International Journal of Cyber Criminology
Vol 13 Issue 1 January – June 2019

Book Review of *Principles of Cyber Crime*

Joydeep Dass[1]
International School of Management Excellence, Bengaluru, India

Principles of Cyber Crime (2015). Jonathan Clough, Cambridge University Press, New York, NY. U.S, ISBN-13, 978-0-521-89925-3, Available at www.cambridge.org/9780521899253.

Part-I, "Introduction", (Pages 59-80) of the book begins with a discussion on the evolution of cyber-crime with the advent of the digital technology. The inroads of technology in every sphere of human activity, both personal and business. Subsequently few countries introduced legislations to counter these attacks from cyber criminals. Technological advancements will continue and will offer new challenges making every individual vulnerable to cyber-attacks. The next section discusses the prominent factors, which facilitates the commission of cyber-crime. The internet has penetrated across the globe on a mass scale giving increasing scope to offenders, enhancing vulnerability and exploitation of the victim. The technology is so easily accessible and available to all giving an easy handle to offenders to commit crimes. Anonymity is another advantage to the offender who can easily conceal identity without leaving a trace of a crime committed. Millions of data can be stored and transmitted in seconds and the convergence of computing and communication has made this seamless across the globe. Law is restricted to regions but technology has transcended national boundaries and cyber offenders can execute attacks from any part of the world. Lastly, electronic data are sophisticated, exist in various forms, difficult to preserve and retrieve for prosecution and trial of criminals, which is a big challenge for the law enforcement agencies. Further, in cyber-crimes the offender and the victim is in different geography, the investigative actions becomes a challenge because of myriad of laws coupled with the problems of administrative sanction, coordination and communication.

The author emphasized the role of technology in the commission of the crime, used the word 'Cybercrime' in the entire book because of its common usage, obvious reference to networked computers, and specific definition given by the Council of Europe convention on cyber-crime. The author has quoted the definition of the US department of justice. First, computer or computer network is the target of the crime. Second, Computer is a tool used in the commission of the crime and third, computer records as evidence incidental to the occurrence of the crime. Cyber terrorism is a term used similar

[1] Assistant Professor in Finance, International School of Management Excellence, 88 Chembanahalli, Near Dommasandra Circle, Sarjapura Road, Bengaluru, Karnataka, 562125, India. Email: joydeep@isme.in

to cyber-crime to describe attacks on critical infrastructure to disrupt essential services as opposite to terrorism that focus on the use of violent action. Technology is the enabler of cyber terrorism and the underlying motivation may be to cause harm to person or property, propagate ideological agendas, garner public opinion or to influence some form of government action. Survey number indicate that cyber-crime related cases either are ignored or deliberately not reported in crime statistics especially those, which has the extensive use of technology.

The author further urges that there should not be any distinction or inconsistency between online or offline cybercrimes concerning regulation and prosecution. Debates related to virtual crime is beautifully explained with two debatable questions as to where such crimes occur and if they do, does it occur in cyberspace and whether there should be separate and distinct legislations to counter these crimes. Finally, there is a growing international consensus on the global problem of cyber-crime with greater awareness and harmonization of procedures by OECD, UN, Council of Europe, G8, G20 and the Interpol. The cybercrime convention is an international response to the problems of cyber-crime with separate chapters in the book covering categories of offence, procedural and substantive law, international cooperation, information exchange, extradition, mutual assistance, liability, sanctions and jurisdictional principles. The writing style is conversational, simple, clear, concise and easy to understand for the readers. Appropriate references are available wherever relevant against each paragraph.

Part-II titled 'Computer as Target', (Pages 83-179) of the book contains eight sections with specific subjects discussed in sub-sections. 1) Introduction – The author discusses 'Hacking' and the underlying motivations for this class of offense. Hacking involves three categories of conduct, unauthorized intrusion to computer networks, circulation of malicious software (Malware) or codes for damaging and impairing of computer data and denial of service attacks with an intention to access information, modify or tamper data and unauthorized use of computers. 2) The prevalence of cyber-crime –Majority of cyber-crime incidents go un-recorded in crime statistics and most of them relate to virus infection, insider abuse of access and thefts. 3) The legislative environment – Conviction and trials in offences related to cyber-crime is not fair and speedy due to different interpretations in various jurisdictions. Example, if computer to be categorized as 'property' or a theft of computer data as cybercrime or simply property theft. This hampers international cooperation, investigation and prosecution. The author has given a brief description of exact meaning of access offences, computer trespass, perspective of what exactly is an internal or an external access, data information or computer program. The explanation of 'fault element" which includes the intention to commit fraud and the type of information accessed. The definition provided by Cyber-crime convention, criminal law provisions and codes in Australia, Canada, UK, and USA.4)

Impairment of data –This section discusses the conduct, which constitutes data interference, deletion, deterioration, suppression, modification and impairment, damage, loss, as encompassed by the cyber-crime convention and the legislative provisions in Australia, Canada, UK and USA.5) Misuse of devices –Writing malicious code, gaining access to passwords, creation of black market, trafficking of information on the internet, posting security weaknesses on the internet falls in this class of offence. This offense comprises of two parts, first possession, control of data, and second producing, obtaining, trafficking and supply of information. Legislative provisions of cyber-crime convention,

Australia, Canada, UK and USA have been explained briefly. The provisions and definitions related to Counterfeit and unauthorized access device have been adequately discussed 6) Interception of data –The author talks about the next step of vulnerability of the media, that is the interception of data when transmitted over computer Local area network (LAN), Wide area network (WAN) or wireless communication networks. The features of telecommunication, distinction between content and traffic data, live and stored data and these categories of offences include harassment, blackmail, fraud and espionage. The legislative framework of cybercrime convention, Australia, Canada, UK and USA been covered in depth with respective country analysis.

Part-III titled 'Fraud and Related offences', (Pages 239-300) of the book talks about online frauds, especially the anatomy of Nigerian mail frauds, the solicitation of email messages that asks the recipient to help the sender to move large amount of funds out of the country in exchange of commissions and a upfront deposit of fees to bribe the custodian of funds. The author explains how this email fraud which originally started by conventional mail grew into a worldwide scandal with the growth of internet as a large dominant marketplace. 1) Fraudulent sales online - Merchant solicitation emails for release of goods in exchange for funds. The prominent fraud committed under this category is the auction frauds, non-delivery of merchandize, inferior quality delivered, or non-payment for goods ordered, card not present transactions, billing done for services not existing, and long-distance telephony charge levied for internet and 'Scareware'. Scareware is a free file scan download request made to cleanup computers and later the customer discovers that with the download the computer was infected. The customer is than asked to purchase software to clean up the computer. 2) Advance fee scheme, the victim is lured to purchase some benefits or services which is non-existent. Work from home schemes where the bank account information is fraudulently collected for money laundering purposes by promising home assignments and in exchange asking bank account numbers to deposit the remuneration. The author has justified the enormity of these crimes with actual survey results. 3) Electronic fund transfer crime, where virtual money instead of the hard cash is transferred using unauthorized passwords to jurisdictions with lax regulations in order to escape detection or evade taxes. Real life examples and incidents have been narrated wherever appropriate. 4) Fraudulent investments, attractive return generating schemes are launched to solicit investment, which eventually turn out to be fake. Typically, these frauds are called 'Get rich quick' schemes. Some of the investment frauds to influence share prices artificially like 'pump and dump', 'trash and cash', 'stock price' scheme is discussed in brief. 5) Identity crime, the taxonomy is explained in brief, identity fraud where false identity is used to earn money, goods or services or government benefits. Identity theft, the assumption of pre-existing identity, identity breeding, continuing with the false identity to commit successive frauds. The category of offence include money laundering, drug trafficking, tax evasion, illegal immigration, and terrorism and how the digital technology has accentuated this type of crime. Further, there is a lucid explanation of the techniques of committing this crime like 'dumpster diving', that is looking for discarded financial statements or other identifying information. 'Social engineering', where the victim is tempted to provide personal information with the promise to offer jobs or an assurance of guaranteed gifts or prize money from a contest. Signature forgery, the ability to create false identification documents from scanned images or from reproduced documents.

6) Phishing, a technique used to gather personal, financial and sensitive information using fake web links, the request appears to have come from legitimate sources. For example a bank asking to re-verify account numbers. 7) Pharming, the technique to divert valid emails to phishing sites when an unsuspecting user types in the browser. Techniques of pharming like Domain Name Servers (DNS) poisoning, conversion of web text address to numeric IP address. The author has touched upon few technical skills, in simple language, like the methodology used by key loggers to collect and steal data which will be of interest and knowledge to the readers. 8) Credit card skimming, the process of exploiting the magnetic strip technology to illicitly capture or copy credit card information. The modus operandi of card skimmers and 'Shoulder Surfing', the covert observation of a person entering his Personal Identification Number (PIN) using a concealed camera is explained in a clearly understandable language. 9) Carding, the acquisition, distribution and use of credit and debit card information for monetary gains and the trading of that identity information on the Internet by Organized crime gangs. 10) Scale of the problem – The author contends that identity crime is mostly financial, difficult to record and crime statistics record the occurrence of fraud but not the methods used to commit the fraud. Statistical collation is difficult, victims generally write off the loss, and Organizations are reluctant to report incidents for fear of undermining consumer confidence and cost burdens associated with rectifying and investigation of identity crime is high. Prevention and countering these frauds involve coordinated approach from consumers, business groups, enforcement authorities and strong privacy legislation. Identity fabrication or the creation of false identity or identity manipulation the alteration of existing identity are the common types of identity frauds. The author categorizes identity information into three types. Biometric identity, physical features of the individual, like DNA profile, fingerprints. Attributed identity, aspects related to birth like body mark, parental characteristics. Biographic identity, identity acquired over a period like qualifications, employment history, license and passports. The jurisdictional definition of identity documentation, authentication feature, possession and dealing of identity information, tracking of identity information, manufacturing identity information is discussed at length.

11) Criminal copyright infringement –The author says that copyright infringement is neither a theft nor a fraud, but the abuse of exclusive rights of the copyright holder. Copyright infringement, most significantly are those related to reproduction and distribution on the P2P network. The author has provided the statistics of copyright violations in the US, the progress made so far, the increasing crime of piracy in China and the survey results in UK. The enforcement of copyright infringements have been a matter of civil law but the perception is gradually changing to make copyright infringement a subject of criminal law and enforcement action have assumed international dimensions. The legislative provisions of cybercrime conventions, specially the digital rights management (DRM) protection, the technology to identify and protect intellectual property in digital format. Technology protection measures (TPM), technical measures to protect copying and Rights management information (RMI), management and distribution of digital works to consumers is discussed in brief. The author attempts to differentiate civil and criminal copyright infringement especially the digital part. First, the requirement that infringements should be commercial in nature, second, the exclusive rights of distribution, third the requirements and application of *mens rea* (evil motive) or

extent of culpability, fourth, the imposition of penalties and fines. 12) Spam or the electronic junk mail –The author speaks about the unsolicited spam emails and how it has assumed enormous unmanageable proportions, modern communication has enabled the growth of spams, with significant reach of audience. Major efforts to mitigate the spread of spams has not yielded any meaningful results, filtering software's have been inefficient, cost burden on the consumer has increased, spam content is offensive, malicious and offensive, a medium to spread virus and the dangerous trend is the use of botnets. The author suggests that to regulate the growth of spam, there has to be a strong anti-spam legislation, education and awareness of the email users and Industry code of conduct to be introduced specially for the direct marketing industry. Present efforts to contain the growth of spam has not been successful due to the inability to locate the origin of spam, variety of techniques used by the spammers, agencies dealing with these cases have restricted and limited powers, absence of a common civil enforcement approach in different jurisdictions, and the inability to prove damages in spam related cases. Nevertheless, Australia, Canada, UK and the USA has passed some legislations and key features of the legal provisions relate to civil and criminal enforcement of commercial and bulk email, consent of the recipient, spam related conduct like address harvesting, forgery of the subject line, automatic generation of multiple emails, unauthorized relay or transmission of messages, sending emails to non-existent addresses and criminal provisions only.

In Part IV titled 'Content Related offence', (Pages 303-384) the author starts with the discussion on the menace of child pornography 1) child abuse online, the massive proliferation of digital technology and the dissemination of sexually abusive material on the internet. In earlier days, the crime was difficult to commit because it required physical processing of films, costly equipment, difficulty in use and the transportation of content was difficult and hardly escaped detection. The significant rise of this form of crime was in the last two decades was possible due to relatively internet becoming more pervasive, cheaper technology, easier access and transmission, storage and portability. Further, the technology has also enabled "virtual child pornography" where an image is created, copied and transferred in real time and multiple copies flashed without involving any actual children. The spread is faster, in large volumes with minimal cost and anonymity without leaving any trace of the perpetrator. The communication technology further facilitated exchange of information, techniques to avoid detection and strategies to encourage and exploit the children to engage in sexual activity. Spurt of incidents related to trade in child pornography have been reported and is emerging as a profitable business for organized crime groups. Much of the international effort to tackle cyber-crime is focused on containing child pornography and presents a considerable challenge for the law enforcement agencies.

2) Criminalization of child pornography, initially production and distribution of child pornography was an offence but not the possession of obscene materials. Now it extends to all forms and all jurisdictions have realized the need for strong prohibitions in order to stop the international trade of such materials. The author has narrated the famous case of *R vs Sharpe*. The Supreme Court of Canada has accepted the fact that prohibition of child pornographic material is linked to reducing sexual abuse of children in five ways. The author provided five arguments in support to justify criminalization of child pornography. First, child pornography creates cognitive distortions in the mind of the offender, which could lead to actual sexual abuse. Second, child pornography could instigate feelings of fantasy and ultimately lead to child abuse even if there is no direct assault on children.

Third, prohibition of child pornographic material has a direct impact in controlling such crime by law enforcement agencies, seen as a positive side effect of law. Fourth, child pornography could be an aid to grooming and seducing child victims and lastly, child pornography uses real children, which gives a supreme feeling to the offender that he created something extraordinary and attempts to trade and build a market out of it. Legislators in all jurisdictions are either framing new rules or amending existing ones to curb the spread of child pornography.

The author has mentioned some notable laws with criminal provisions like the 474.19 and 474.20 federal criminal code of Australia, 163.1 of Canada, Protection of Children Act 1978 of the UK. Protection of children against sexual exploitation act of 1977, Child protection act of 1984, Child protection restoration and penalties enhancement act of 1990, Child pornography prevention act of 1996 and the Prosecutorial remedies and other tools to end the exploitation of children act of 2003 (PROTECT) of the US. 3) Definition of child pornography, given the nature of crime, the author has provided the definition of child pornography as per the cybercrime convention and includes visual depiction of minor or a person appearing to be a minor engaged in sexually explicit conduct or realistic images representing a minor in sexually explicit conduct. The author focuses his discussion on four issues, the definition of the 'minor', acts that constitute 'sexually explicit conduct', definition of pornographic data and 'virtual' child pornography. Minor constitutes a person who is under the age of 18 years and in some jurisdictions, it is 16 years. There is a thin line of difference between the legal age to consent for sexual activity and actual participation in sexually acts.

Sexually explicit activities include real or simulated intercourse between minors, or between an adult and a minor of the same or opposite sex. Bestiality, masturbation, sadistic or masochistic abuse, extreme nudity, unnatural pose, inappropriate attire full or partial, lascivious exhibition of the genital or the pubic area of the minor or child erotica. In the internet age, all material exists in the form of data but child pornography materials constitute any medium of depiction to include text, sound, speech, video, visual images, photographs, pseudo-photographs, representation, morphed images, signals, and data or in any other form or combination of forms. Different courtroom interpretations and judicial pronouncements in various case laws are given in support. Offenders are smart enough to use sophisticated means to create 'virtual' child pornography. For example manipulating an adult image to appear childlike or composite image where the part of one image is transferred to another part of another image to appear as if the whole image is that of the child. 'Morphing' is an act of producing a new image using other two images. Cybercrime convention describes specific offences, which are criminal implications if committed intentionally and encompasses several acts suggestive of sexual willingness. These include producing, offering or making available, distributing or transmitting, procuring and possessing child pornographic materials using a computer system. Producing would mean directing, manufacturing, issuing, publishing and advertising. Offering or making would mean publishing, making available, soliciting, showing or advertising. Distributing or transmitting would mean transporting, importing and exporting of images. Procuring would mean accessing, downloading of content, causing to transmit, receiving or requesting pornographic material. Lastly, possession of pornographic content, which could be intention to possess, simple possession or physical possession with an additional intent to supply or sell. It also includes actual physical custody, de facto custody, and knowledge

of possession. Accidental possession or ignorance would require extra judicial scrutiny. In number of cases, prosecution for possession is initiated based on deleted or destroyed images from the records available with forensic experts and could be a sufficient ground for conviction. Similarly, pleading forgetfulness, carelessness or negligence in possession of pornographic materials also calls for separate investigation to determine offence under the law. Certain defenses are available against the offense of possession of pornographic material, which could be for a 'legitimate or genuine reason' or for 'public good or morality' like administration of justice, pursuit of science, literature, art or for general public interest. For example, a police officer coming across such material in the course of performance of his duties or an academic researcher studying the effects and exposure of child pornography on the society and community life. Honest intention and good faith is a precondition to absolve oneself from the charges of offense under the laws.

In Part V, titled "Offences against the Person", (Pages 387-458) the author starts with an online conversation named 'caspercock' and 'angelgirl12yo'. 'angelgirl12yo' is a male special agent working with Wyoming Division of criminal investigation and 'caspercock' an online sexual predator, named Timothy Wales, a convict sentenced on charges of sexual assault and served prison term for over 15 years. 1) Online grooming, the act of befriending a child by an would-be abuser with an intention to gain the child's confidence and trust and get the child to acquiesce to abusive activity. With Internet penetrating in every house across the globe, communication with children is easier, intimate, and the abuser is able to adopt different persona, operate remotely, and conceal his actual identity to hoodwink the victim. Grooming involves a range of behavior. The author has used the typology used by O'Connell (2003) in his paper titled *"A Typology of Child Cybersexploitation and Online Grooming Practices"*. First, the friendship forming state the offender attempts to establish connection with the victim and finds out if the victim is willing to continue the communication. Second, the relationship forming stage where the offender wins the victims trust and confidence and attempts to gather information. In this stage, the offender deceives and exploits victim's feeling of loneliness, curiosity, low self-esteem, and sexual curiosity, temptation to earn money or exploit the vulnerability to minor psychological disorder. Third, risk assessment stage the offender conducts investigation and gathers information of the victim's location, distance of police from the place of the victim, computer network, family members or siblings to assess the risk of getting exposed in the crime commonly called the 'dry run'. Fourth, the exclusivity stage where the trust and confidence fully develops between the victim and the offender. Communication starts with the victim via private chat, email, and phone. Fifthly, the sexual stage where the offender advances to more intimate topics like kissing, request for sexual favors, meeting privately, sexual topics during online communication, exchanging sexual pictures and sharing obscene photographs. Lastly, the conclusion where the offender may abruptly disconnect contact with the victim or may continue the relationship based on apprehension of chances of being caught in the crime or on suspicion that the victim might report to the police or to the relatives or neighbor. Grooming is an inchoate offense and usually precedes the actual commission of the crime and reflects a range of offenses in the continuum. The author categorizes grooming offense asi) transmitting indecent and obscene materials to minors ii) Preparatory offence of sexual grooming aimed at winning the trust of the victim and thereafter the actual commission of the crime. iii) Inducing or procuring, the offender encourages, entices or coerces the

minor to indulge in sexual activity, for example masturbation or persuade the minor to observe masturbation, or using webcam to depict any other indecent sexual activity. iv) The final stage of grooming is the offender travelling to the victim's place or taking the victim to undisclosed locations for the purpose of sexual activity.

2) Cyberstalking, a conduct in which the offender inflicts unwanted repeated intrusions and communication on another to such an extent that the victim develops fear for safety. The purpose could be simple enjoyment, lust, jealousy, resentment, obsession, or a desire to exert control. The offender could be an ex-partner, former colleague, distant acquaintances or a stranger and these class of offenders are predominantly male suffering from Erotomania or delusional conditions. Some of the common forms of stalking could be online surveillance, harassing phone calls, tagging the victim in social media sites, sending offensive pictures and emails or damaging the property of the victim. Stalking, though does not involve physical violence but could last for a period ranging from few days to few years. The consequences of stalking could be lead to deep psychological impact on the victim, reluctance to move out of home or office or in social gatherings, emotional distress, unwillingness or negligence in normal daily life activities, anxiety, constant worry, develop feelings of irritation, sleep disorders, suicidal tendencies or traumatic stress disorders. Cyberstalking is the use of internet, e-mail or other communication devices to stalk another person. It is more common because there is no physical contact with the victim, possibility of direct communication, easily available material on the internet, online forums, chatroom introductions, address books, call records, SMS/MMS, capability to install malwares to gain information to victims personal information. Stalking offences are difficult to prove because of non-availability of accurate data, imprecise definition as to what exactly is stalking making prosecution difficult and another form of stalking which is gaining ground is the online harassment or 'cyberbullying'. In absence of specific anti-stalking legislations in different jurisdictions, the author discussed the key components of staking offences as i) conduct element, includes a list of all activities that the offender may engage in ii) fault element as the subjective fault element, like intention or fear or the objective element that the offender is aware of the consequences and circumstances of the conduct. iii) Impact on the victim in terms of fear or bodily injury.

3) Forms of cyber stalking include i) communicating with the victim via anonymous emails or remailers, threatening emails, electronic chatrooms or instant messenger etc. ii) publishing threatening information or posting false unverified information on the internet about the victim, with an intention to cause harm, intimidate, harass or humiliate the victim. iii) Targeting the victim's computer, with the motive to interfere with the computer network to gain control of activities, modify or delete information. iv) Surveillance, with the purpose of gaining information about the victim or people and close relatives around the victim, maintaining proximity with the victim, monitoring and tracking the movement, physical activities, location of the victim, or invasion of privacy of the victim.

4) Voyeurism, or simply digital voyeurism, an act of surreptitious observation or recording, filming of the activities of another person in a private place without proximity to the victim. Miniature cameras and small mobile phones have made this possible and much easier to engage in covert surveillance. Digital technology has made the still or video images easily reproducible and distributable and the sources of these materials are

hard to retrieve. ii) Criminalization of voyeurism, Voyeurism being covert conduct of observing, recording, and the victim being unaware makes it difficult to prosecute for indecency or distribution of voyeuristic images. The nature of the activity that falls within the scope of 'Private activity' is also limited making it difficult to prove the offense. The author supports the argument for criminalization of voyeurism for the following four reasons. First, it is a privacy offense and the individual right has to have a balance against abusive and arbitrary interference by others. Second, legitimate social, business or legal activities like a journalist taking pictures or an artist making of video in public place or a law enforcement agency engaged in surveillance, freedom of expression should have a tradeoff with voyeurism laws without causing any unnecessary hardship to the victim. Third, voyeurism is in itself a sexually motivated behavior and there has to be a policy justification for prevention of sexual exploitation regardless of whether the victim is aware or not. Fourth, the impact of voyeuristic conduct on the social community and on the victim's feeling of distress, disgust, helplessness, humiliation, violation makes it a strong case for a criminal offense. The author discusses the class of offenses and acts punishable under the voyeurism laws with respect to the following i) Depictions in voyeuristic conduct, include images of nudity, semi-nudity, sexual activity, recording a person in changing rooms, private area or in a lavatory. Passing of illicit material for sexual gratification or stimulation, or involvement in sexual acts of a kind not in public like intercourse or masturbation, passionate kissing, or fondling. ii) Places where the offence is committed such as the toilet, bathrooms, bedrooms, enclosed space, living rooms, saloons or changing rooms, or a place where a person is in a state of undress or engaged in intimate sexual activities normally not in public. Purpose of the act either deliberately or ignorantly is not materially important but as long as the activity is recorded without consent, the offense is considered to have been committed. iii) Medium of recording could be mechanical electronic, or visual. Videotape, web camera, photograph, film, remote surveillance or broadcast and includes any other surreptious mode of conduct. iv) Identification of the fault element is an essential precondition for this offense. It is presumed that the observation or recording has been intentionally done even if it not or for amusement and pleasure. The motive has to be 'sexual purpose'. v) Distribution of images, manual or electronic transmission of recordings, intention to sell, print, copy, publish, circulate or advertise will also constitute an offense but the suffering and humiliation that the victim faced has to be proved. The obscene and indecent content of the communication would determine the quantum of punishment. vi) Defenses or excuses available for this offense are specific government enforcement actions or any action for the interest of safety, security and public good. Acts, which are for non-sexual purpose, may also be available as defense provided the prosecution is able to prove it.

In Part VI, titled "Jurisdiction", (Pages 461-472) the author contends that, territorial based laws is largely ineffective because the offender may be located in any part of the world. Criminal jurisdiction should transcend national boundaries and extend beyond geographical locations for extraterrestrial reach based on the seriousness of the crime, country and international law. He discusses the topic in three contexts:

1) Prescriptive jurisdiction, which is if the state has legislative powers over a particular conduct. Matters become critical when crimes in cyberspace occur in international waters, airspace, or so transient that determining jurisdiction becomes practically impossible. Cybercrime convention has specific provisions, which talk about "Objective territoriality' means claim of jurisdiction for conduct occurring outside but has significant effect within

its jurisdiction. Another provision is 'Protective principle' where the offense committed may have a fundamental interest in the country. The other basis is the 'Nationality principle', which means offenses committed by citizens where the nationality has to be proved irrespective of the place of occurrence. The legislature should be competent and express its intention to define jurisdiction. The author discussed the basis of liability of Australia, Canada, UK and the US.

2) Adjudicative jurisdiction, the question if the particular court has adjudicative jurisdiction on specific class of offences. Supreme court of Canada in one of its judgment in extraterritorial cases gave a verdict that the test of 'Real and substantial link' should be established between the offence and the country in which it is committed. American courts say that an offense cannot have two loci and the origin of the crime should determine the jurisdiction. In Australia and in the US the courts derive their jurisdictional authority from the 'interstate trade and commerce'. Cybercrimes are committed mostly on the internet and it is the dominant source of interstate trade and commerce. Further due to extensive enhancement of telecommunication networks in cybercrimes the jurisdiction has also extended proportionately. In cases of conflicting, jurisdictional claims the test of 'reasonableness' should be applied. The sovereign interests of individual nations ought to be protected and more appropriately, each nations should obtain consent, consult and discuss for the sake of international comity and mutual respect for each other. Cybercrime is predominantly an online activity where multiple jurisdictions overlap with each other and correlation between the factors of crime is difficult to establish. Other factors needs to be considered when the resolution of jurisdictional conflicts seems difficult, like location of the offence and the offender, the nationality of the offender and the victim, degree and the graveness of the crime, the location of the evidence and the quantum of punishment.

3) Enforcement jurisdiction, the jurisdiction who has the control and custody of the offender is generally the one who practically exercises jurisdiction over the crime. The location of the crime, data or device would determine jurisdiction. The cybercrime convention recognizes extradition for the purpose of prosecution. Extradition treaties require conformity to bilateral agreements and international obligation between both the Countries. The author did not address the issues of cross border investigation, data interception, use of intelligence services in respective countries. There has to be an existence of 'dual criminality' where the cyber offence committed should be illegal in both the countries. To make enforcement actions easier across jurisdictions it is essential that offences are declared extraditable by both the countries to make them punishable.

Finally, on page 473-505 the author concludes the book with a detailed bibliography, of the relevant references and court cases appropriate to the subject of cybercrime. Further, the book is supplemented with a list of index and reference number of pages for words used in the text.

The author is of the opinion that much of the research on the area of cyber-crime has been more on the criminological side rather than the doctrinal analysis. The writing of this book is a work towards that direction. The book is primarily for academics, legal advisors, law enforcement agencies and the student fraternity. It covers the major common law jurisdictions of US, UK, Canada and Australia because they share a common law heritage, they have dealt extensively with cyber-crime and all are signatory to the European convention on cyber-crime. The book does not cover information technology (IT) security, investigation and procedural matters but contains a comparative review of

relevant case laws. The author mentioned in details the overall structure of the book and the categorization of each cyber offences with respect to the respective jurisdiction law. The author further acknowledges the support received from his network of academicians, close acquaintances for their assistance with the publication of this book. Necessary abbreviations been cited with a geographical listing and table of all cases and legislation's.

References

Judgements of the Supreme Court of Canada. Retrieved from https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1837/index.do

O'Connell, R. (2003). Cyberspace Research Unit University of Central Lancashire: A Typology of Child Cybersexploitation and Online Grooming Practices. Retrieved from http://image.guardian.co.uk/sys-files/Society/documents/2003/07/17/Groomingreport.pdf