Preface

ABOUT THE SUBJECT

In the digital age, ICT raises new concerns that are not accounted for within the existing data protection/privacy legal framework, so some action is necessary to ensure that individual rights are protected. After providing an overview of ICT as a new development that creates opportunities but also risks, this book discusses the need to integrate, at a practical level, data protection, privacy, and security from the very inception of new information and communication technologies.

Digital crime is prevailing in all sectors of activity in our dynamic world and assuming a threatening dimension to people, society, and organizations. The combat to this form of crime is increasing awareness towards fast developments in the area of computer science forensics, investigation methods, technologies, and tools, and appealing to the global information security and assurance and ICT Law fields and its applications.

ORGANIZATION OF THE BOOK

This handbook of research collects the most recent discoveries in cyber-crimes approaches, developments, practical examples, and case studies, together with the counterpart of cyberspace security developments, personal and global privacy, information assurance, protection, and ICT Law in all the embraced dimensions. The book is intended to support a professional audience of investigators, practitioners of computer forensics, security, experts in ICT law, and also an academic audience (teachers, researchers, and students, mainly of post-graduate studies).

This collection of 32 chapters is written by a group of 62 authors that includes many internationally renowned and experienced authors in the field and a set of younger authors, showing a promising potential for research and development. At the same time, the book integrates contributions from academe, research institutions, and industry, representing a good and comprehensive representation of the state-of-the-art approaches and developments that address several dimensions of this fast evolutionary thematic.

A very important and enriching characteristic of this handbook of research is that it includes contributions from the five continents. Contributions came from Australia, Belgium, Brazil, France, Greece, India, Ireland, Israel, New Zealand, Nigeria, Poland, Portugal, Romania, Serbia, Spain, Taiwan, the United Kingdom, and the USA.

The Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance integrates 32 chapters organized in four sections, which are briefly introduced below.

With 10 chapters, Section 1, “Cybercrimes Examples, Risks, and Threats” presents a compilation of examples and reviews of digital crime, threats, risks, techniques, and challenges.
We are facing the expansion of cyber incidents, and they are becoming more severe. This results in the necessity to improve security, especially in the vulnerable field of critical infrastructure. One of the problems in the security of critical infrastructures is the level of awareness related to the effect of cyberattacks. The threat to critical infrastructure is real, so it is necessary to be aware of it and anticipate, predict, and prepare against a cyber attack. The main reason for the escalation of cyberattacks in the field of Critical Infrastructure (CI) may be that most control systems used for CI do not utilise propriety protocols and software anymore; they instead utilise standard solutions. As a result, critical infrastructure systems are more than ever before becoming vulnerable and exposed to cyber threats. It is important to get an insight into what attack types occur, as this may help direct cyber security efforts. In the 1st chapter, “Cyber Attacks on Critical Infrastructure: Review and Challenges,” Kovacevic and Nikolic defend that the threat to critical infrastructure is real, so it is necessary to be aware of it, and anticipate, predict, and be prepared against a cyber-attacks.

The shift towards cyberspace created a very wide range of opportunities for various criminal activities, in both the real and the virtual world, such as identity theft, fraud, organized crime, and seriously organized crime, on an unprecedented scale. In “Raptor: Early Recognition and Elimination of Network Attacks,” Grzonkowski, Vasiliu, and Koumpis propose a combination of integration activities for the best tools that help identify threats and security gaps for business and industrial users, for new analytical tools proposed to check if existing security features of the used networked structures are adequate and up-to-date and up-to-speed to address potential threat scenarios.

The Internet imprints a great complexity to new and old risks as threats become more available in children’s lives. Criminals have greater access to the victims and Internet crimes are favoured by ambiguities in the law. The 3rd chapter, “Online Violence: Listening to Children’s Online Experiences,” by Castro and Osório, presents preliminary data from an on-going doctoral investigation about the upsetting phenomenon of violence perpetrated by, with, and among school-aged children using online services and devices. To better understand the subjectivity, delicacy, and complexity of matters and meanings that participants bring to their online experiences, the authors follow a qualitative approach, based on a structured and interpretive analysis. With this chapter, the authors intend to contribute to a greater understanding and reflection about this complex problem and its impact in order to increase awareness about how children behave online and in what way it may influence their well-being.

As mobile applications are being developed at a faster pace, the security aspect of user information is being neglected. A compromised smartphone can inflict severe damage to both users and the cellular service provider. Malware on a smartphone can make the phone partially or fully unusable, cause unwanted billing, steal private information, or infect every name in a user’s phonebook. A solid understanding of the characteristics of malware is the beginning step to prevent much of the unwanted consequences. The 4th chapter, “Development and Mitigation of Android Malware,” an overview of security threats posed by Android malware. In particular, the authors focus on the characteristics commonly found in malware applications and understand the code level features that allow us to detect the malicious signatures. The authors also discuss some common defense techniques to mitigate the impact of malware applications.

In “Answering the New Realities of Stalking,” Avelina Escamilla presents the study of a new way of harassment named stalking. After the study of its contents through the opinions of the most recognized specialist on it, the chapter defines the crime based on the expert’s opinion. A study of comparative law is done, and this study focuses on the different ways stalking happens. This chapter offers a critical study of the inclusion of stalking as a felony in the criminal amendment Organic Criminal Law 10/1995 of 23 November, Criminal Law Code. To finish, this chapter proposes some improvements to that regulation and focuses on the new realities that bring about cyber stalking.
In the 21st century, thus far, we have seen a growing dependence on and usage of the Internet and communications technology. This has been especially true for youth who spend much of their time communicating in cyber space. This allows for developing and maintaining relationships. At the same time, an ugly and dangerous phenomenon called cyber bullying has reared its head. In this 6th chapter, “Cyberbullying: Keeping our Children Safe in the 21st Century,” Iris and Sukenik discuss various aspects of this phenomenon, including, but not limited to, incidence rates, comparison to traditional bullying, risk factors for being involved either as a bully or a victim, how it affects its victims, relevant legal aspects, and most importantly, how to defend against it. The discussion of coping strategies is especially detailed and provide suggestions for schools, parents, bystanders, victims, and broader society.

“DNA Databases for Criminal Investigation,” by Henrique Curado, presents the establishment of DNA databases and their relevance at two levels. On the one hand, as a basis for criminal investigation, they contribute to the protection of the public against potentially criminal behavior. In our societies, mass violence is not a sporadic occurrence and knowledge. When DNA databases allow for preventive action, they may be synonymous with safety. On the other hand, DNA databases pose deeper problems, such as a felon’s data are still personal data and as such need to be protected. Any violation of this right is against the law. Therefore, a society that wants to be lawfully protected must first protect. The study is focused on Spanish and Portuguese statutes enforced in 2007 and 2008, respectively, as well as on doctrine and jurisprudence produced in both countries and intended to strengthen cyberspace security and to guarantee access to information.

Given the multifaceted problems and complexities of information security, the manner in which top management teams make investment and management decisions regarding security technologies, policy initiatives, and employee education could have a significant impact on the likelihood of information security breaches in organizations. In the context of information security management, it is not clear from management literature regarding how the characteristics of the top management team are associated with the possibility of information security breaches. In the 8th chapter, “Composition of the Top Management Team and Information Security Breaches,” Hsu and Wang demonstrate that the average length and heterogeneity of tenure could increase the possibility of breaches. However, age heterogeneity and the size of the top management team are negatively related to such a possibility. In addition, the findings suggest a nonlinear association between average age and tenure and the possibility of security breaches. The authors conclude the chapter with theoretical and practical implications on the organizational and managerial aspects of information security management.

Clickjacking attacks are an emerging threat on the Web. The attacks allure users to click on objects transparently placed in malicious Web pages. The resultant actions of the click operations may cause unwanted operations in the legitimate websites without the knowledge of users. Recent reports suggest that victims can be tricked to click on a wide range of websites such as social network (Facebook, Twitter), shopping (Amazon), and online banking. One reported incident on clickjacking attack enabled the webcam and microphone of a victim without his/her knowledge. To combat against clickjacking attacks, application developers need to understand how clickjacking attacks occur along with existing solutions available to defend the attacks. In Chapter 9, “Hijacking of Clicks: Attacks and Mitigation Techniques,” Shahriar and Devendran show a number of detection techniques available at the client, server, and proxy levels.

The use of Internet by organized crime groups to commit their crimes is increasing and sometimes there is no other effective way to fight it other than by exploring the Internet, as discussed by Valls-Prieto in Chapter 10, “Fighting Cybercrime and Protecting Privacy: DDoS, Spy Software, and Online Attacks.” The use of an environmental scanner to fight cybercrime—as an organized crime—is the project for
using this technique of large-scale databases to try to guarantee the security against the risk of new, developing forms of criminal activities. On the other hand, the use of large-scale databases utilizes a great amount of personal data to try to predict where and how organized crime or new forms of criminality will develop. This means that we have to evaluate the interests of security of society and the privacy of the person, and we have to find the way to balance both in a democratic society. As these tools are not limited to one national state, but affect the whole world, the author discusses the European regulation on the use of large-scale databases and the limits needed to protect privacy rights. On 31 July 2013, in reaction to the use of these instruments by NSA, a group of institutions linked to privacy on the Internet created a project with the rights that should be guaranteed when processing this type of investigation as a way of controlling their use by the state. There are important ethical issues to be considered in the employment of this new and unregulated instrument; the third part of the chapter deals with the multiple possibilities of massive data.

Section 2, “Cyber Security Approaches and Developments,” presents a collection of 12 chapters addressing the latest techniques, technologies, and contributions to prevent digital crime and its associated consequences.

Workflow management systems are used to run day-to-day applications in numerous domains, often including exchange and processing of sensitive data. Their native “leakage-proneness,” being the consequence of their distributed and collaborative nature, calls for sophisticated mechanisms able to guarantee proper enforcement of the necessary privacy protection measures. Motivated by the principles of Privacy by Design and its potential for workflow environments, in “Privacy Compliance Requirements in Workflow Environments,” Koukovini et al. investigate the associated issues, challenges, and requirements. With the legal and regulatory provisions regarding privacy in information systems as a baseline, the chapter elaborates on the challenges and derived requirements in the context of workflow environments, taking into account the particular needs and implications of the latter. Further, it highlights important aspects that need to be considered regarding, on the one hand, the incorporation of privacy-enhancing features in the workflow models themselves and, on the other, the evaluation of the latter against privacy provisions.

In a bid to discover, uncover, and stamp out digital crime while ensuring information security and assurance, there is a need to investigate the crime once it has taken place. This will help trace the criminals and also secure an organization against future attacks. Forensic readiness entails that an organization be at alert in terms of digital evidence collection and storage – that is, collecting and storing such evidence constantly in a forensically sound manner, not just when the need for such evidence arises. In the event litigation arises or is anticipated, digital evidence may need to be reviewed by the opposing parties prior to court proceedings to assess quality of the evidence; this is eDiscovery. Digital evidence for eDiscovery needs to be forensically sound and provided in a timely and efficient manner, and forensic readiness helps to ensure this. In “Forensic Readiness and eDiscovery,” Sauda Sule seeks to establish how forensic readiness is relevant to the eDiscovery process.

The Internet has become an essential service to depend on for many industries, such as news agencies, airports, and even utility companies. This was the beginning of a new-trillion-dollar industry: the Internet industry. However, the Internet was designed to be an open, academic tool, never to be secure. As a result, cybercrimes, cyber warfare, and other cyber illegal activities have spread to become a significant portion of Internet traffic. Cybercrimes often challenge law enforcement. It is difficult to know the exact location where an attack originated, and there are no cyber borders between nations. As a result, fighting cybercrimes requires international cooperation. The purpose of this chapter, “Cybercrimes Technologies and Approaches,” is to shed some light on motives of cybercrimes, technologies used by hackers, and
solutions that can be adopted by individuals, organizations, and governments. This chapter also presents
the United States (USA) and international perspectives on cybercrimes and privacy laws. In summary,
individuals, organizations, and nations have roles to play in achieving security and reducing cyber risks.

At young ages there is an increase in reports of intimidation, harassment, intrusion, fear, and violence
experienced through Information Technologies (IT). Hacking, spamming, identity theft, child pornography,
cyber bullying, and cyber stalking are just few examples of cyber-crimes. Chapter 14, “Cyber-Crimes
against Adolescents: Bridges between a Psychological and a Design Approach,” by Pereira, Matos, and
Sampaio, aims to contribute, from a psychological and design perspective, to an integrative viewpoint
about this complex field of cyber-crime. The most common types of cyber-crimes, epidemiological
data, and the profiles of cyber victims and aggressors’ are approached. The studies that identify the
factors contributing to IT misuse and to growing online vulnerability, principally in adolescents, are
discussed. Likewise, the central explanatory theories for the online victimization and the risk factors for
victimization and perpetration online are addressed. Finally, some cyber-crime prevention strategies are
anticipated, in particular among young people, seeking to provide clues to the consolidation of recent
policies, namely at the digital design level.

Event reconstruction is one of the most important steps in digital forensic investigations. It allows
investigators to have a clear view of the events that have occurred over a time period. Event reconstruc
tion is a complex task that requires exploration of a large amount of events due to the pervasiveness of
new technologies. Any evidence produced at the end of the investigative process must also meet the
requirements of the courts, such as reproducibility, verifiability, validation, etc. After defining the most
important concepts of event reconstruction, Chabot, Bertaux, Kechadi, and Nicolle present a survey of
the challenges of this field and solutions proposed so far, in their chapter, “Event Reconstruction: A
State of the Art.”

We are now in an era of cyberconflict, where nation states, in addition to private entities and individual
actors, are attacking each other through Internet-based mechanisms. This incorporates cyberespionage,
cybercrime, and malware attacks, with the end goal being intellectual property, state secrets, identity
information, and monetary gain. Methods of deterring cybercrime ultimately require effective attribution;
otherwise, the threat of consequences for malicious online behaviour will be diminished. The 16th chapter,
“Indirect Attribution in Cyberspace,” by Layton and Watters, reviews the state of the art in attribution
in cyberspace, arguing that due to increases in the technical capability of the most recent advances in
cyberconflict, models of attribution using network traceback and explicit identifiers (i.e. direct models)
are insufficient build trustworthy models. The main cause of this is the ability of adversaries to obfus
cate information and anonymise their attacks from direct attribution. Indirect models, in which models
of attacks are built based on feature types and not explicit features, are more difficult to obfuscate and
can lead to more reliable methods. There are some issues to overcome with indirect models, such as the
complexity of models and the variations in effectiveness, which present an interesting and active field
of research.

The performance of Next Generation Networks (NGN) in terms of security, speed, synchronization,
latency, and throughput with variable synchronous or asynchronous packet sizes has not been sufficiently
addressed in novel crypto systems. Traditional crypto systems such as block and stream ciphers have
been studied and implemented for various networks such as wire line and wireless systems. Since NGN
comprises of wire line and wireless networks with variable packet-based communication carrying various
traffic like multimedia, video, audio, multi conferencing, and a large amount of data transfers at higher
speeds, the modern crypto systems suffer with various challenges such as algorithm implementation,
variable packet sizes, communication, latency, throughput, key size, key management, and speed. In
“Modern Crypto Systems in Next Generation Networks: Issues and Challenges,” Biradar and Nayaka discuss some of the important issues and challenges faced by modern crypto systems in Next Generation Networks (NGN) such as algorithm implementation, speed, throughput and latency in communication, point-to-multipoint, broadcast and key size, remote key management, and communication speed.

The Internet has become an inevitable form of communication, which enables connections with colleagues, friends, or people with similar interests, regardless of physical barriers. However, there is also a dark side to the Internet, since an alarming number of adolescents admit they have been victims or bystanders of cyberbullying. In order to make the Internet a safer environment, it is necessary to develop novel methods and software capable of preventing and managing cyberbullying. In Chapter 18, “Automatic Detection of Cyberbullying to make Internet a Safer Environment,” Kovacevic and Nikolic review existing research in dealing with this phenomenon and discusses current and potential applications of text mining techniques for the detection of cyberbullying.

Browser attacks over the years have stormed the Internet world with so many malicious activities. They provide unauthorized access and damage or disrupt user information within or outside the browser. This chapter focuses on the complete attack actions adopted by an attacker while crafting an attack on Web browser. The knowledge gained from the attacker’s actions can be framed into a suitable taxonomy, which can then be used as a framework for examining the browser attack footprints, vulnerability in browser design, and helps one to understand the characteristics and nature of an attacker. Saini, Gaur, and Laxmi present “A Taxonomy of Browser Attacks” that helps in combating new browser attacks, and improving browser security.

This chapter addresses some concerns and highlights some of the major problems affecting cyberspace. In “Defending Information Networks in Cyberspace: Some Notes on Security Needs,” Alberto Carneiro focuses on defensive attitudes and concerns pertaining to the cybersecurity issues. Section 1, “Facing Cyberspace Security,” opens the area of threats and the need of defensive attitudes. Section 2, “Remembering Internet Issues,” deals with known Internet problems in what concerns cybersecurity as a generic term. In –Section 3, “Defensive Cybersecurity,” the focus is on the need to add more defensive features to security policies. Section 4, “In Search of Better Solutions,” emphasizes the need to invest continuously in scientific research and the creation of more sophisticated processes in order to prevent new forms of attack and mitigate negative results.

Chapter 21, “Network Situational Awareness: Sonification and Visualization in the Cyber Battlespace,” by Fairfax, Laing, and Vickers, treats computer networks as a cyber warfighting domain in which the maintenance of situational awareness is impaired by increasing traffic volumes and the lack of immediate sensory perception. Sonification (the use of non-speech audio for communicating information) is proposed as a viable means of monitoring a network in real time and a research agenda employing the sonification of a network’s self-organized criticality within a context-aware affective computing scenario is given. The chapter views a computer network as a cyber battlespace with a particular operations spectrum and dynamics. Increasing network traffic volumes are interfering with the ability to present real-time intelligence about a network and so suggestions are made for how the context of a network might be used to help construct intelligent information infrastructures. Such a system would use affective computing principles to sonify emergent properties (such as self-organized criticality) of network traffic and behaviour to provide effective real-time situational awareness.

The research presented by Raisinghani and Jarret in “Can Total Quality Management Exist in Cyber Security: Is it Present? Are we Safe?” examines the threats in cyber security. It identifies the risk of cyber attacks and argues the inability to defend against those threats in a cyber security program. The introduction provides a brief history of cyber security and how the information highway arrived at this
point in cyber security. The first analysis examines the threats in cyber security in personal, private, and government computer systems. The second analysis examines the approaches to attacking those systems. The third analysis examines threats against private companies and government agencies. The final analysis examines major threats to cyber security.

Section 3, “Legal Aspects and ICT Law,” discusses several aspects of cyberspace regulation and cybercrime combat.

Cyberspace, like the territories grounded in the physical world, is an environment subject to border control and surveillance for various purposes: governmental, economic, security, among others. As in the physical sphere, governance can serve to enforce rules to avoid abuses and to allow users and institutions to build effective relationships, transparent and harmonious. The purpose of Chapter 23, “The Gatekeepers of Cyberspace: Surveillance, Control, and Internet Regulation in Brazil,” by Elisianne Soares, is to discuss the Civil Rights Framework for the Internet in Brazil (“Marco Civil da Internet”), a project created in 2009 that aims to establish rights and obligations for the operation of the network in this Latin American nation.

Chapter 24, “Surveillance, Privacy, and Due Diligence in Cybersecurity: An International Law Perspective,” by Joanna Kulesza, covers the international law due diligence principle as applied to the prevention of transboundary cyberthreats. The analysis is based on the work of the International Law Commission referring to state responsibility and international liability as applicable to the challenge of international cybersecurity. The first attempts of this application done by European international organizations are discussed. This is done in the light of the current political challenge of engaging all states in the discussion on the appropriate standard of cyberthreats prevention. Reaching to the no harm principle of international law, the author argues that all states need to take all necessary measures in order to prevent significant transboundary damage originated by online activities of individuals within their jurisdiction, power, or control. Should they fail to show due diligence they may be held internationally responsible for an omission contrary to their obligation of preventing harm to other states, foreigners, or shared resources.

Since the government began tackling the problems of cybercrime, many laws have been enacted. A lack of a comprehensive definition and taxonomy of cybercrime makes it difficult to accurately identify report and monitor cybercrime trends. There is not just a lack of international agreement on what cybercrime is; there are different laws in every state within the United States, reflecting the inconsistency of dealing with cybercrime. There is also concern that many times lawyers and information technology professions are unable to understand each other well. The deficiency of cyber laws is an obvious problem and development of effective laws is emerging as an important issue to deal with cybercrime. The research presented by Glasser and Taneja in “A Routine Activity Theory-Based Framework for Combating Cybercrime” uses the routine activity theory to develop a unified framework by including the motivation of the offender to use a computer as a tool/target, suitability of the target, and the presence (or absence) of guardian. It could help states that want to update their existing laws and cover areas that were previously uncovered.

The Internet of Things (IoT), a metaphor for smart, functional Cyberphysical Environments (CPE), is finding some usefulness in various sectors including healthcare, security, transportation, and the Smart Home (SH). Within the IoT, objects potentially operate autonomously to provide specified services and complete assigned tasks. However, the introduction of new technologies and/or the novel application of existing ones usually herald the discovery of unfamiliar security vulnerabilities, which lead to exploits and sometimes to security breaches. There is existing research that identifies IoT-related security concerns and breaches. Edewede Oriwoh discusses existing Digital Forensics (DF) models and methodologies for
their applicability (or not) within the IoT domain using the SH as a case in point, in his chapter, “Internet of Things: The Argument for Smart Forensics.” The chapter also makes the argument for smart forensics, the use of a smart autonomous system (tagged the Forensics Edge Management System [FEMS]) to provide forensic services within the self-managed CPE of the SH.

“Sticks and Stones” is a well-known adage that means that whatever nasty things people say, they will not physically harm one. This is not often the case, as bullying, especially via the Internet, can be quite harmful. There are few anti-bullying laws emanating from the European Union, which is a trading block of 28 member states that have pooled their sovereignty in order to have common laws and practices to boost trade and peace. However, the common legal rules that exist in the EU have implications for those who run websites, including relating to cyber-bullying. These people, known as systems operators, or sysops, can be limited in the powers they have and rules they make through “sysop prerogative.” Sysop prerogative means that a systems operator can do anything which has been permitted or not taken away by statute, or which they have not given away by contract. Chapter 28, “Sticks and Stones will break my Euros: The Role of EU Law in Dealing with Cyber-Bullying through Sysop-Prerogative,” by Jonathan Bishop, reviews how the different legal systems in Europe impact on sysops and change the way in which sysop prerogative can be exercised. This includes not just from the EU legal structure, but equally the European Convention on Human Rights (ECHR), which also has implications for sysops in the way they conduct their activities.

In “Trolling is not just an Art. It is a Science: The Role of Automated Affective Content Screening in Regulating Digital Media and Reducing Risk Trauma,” Jonathan Bishop seeks to explore the role media content ratings play in the age of “Internet trolling” and other electronic media issues like “sexting.” Using ANOVA to validate a four-factor approach to media ratings based on maturity, the chapter finds the ability of a person to withstand various media content, measured in “knol,” which is the brain’s capacity to process information, can be used to calculate media ratings. The study concludes it is feasible to have brain-computer interfaces for PCs and kiosks to test the maturity of vulnerable persons and recommend to parents/guardians or cinema managers whether or not to allow someone access to the content they wish to consume. This could mean that computer software could be programmed to automatically censor content that person is likely to be distressed or grossly offended by. Public policy issues relating to these supply-side interventions are discussed.

The last section of this handbook of research, Section 4, “Case Studies,” offers four analysis and discussions on threats and attempts to privacy, security, and integrity.

The 29th chapter, “Honeypots and Honeynets: Analysis and Case Study,” by Marin, Naranjo, and Casado, presents a review and a case of study of honeypots and honeynets. First, some of the most important and widely used honeypots in the current market are selected for comparative analysis, evaluating their interaction capacity with an attacker. Second, a self-contained honeynet architecture is implemented with virtual machines. An intrusion test is performed against the honeynet to observe the quality and quantity of the information collected during the attack. The final goal of this analysis is to assess the capacity of monitoring and threat detection of the honeynets and honeypots.

The main objective of the study presented in Chapter 30, “Analysis of the Cybercrime with Spatial Econometrics in the European Union Countries,” by Vítor Martinho is to analyze the crimes related to the new information technologies in the European Union using the data provided by the European Commission and the spatial econometrics approaches. The data were analyzed with several tests, namely the Moran’s I, to verify the existence of global (for all countries of the European Union) and local spatial autocorrelation. The presence of spatial autocorrelation in the data means that the variable analyzed in a determined country is auto correlated with the same variable in the neighboring countries. The data
analysis was complemented with some cross-section estimations, considering namely the Lagrange Multiplier tests, to examine the spatial lag and the spatial error autocorrelation. The spatial autocorrelation is a statistical infraction, so the consideration of these subjects prevents result bias and on the other hand allows some conclusions important to help in the definition of adjusted policies.

Cyber Security Model of Artificial Social System Man-Machine takes advantage of an important chapter of artificial intelligence, discrete event systems applied for modelling and simulation of control, logistic supply, chart positioning, and optimum trajectory planning of artificial social systems. Despite conventional approaches, Cyber Security Model of Artificial Social System Man-Machine is not guided by rigid control algorithms but by flexible, event-adaptable ones that makes them more lively and available. All these allow a new design of artificial social systems dotted with intelligence, autonomous decision-making capabilities, and self-diagnosing properties. Heuristics techniques, data mining planning activities, scheduling algorithms, automatic data identification, processing, and control represent as many trumps for these new systems analyzing formalism. In “Cyber Security Model of Artificial Social System Man Machine,” Calin Ciufudean challenges these frameworks to model and simulate the interaction of man-machine in order to have a better look at the human, social, and organizational privacy and information protection.

The last chapter, “Information Disclosure on Social Networking Sites: An Exploratory Survey of Factors Impacting User Behaviour on Facebook,” by Doherty, Lang, Deane, and Connor, explores how six constructs—control, trust, perceived risk, risk propensity, perceived legal protection, and privacy disposition—affect information disclosure on the Social Networking Site (SNS) Facebook. Building upon previous related work, an extended causal model of disclosure behaviour is proposed. The hypothesised relationships in this model were tested using survey data collected from 278 social networking site users in Ireland. The results of the analysis provide strong support for the proposed model.

EXPECTATIONS

The book provides researchers, scholars, and professionals with some of the most advanced research, developments, discussions, and case studies on digital crime and digital threats from one side, and security, privacy, information assurance, law and regulation, and human aspects on the other. It was compiled and edited to be a tool for academics (teachers, researchers, and students of several graduate and postgraduate courses), professionals of law, information technology, psychology, and policymakers.

We strongly hope it meets your expectations!

Maria Manuela Cruz-Cunha
Polytechnic Institute of Câvado and Ave, Portugal

Irene Maria Portela
Polytechnic Institute of Câvado and Ave, Portugal