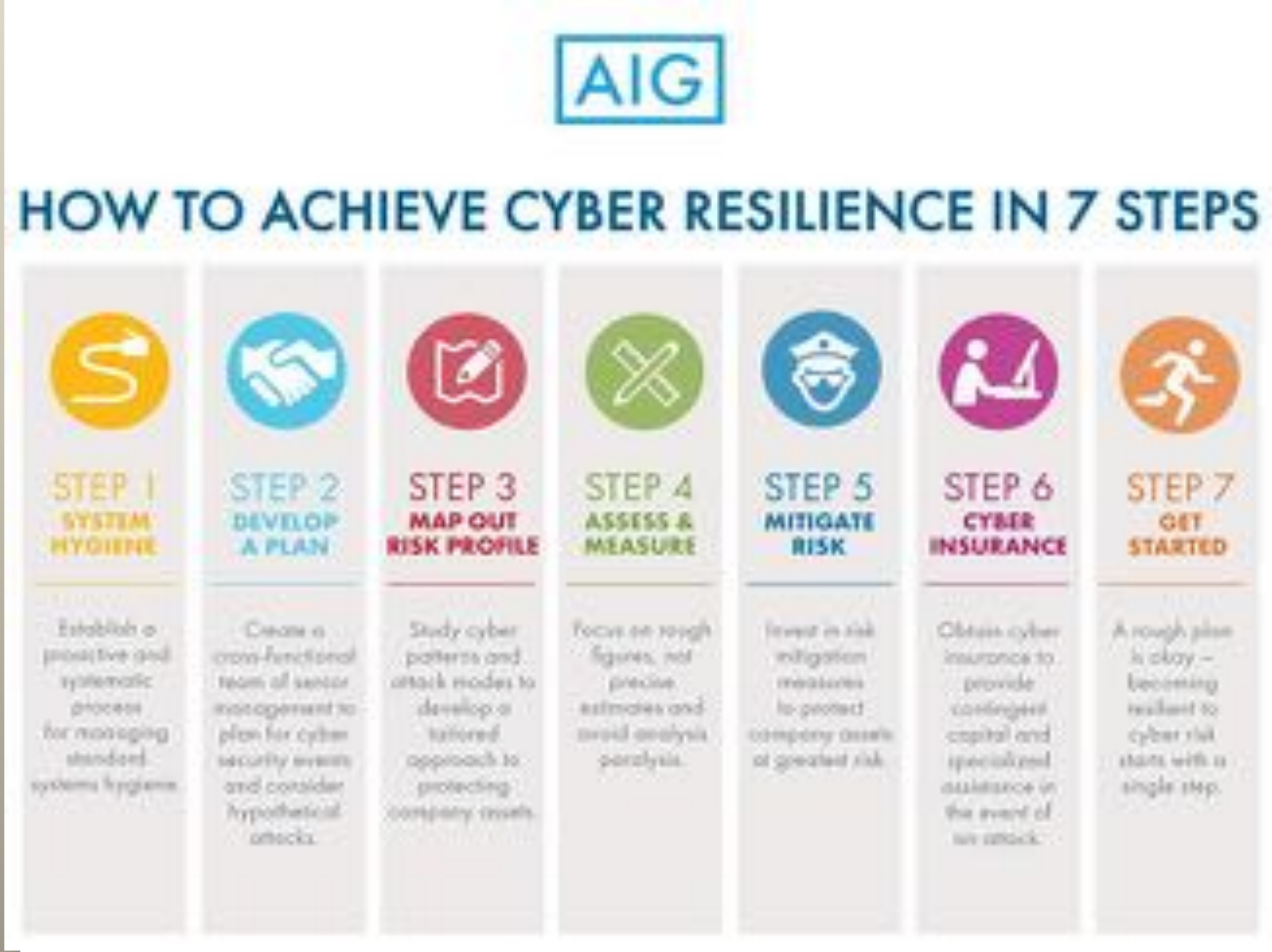
SCOPE OF ICT POLICY

- an effective ICT Policy usually deals with the issues necessary to guarantee an efficient and effectively competitive communications (encompassing ICT) market .
- 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.
- To fulfill the requirements of an information society, the information technology, broadcasting and telecommunications components have to all contribute holistically.

INTERNATIONAL COMMISSION ON CYBER SECURITY LAW

- The International Commission on Cyber Security Law is examining the legal, policy and regulatory issues concerning cyber security not only in the physical world but also on the darknet as also ICTs Securitys

CYBER RESILIENCE



AIG

HOW TO ACHIEVE CYBER RESILIENCE IN 7 STEPS

STEP 1
SYSTEM HYGIENE
Establish a proactive and systematic process for managing standard systems hygiene.

STEP 2
DEVELOP A PLAN
Create a cross-functional team of senior management to plan for cyber security events and consider hypothetical attacks.

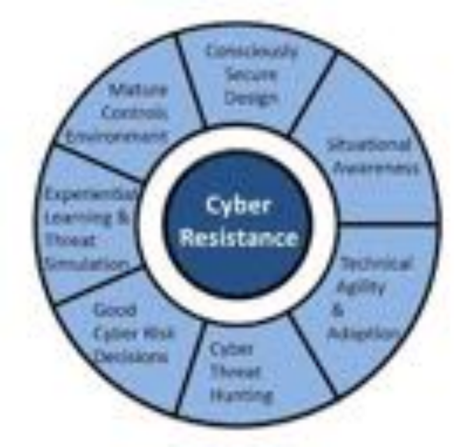
STEP 3
MAP OUT RISK PROFILE
Study cyber patterns and attack modes to develop a tailored approach to protecting company assets.

STEP 4
ASSESS & MEASURE
Focus on rough figures, not precise estimates and avoid analysis paralysis.

STEP 5
MITIGATE RISK
Invest in risk mitigation measures to protect company assets at greatest risk.

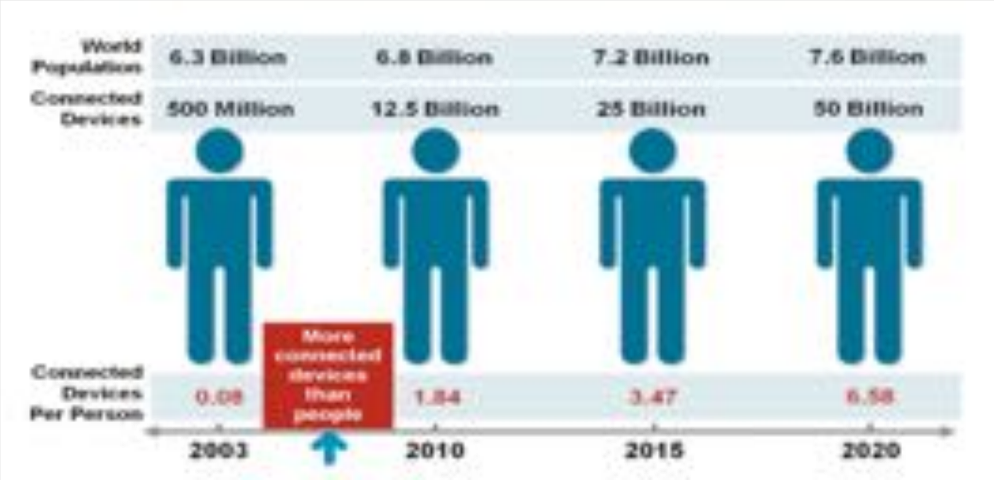
STEP 6
CYBER INSURANCE
Obtain cyber insurance to provide contingent capital and specialized assistance in the event of an attack.

STEP 7
GET STARTED
A rough plan is okay – becoming resilient to cyber risk starts with a single step.


Cyber Resistance
Consciously Secure Design
Situational Awareness
Technical Agility & Adaption
Cyber Threat Hunting
Good Cyber Risk Decisions
Experiential Learning & Threat Simulation
Mature Controls Environment

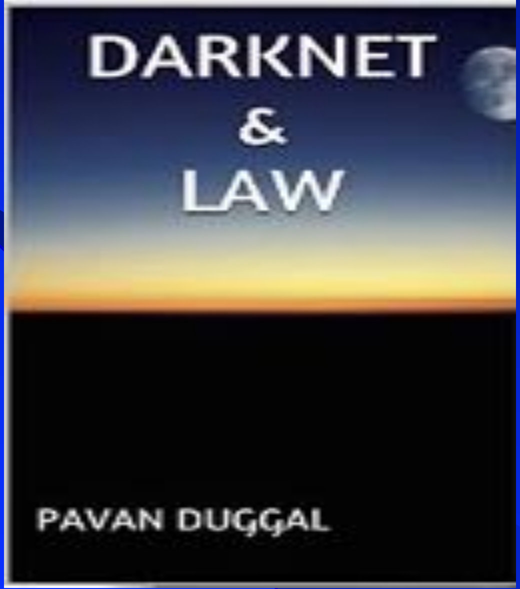
INTERNET OF THINGS

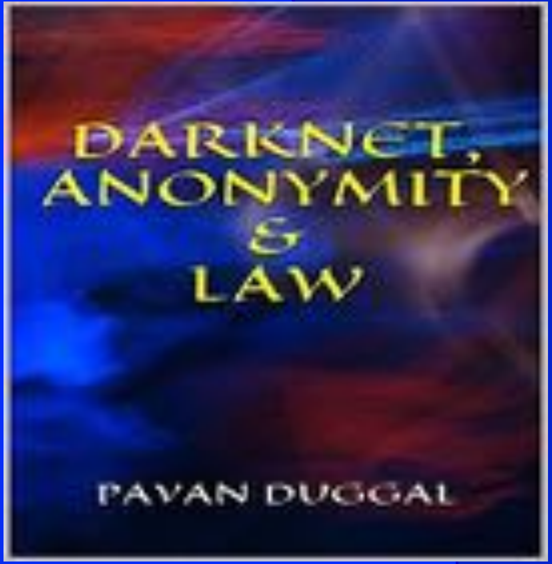
❑ Internet of Things is going to be come huge, with almost 50 billion devices being connected to the Internet by 2020, as per figures. So issues pertaining to IOT and privacy, IOT and cyber security, IOT and data protection will assume more significance.



DARK WEB & CYBERLAW

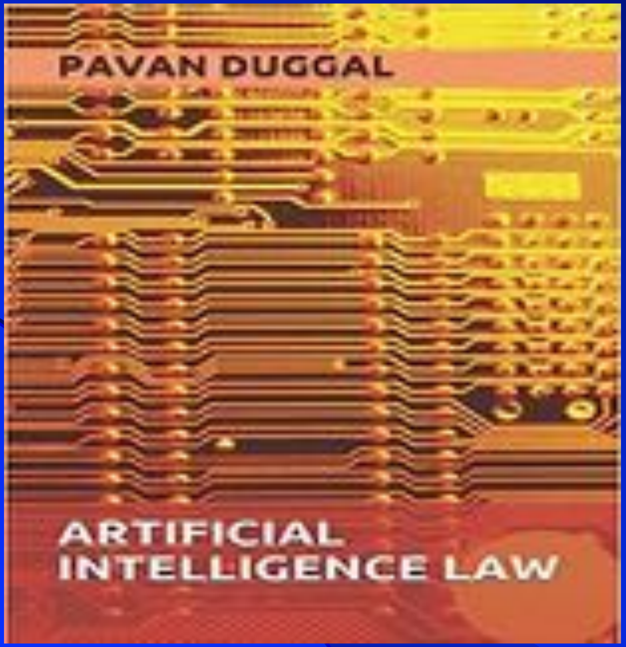
- ❑ Dark web is a new reality. However, the law-enforcement agencies and legal regimes are thoroughly incapable of dealing with dark web.
- ❑ Use of Dark Net for cybercrime activities- Cybercrime as a way of life





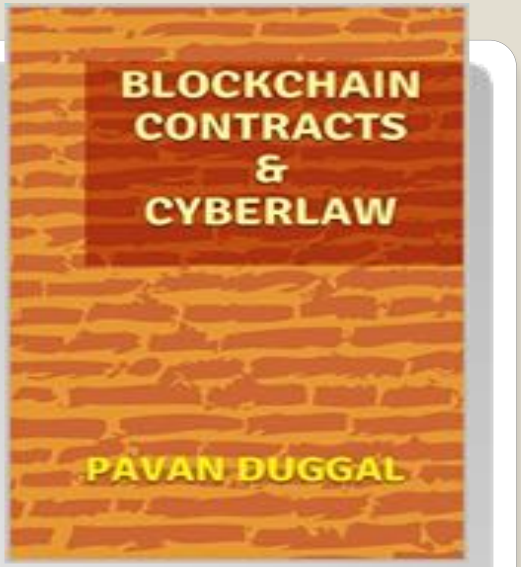
© of images belongs to the respective copyright holders

ARTIFICIAL INTELLIGENCE



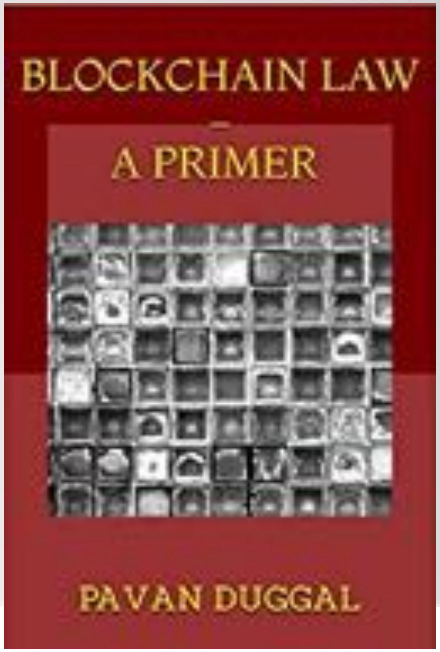
BLOCKCHAINS

- Blockchains are bringing in new opportunities for security for ICTs
- Legalities regarding Blockchains need far more clarity.



BLOCKCHAIN CONTRACTS & CYBERLAW

PAVAN DUGGAL

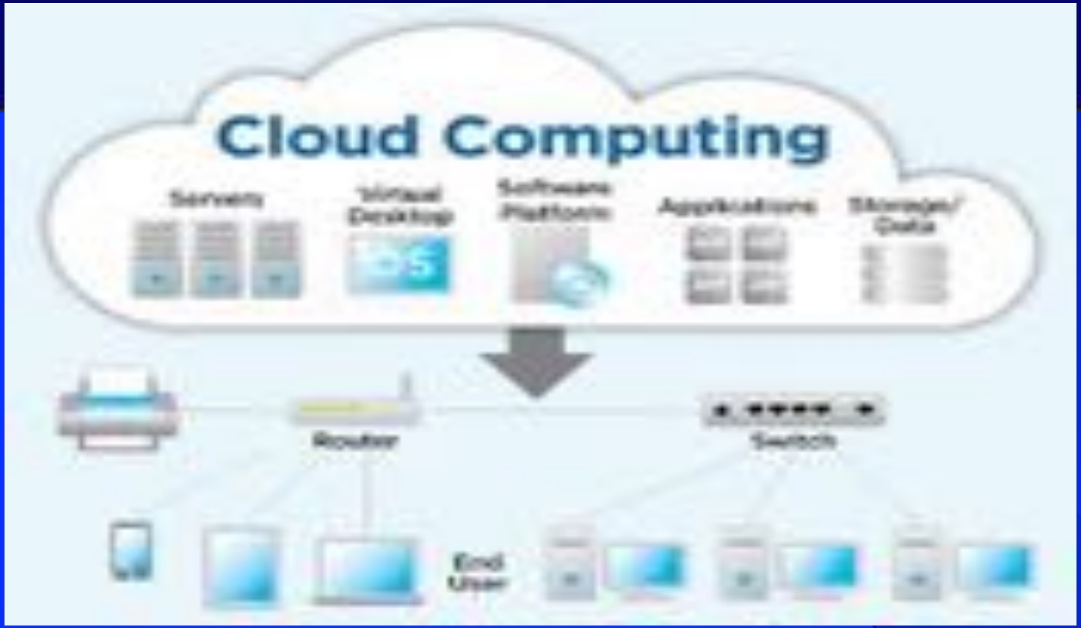


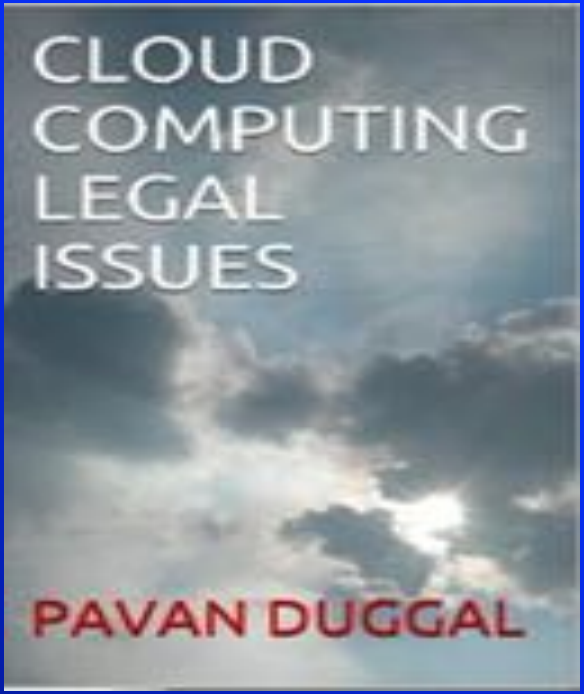
BLOCKCHAIN LAW

A PRIMER

PAVAN DUGGAL

CLOUD COMPUTING

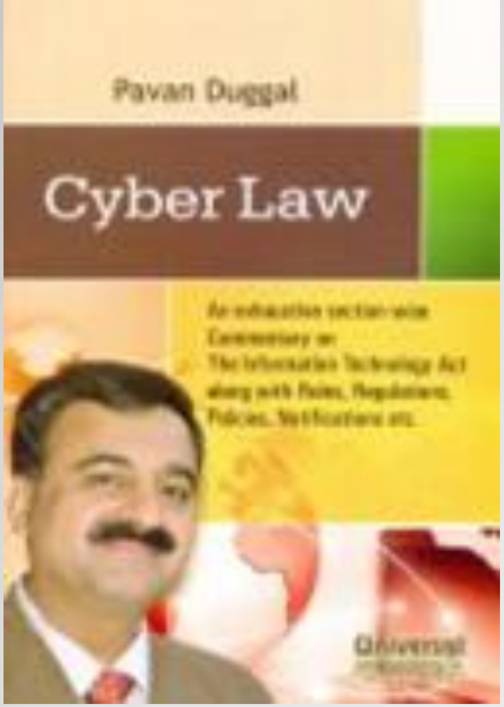


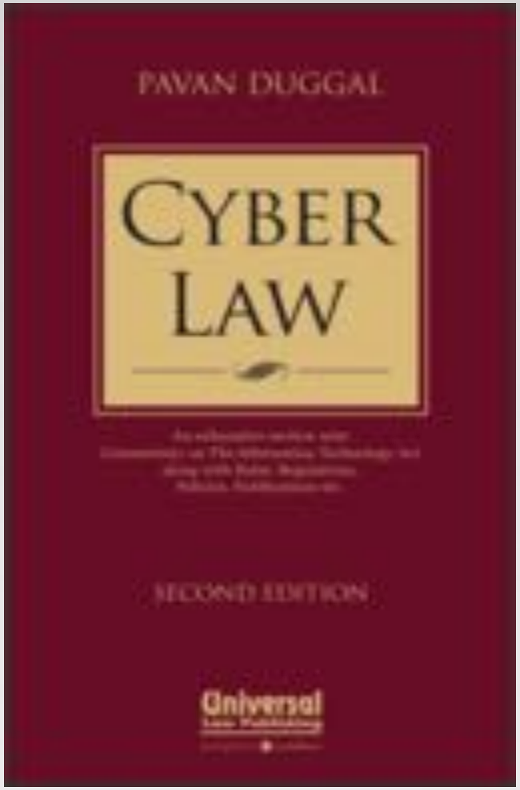

CLOUD COMPUTING LEGAL ISSUES

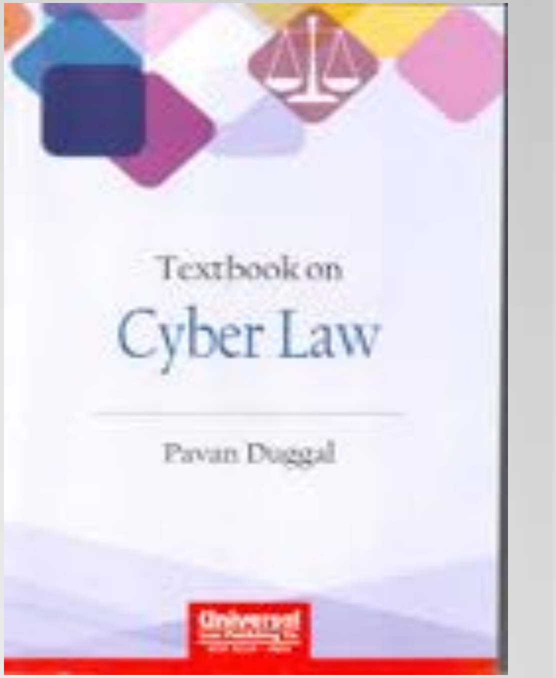
PAVAN DUGGAL

CYBERSPACE – THE NEW SPACE OF WAR

CYBERLAW


Pavan Duggal
Cyber Law
An exhaustive section-wise Commentary on The Information Technology Act along with Rules, Regulations, Policies, Notifications etc.
Universal





© of images belongs to the respective copyright holders

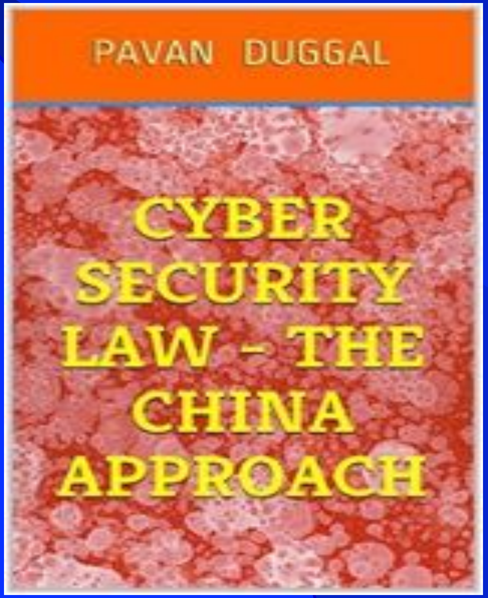
DEVELOPMENTS AT INTERNATIONAL LEVEL

- Countries are now being increasingly concerned about the entire issue pertaining to cyber security, as cyber security impacts not only the economy but also the sovereignty of nations.

- There is no international framework on cyber security and countries are increasingly taking it upon themselves to come up with their own national legislations to deal with cyber security breaches.

ICTS FOR SAFETY AND SECURITY

- 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.



PAVAN DUGGAL

CYBER SECURITY LAW - THE CHINA APPROACH

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 resilience is more a matter of strategy and culture than tactics. Being resilient requires those at the highest levels of a company, organization or government to recognize the importance of avoiding and proactively mitigating risks. While it is everyone's responsibility to cooperate in order to ensure greater cyber resilience, leaders who set the strategy for an organization are ultimately responsible, and have increasingly been held accountable for including cyber resilience in organizational strategy.

STEPS/RECOMMENDATIONS/ MEASURES

- Some countries and international actors have also established bilateral venues for cooperation. The EU, for instance, has established a number of dialogues with third countries to enhance cooperation in the fight against cyber crime. In September 2015, the US and China agreed to establish a 'high-level joint dialogue mechanism on fighting cyber crime and related issues'.

INTERNATIONAL COOPERATION

- In the field of cybercrime international coordination and cooperation is vital.
- Multinational agreement to provide for assistance in the investigation and prosecution of crimes is therefore necessary.

INTERNATIONAL COOPERATION

- In 2005 the Virtual Global Taskforce was established by Interpol in connection with national forces in the United Kingdom, the United States, Australia and Canada to deal with child pornography.
- There have been several initiatives designed to promote international coordination in this area including the OECD Guidelines for the Security of Information Systems and Networks.

INTERNATIONAL CONFERENCE ON CYBERLAW, CYBERCRIME & #CYBER SECURITY –14TH – 16TH NOVEMBER, 2018, NEW DELHI, INDIA

Cyberlaws.Net & Pavan Duggal Associates
Present
INTERNATIONAL CONFERENCE ON
CYBERLAW,
CYBERCRIME & CYBERSECURITY
Microsoft

- The International Conference on Cyberlaw, Cybercrime & Cyber Security (www.cyberlawcybercrime.com) has provided the platform to discuss about emerging Cyberlaw, Cybercrime and Cybersecurity trends.