Preface

This book explores multiple aspects of cyber terrorism and cyber crime in today's society. This book provides insights on the negatives uses of technology with comprehensive review of the associated vulnerabilities and mitigations. In the recent events of cyber warfare most notable are the Flame computer virus, expansion of the National Security Agency (NSA) monitoring programs, and suspected attack on Sony for a movie poking fun at North Korea. As governments scramble for cyber security resources whether technological or people it evident that cyber security is the new war being fought.

Our intention in editing this book was to provide new concepts and techniques that are deployed in secure computing, mobile computing, training, and laws. This book is to provide frontier research to include cases that are applicable to modern events. Since the book covers case study-based research findings, it can be quite relevant researchers, university academics, secure computing professionals, and probing university students. In addition, it will help those researchers who have interest in this field to keep insight into different concepts and their importance for applications in real life. This has been done to make the edited book more flexible and to stimulate further interest in topics.

This book is comprised of three sections.

1. Security in Mobile Computing
2. Cyber Security Techniques and Cases
3. Leadership, Communication, and Education in Cyber Security.

ORGANIZATION OF THIS BOOK

In this book, we present 16 chapters aimed at emphasizing threat and countermeasures that are applicable in today's society. For coherency, we have ordered the chapters in terms of similarity of topic. The topic covered range from threats in mobile devices to developing leaders in cyber security.

Chapter 1, "A Brief Review of New Threats and Countermeasures in Digital Crime and Cyber Terrorism", presents the some of the concepts contained within the book. Further discussed are emerging laws, policies, processes, and tools that are changing the landscape of cyber security. This chapter provides an overview of the research to follow which will provide an in depth review of mobile security, mobile networks, insider threats, and various special topics in cyber security.

Chapter 2, " Mobile Devices: The Case for Cyber Security Hardened Systems", discusses how mobile devices are the preferred device for web browsing, emailing, using social media and making purchases. Due to their size, mobile devices are easily carried in people's pockets, purses or briefcases. Unfortunately, the popularity of mobile devices is a breeding ground for cyber attackers. Operating systems on mobile devices do not contain security software to protect data.

Chapter 3, " Security Threats on Mobile Devices", contains basic introduction into security models of modern operating system like Android, iOS or Windows Phone. There are described the methods of attacks to the mobile devices. Such attacks consist of application based threats and vulnerabilities, network based attacks and internet browser vulnerabilities. Another section in this chapters contains a description of defensive strategies and steps for securing the device. There is also section about securing mobile device for enterprise environment.

Chapter 4, "The Human Factors in Mobile Phishing", presents the use of electronic media, like emails and mobile text messages, to fraudulently elicit private information or obtain money under false pretence.

Chapter 5, " Security Issues in Mobile Wireless Ad Hoc Networks: A Comparative Survey of Methods and Techniques to Provide Security in Wireless Ad Networks", investigates and exposes methods and techniques developed to provide security in wireless ad hoc networks. are investigated and effectiveness and efficiency of these mechanisms are exposed.

Chapter 6, "Legal Issues: Security and Privacy with Mobile Devices", raises the issues of privacy and security being woven into the fabric of American law concerning mobile devices. It is essential to fully understand associated laws and policies to ensure proper execution while upholding the law. As the American society significantly uses mobile devices it is imperative to understand the legal actions surrounding these technologies to include their associated uses. With 9/11 in the not so distant past, cyber security has become a forefront subject in the battle against global terrorism. Mobile devices are not like the devices of the past as the computing power is on par with that of some desktops to include these devices have the ability to execute malicious applications.

Chapter 7, "Survey in Smartphone Malware Analysis Techniques", surveys various approaches used in Mobile malware detection and Investigates weaknesses of existing countermeasures such as signature-based and anomaly-based detection.

Chapter 8, "Trust Management in Mobile Ad hoc Networks for QoS Enhancing", is the proposition of a trust based environment for MANET and securing it against collusion attack in order to enhance the network QoS. This is achieved using three steps: (1) the definition of a formal trust based environment (2) the addition of a process handling collusion attack and (3) the extension of the whole proposition by a delegation process allowing nodes functionalities sharing.

Chapter 9, "Insider Threats: Detecting and Controlling Malicious Insiders", presents how malicious insiders are posing unique security challenges to organizations due to their knowledge, capabilities, and authorized access to information systems. This chapter investigates the scale and scope of malicious insider risks and explore the impact of such threats on business operations.

Chapter 10, "Authorship Analysis: Techniques and Challenges", discussed the process of examining documents to determine the stylistic details underlying the document and hence inferring about the characteristics of the author of document in order to attribute the authorship to a particular author or to confirm the authenticity of a claimed authorship. The authors discuss the existing methods that have been used so far to deal with automation of authorship analysis and the challenges faced by them

Chapter 11, "The Need for a Dualist Application of Public and Private Law in Great Britain Following the Use of "Flame Trolling" During the 2011 UK Riots: A Review and Model", recommends further research to establish whether it should be the case that in a society based on dualism that criminal and civil cases should be held at the same time, and that in both instances those being accused of an offence or tort should be allowed to bring a counter-claim. It is discussed that in such a system the cases that would be brought are where there is a clear victim who had no part in the offence against them, such as murder, rape, theft and burglary, which are usually carefully planned and orchestrated acts.

Chapter 12, "Native Language Identification (NLID) for Forensic Authorship Analysis of Weblogs", presents introduces NLID and considers the casework applications with regard to authorship analysis of online material. It presents findings from research identifying which linguistic features were the best indicators of native (L1) Persian speakers blogging in English, and analyses how these features cope at distinguishing between native influences from languages that are linguistically and culturally related.

Chapter 13, "Leadership Approaches for Managing Healthcare Information Security Millennial Employees: Health Information Security Leadership Approaches", presents

Chapter 14 "Learning Management Systems: Understand and Secure Your Educational Technology" presents background data concerning breaches and the lack of associated talent to support these cyber attacks. This chapters explores how to achieve this among millennial employees.

Chapter 15, "The Innovation and Promise of STEM Oriented Cyber Security Charter Schools in Urban Minority Communities: Cyber Terrorism Workforce Development", provides insight on how the US pipeline of minority students studying STEM falls short in producing the next generation of cybersecurity professionals.

Chapter 16, "Communication, Technology & Cyber Crime in Sub-Saharan African", discusses mobile and internet technologies currently being utilized in Sub-Saharan Africa as well as some of the major cybersecurity concerns threatening networks in the region that are associated with the new economic growth on the African continent. This is important as this region is rapidly developing its technology base. Sub-Saharan Africa is experiencing many of the issues associated with the benefits of cyber technology as well as its many negative sides.

Maurice Dawson
University of Missouri – St. Louis, USA

Marwan Omar
Nawroz University, Iraq