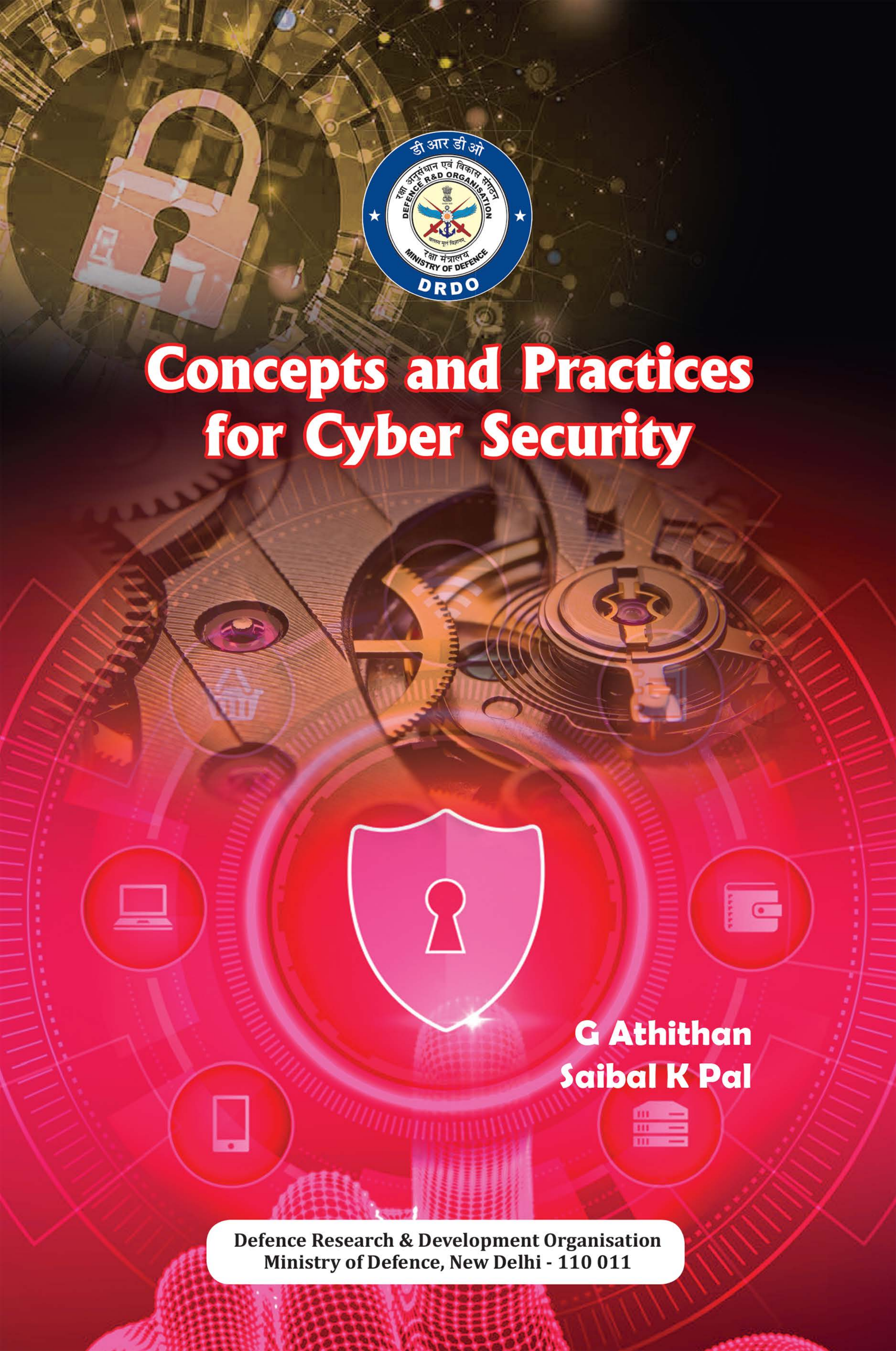

Concepts and Practices for Cyber Security

G Athithan
Saibal K Pal

Defence Research & Development Organisation
Ministry of Defence, New Delhi - 110 011

Concepts and Practices for Cyber Security

Concepts and Practices for Cyber Security

Dr G Athithan
Former Distinguished Scientist & Director General, DRDO

Dr Saibal K Pal
Scientist G
Scientific Analysis Group, Delhi

Defence Research and Development Organisation
Ministry of Defence, New Delhi – 110 011
2022

DRDO MONOGRAPHS/SPECIAL PUBLICATIONS SERIES

CONCEPTS AND PRACTICES FOR CYBER SECURITY

Dr G Athithan and Dr Saibal K Pal

Cataloguing-in-Publication

Athithan, G and Pal, Saibal K

Concepts and Practices for Cyber Security

DRDO Monographs/Special Publications Series
1. Cyber Security 2. Cryptography 3. Cybernetics
I. Title II. Series
004.056.54

ISBN 987-93-94166-07-3

The views expressed in the book are those of the authors only. The Editors or the Publisher do not assume responsibility for the statements/opinions expressed by the authors.

Cover Design	*Printing*	*Marketing*
Rajesh Kumar	SK Gupta	Tapesh Sinha

Published by Director, DESIDOC, Metcalfe House, Delhi – 110 054.

Contents

Foreword *ix*

Preface *xi*

CHAPTER 1: INTRODUCTION **1**

1.1 Data, Information and Knowledge 3

1.2 Information Processing 13

1.3 Cyberspace 27

1.4 Cyber Security 37

CHAPTER 2: CONCEPTS OF INFORMATION PROCESSING **43**

2.1 Basic Models of Information Processing 44

2.2 Synthesis of a Practical Model 59

2.3 Nature of Processing Functions 62

2.4 Validation of Input 66

2.5 Unintended Output 69

2.6 Communication Links and Paths 71

2.7 Information Processing Networks 79

CHAPTER 3: THE CYBER THREAT LANDSCAPE **85**

3.1 Motives of Cyber-Attacks 86

3.2 The Domain of Targets 88

3.3 Threats 91

3.4 Vulnerabilities 98

3.5 Attack Scenarios 101

3.6 Attack Envelope 105

3.7 An Integrated Picture 107

CHAPTER 4: CYBER SECURITY POLICY FRAMEWORK 109
4.1 Guiding Principles 111
4.2 Security Policies 122
4.3 System Requirements 128
4.4 Best Practices 129

CHAPTER 5: CRYPTOGRAPHY FOR CYBER SECURITY 133
5.1 Encryption Techniques 135
5.2 Key Management 142
5.3 Hashing Techniques 148
5.4 Cryptographic Applications 152
5.5 Perfect Secrecy of Communications 160

CHAPTER 6: ACCESS CONTROL MODELS 163
6.1 Design Principles 164
6.2. Bell-LaPadula Model 167
6.3 Biba Model 169
6.4 Clark-Wilson Model 171
6.5 The World of Networks and Hosts 171

CHAPTER 7: CYBER SECURITY TECHNOLOGIES 175
7.1 Security Controls 176
7.2 Security Processes 230
7.3 Security Testing 240

CHAPTER 8: OPERATIONAL CYBER SECURITY 267
8.1 Starting Cyber Secure 269
8.2 Cyber Security Management 287
8.3 Usage Guidelines 298
8.4 Personnel Cyber Security 310
8.5 Incident Detection and Response 315

CHAPTER 9: DEVELOPMENT OF INFORMATION SYSTEMS 319
9.1 Key Aspects of the Development Process 320
9.2 Assessment of Required Certification 323
9.3 Security by Design 329

9.4 Secure Implementation Guidelines 343
9.5 Testing and Certification 356

CHAPTER 10: CYBER SECURITY STANDARDS 373
10.1 Federal Information Processing Standard of US 375
10.2 Common Criteria 379
10.3 Information Security Management System 385
10.4 Internet Standards and Security Protocols 389
10.5 Legal Standards for Data Protection 391

CHAPTER 11: QUANTUM COMMUNICATION AND COMPUTING 393
11.1 Basics of Quantum Mechanics 396
11.2 Quantum Communication Technology 407
11.3 Quantum Computing Technology 413

CHAPTER 12: CONCLUSION 431
12.1 A Summing Up 432
12.2 Outlook to the Future 450

REFERENCES 469

INDEX 487

Foreword

Books are the widely preferred medium for recording and disseminating of knowledge from time to time. Indeed, they are the foundation for ensuring the continuity of even human cultures and civilizations. Therefore, it is a privilege to pen a foreword to a book authored by two of my professional colleagues. The title "Concepts and Practices for Cyber Security" suggests that this book is intended to provide insights into the domain of cyber security from a practitioner's point of view. This was expected from the two authors, Dr G Athithan and Dr SK Pal, as both have deep knowledge and working experience in this domain. It has been my pleasure to know them for the last several years in different capacities. What started initially as a mere official acquaintance, later evolved into a long-term valuable association and mutual knowledge sharing on a regular basis.

My former role as the Director General of the Microelectronic Devices and Computational Systems laboratories of DRDO demanded addressing the cyber security requirements of the organisation. I often sought suggestions from these two authors due to their practical expertise in the subject. I would like to emphasise that cyber security holds value for everyone, particularly when the whole world is forced to work remotely and interact virtually over the Internet and other open communication channels. In addition, the active roles of rogue nation-states and computer hackers alike have led to massive data breaches and also cyber-attacks on national critical infrastructure. In this scenario, the need for strengthening cyber security and improving awareness is of utmost importance for every individual, every organisation and entire nations. Perhaps there would not have been any better time to make a book such as this one available to citizens concerned about cyber security.

While there are many good books explaining the theoretical aspects of cyber security, this book is unique in terms of its content and practical orientation. I am impressed by many unique sections that are usually not found in standard cyber security books. Beginning with the basic notions of cyberspace, the first chapter emphasises the entities and aspects that require protection. The next chapter presents some fundamental models of computing and processing functions in order to highlight the fundamental vulnerabilities of computing systems. The information and infrastructure assets, the cyber threats, vulnerabilities and exploits are explained in the subsequent part of the book. This is followed by the sections on cyber security policy framework and formulation of cyber security policies. The chapters covering the role of cryptography in cyber security, access control models and their usage, and emerging cyber security technologies provide fresh thoughts and new directions. The next few chapters on operational cyber security, development of information systems, cyber security standards give insights into the practical world of cyber systems and their security requirements. The book covers these aspects of cyber security that only such experienced professionals can present in a lucid form. The careful planning and the organisation of the contents in simple language make for a fruitful outcome for readers to enjoy and learn in equal measure.

I am sure that the book will be a unique and important addition to any scientific and technical library. The reader would certainly gain valuable insights into the practical world of cyber security. As a timely offering, this book will find a wide readership among information security managers, cyber security officers, and professionals developing IT-based tools and applications. It will also be a welcome guide for researchers and students as it can help to identify research gaps and motivate them to work on open problems highlighting different dimensions and frontiers of cyber security. I congratulate the authors for their tireless efforts and hard work that has resulted in an informative and well-timed monograph.

New Delhi
January 2022

Dr Sudhir Kamath
Former Director General, DRDO

Preface

The transformational impact of information technology on the lives of individual citizens in recent times is only too well-known. It is safe to say that its impact on the functioning of corporations and nations has been even more transformational in scope. No other technology, now or in the past, has had the same kind of impact. Its arrival in the early 1970s, around half a century ago, truly marked the onset of what is now widely known as the modern information age. A significant feature of this age is the increasing migration of human memory, compute, and cognitive functions to information systems aka computers. Consequently, ensuring their trustworthiness and functional integrity has acquired huge importance. These two aspects are even more important in the sphere of defence information systems.

In this context, cyber security emerged as the natural response to assure trust and predictable behaviour on the part of diverse kinds of information systems. This emergence happened more or less around the end of the 1990s, just when the public careers of both of us, the authors, entered their middle phases. Backed by some predominantly computer science-based work experience until then, we were led into activities towards the development of cyber security technologies since then. As the focus was more towards meeting defence requirements, our experience and learning were that much more specialised and unique. With due respect to our cherished academic community, in contrast to the knowledge they impart, we had something complementary to offer, especially to the line managers. In his capacity as the National Security Advisor to the Government of India (2010-2015), Shri Shivshankar Menon remarked in one of his addresses to DRDO officers in New Delhi that the experiential learning of public servants is private education at public expense. As one among the audience, the first author resolved then to pen down his learning from his work experience at the first available opportunity. His co-author became a willing partner in this obligatory enterprise.

Unlike during earlier technological eras, the pace of change in the information technology era has been unprecedented and rapid. Furthermore, as a relatively late starter, our country embraced this technology at a faster clip in comparison to many other countries. Along with this rapid adoption of information systems for public good and governance came the urgent need for cyber security measures as well. On the one hand, the technological measures had to be put in place as much as possible. On the other hand, the weakest links in the security chain, namely the human users and managers, had to be continually made aware of the need for cyber security and the required measures. As a saying goes, cyber security is the responsibility not of security managers alone, but of everyone in the country. One person's weakly protected information system can become an attacker's opportunity to succeed on a large scale. Our motivation to write this monograph has been also to create awareness in every potential reader to keep his or her information systems safe. In the process, our effort has been to give the reader a holistic overview of the subject matter of cyber security.

While explaining any evolving domain such as cyber security, the focus on its fundamentals is paramount. Therefore, Chapter 1–The Introduction clarifies basic notions such as data, information, knowledge, and cyberspace. Chapter 2–Concepts of Information Processing enumerates the fundamentals of the domain starting with well-known models of computing. A highlight of this chapter is a discussion on the nature of processing functions with an emphasis on mobile and undocumented functions. Any awareness of security has to begin with an appreciation of threats to the assets to be protected. Accordingly, Chapter 3–The Cyber Threat Landscape lists cyber threats in various categories. It also identifies the vulnerabilities that these threats are likely to exploit and the corresponding attack scenarios. Measures to address security have to start with a plan, and a policy framework is needed to guide the planning process. Keeping this in view, Chapter 4 spells out the various aspects of a Cyber Security Policy Framework. An important aspect of the framework is the set of guiding principles and their role in policy formulation and finalisation of security requirements.

Plans are important, but more so are their implementation. Cryptography, access control, and cyber security technologies are the three pillars of implementation. Chapter 5–Cryptography for Cyber Security explains the role of encryption and hashing methods for ensuring confidentially and integrity of information. It covers the vital topic of management of the life cycle of encryption keys. Classical access control models provide the details for implementing the second pillar. Chapter 6–Access Control Models gives a detailed account of Bell-LaPadula, Biba, and Clark-Wilson models including an introduction to network firewalls. Chapter 7–Cyber Security Technologies is the largest in the monograph. It provides the details of the technologies required in three buckets namely, for controls, processes, and testing. It points out that security controls involve fewer human interventions, while security processes are largely people-oriented.

Careful planning and implementation can ensure that information systems are trustworthy and dependable. At installation time and before usage they have to start in a secure state. To remain secure, they need to be operated and used securely. Keeping these in mind, Chapter 8–Operational Cyber Security enumerates secure installation, configuration, and usage guidelines and best practices. It goes onto provide details of the management of privacy and legal obligations of personnel in the workplace among other important things. It caps the operational security or Opsec discussion with a section on how to analyse and identify insider threats. Cyber security solutions may mostly be sourced from the market. In a few cases, user agencies may even develop them in-house. In either case, the stages of the development life cycle have to follow guidelines to ensure security is built into the process and its outcome. Chapter 9–Development of Information Systems looks into the key aspects of the development process starting with a new approach to assess the required certification. It goes on to highlight the principles and practices for the secure design, implementation, and testing stages.

Standards are vital in any domain for quality and interoperability. It is more so in cyber security. Thus, Chapter 10–Cyber Security Standards helps the reader to look at the Federal Information Processing Standard (FIPS) related to cryptography, the Common Criteria (CC), the Information Security Management System (ISMS), and Internet Protocols. Besides giving an overview of each of them, the chapter also provides a critical review and an outlook on each case. The penultimate Chapter 11–Quantum Communication and Computing is all about the fast emerging domain called quantum information technologies. This new domain is poised to take the current impact of information technology to a whole new level. Keeping its complex nature in mind, the necessary background material is included in this chapter. In particular, the three fundamental quantum concepts of superposition, entanglement, and no-cloning theorem are explained in some detail. Chapter 12 concludes the narrative by providing brief summaries of all the previous chapters. It also gives an outlook on a few important emerging topics such as the Internet of Things, Artificial Intelligence and cyber security, Blockchain, and Biologically-inspired cyber security.

In our journey of writing this monograph, we have received immense support from a large number of accomplished professionals and colleagues. We owe them for the final outcome of our efforts in print. For the first author, the list begins with his first and foremost mentor, Dr G Venkataraman, former Vice-Chancellor of the Sri Satya Sai Institute of Higher Learning. He showed the way for a scholarship-oriented life and was inspirational for launching into this journey through his own stellar examples. Much of the experiential learning behind the writing was made possible through the leadership of Shri N Sitaram, former Director General, DRDO. His emphasis on user-focus and team work is highly acknowledged. Two other former senior colleagues need to be mentioned for the opportunities they provided for learning cyber security imperatives at a very high level. They are Dr S Christopher, former Chairman DRDO and Secretary Department of Defence R&D and Vice Admiral (Retd.) Raman Puri, former Chief of Integrated Defence Staff. The first author gratefully acknowledges the encouragement he received from them. His position in DRDO Bengaluru as a DRDO Chair from August 2019 enabled the writing process in several ways. He is very thankful to Dr Satheesh Reddy, Chairman DRDO and Secretary Department of Defence R&D for this appointment and facilitation. He is also thankful to Shri K S Varaprasad, Director General, DRDO for the support extended in this regard.

The second author would like to acknowledge the motivation received from his co-author Dr G Athithan, former Director General, DRDO to work in the area of cyber security and explore new domains of research and practice. Thanks are also due to former Directors of SAG, namely Dr CR Chakravarthy and Prof Veni Madhavan for their immense encouragement and support. The writing happened during the tenure of Mrs Anu Khosla, former Director SAG and he would like to thank her for the support he received. He would also like to gratefully acknowledge his research supervisors Prof SK Muttoo and Prof Vijay Kapur from Delhi University.

Dr Sudhir Kamath, during his tenure as Director General, DRDO, was instrumental in flagging off the monograph project and helping in the official process with DESIDOC. We thank him for all his support and guidance. We also thank Dr UK Singh, Director General, DRDO and former Director CAIR for reading the early drafts of the manuscript and providing useful suggestions for improvement. The review process integral to the monograph-writing project gave many insightful comments and suggestions. These inputs from the two anonymous reviewers helped us in improving the quality of the manuscript and in addressing a few overlooked gaps in the narrative. We are hugely thankful to them. The central role of priming the project and following it up belongs to Dr Alka Suri, former Director DESIDOC and her team comprising Ms Alka Bansal, Shri N K Chawla, and Ms Gunjan Bakshi. We cannot thank them enough. Dr K Nageswara Rao, Director DESIDOC ensured that the layout process progressed swiftly resulting in the final print version. We are grateful to him.

For the preparation of around seventy figures and illustrations in the monograph, we received professional help from Shri Sunil Subramanian and Ms Sindhu R. of EDC Creative Technology Solutions, Bengaluru. They deserve our appreciation for the excellent response from their team. Our learning was made possible not the least by our junior colleagues and peers, too numerous to list them individually. We gratefully acknowledge their contributions to our journey of learning and sharing our knowledge. Finally, we both thank our respective families for being supportive and allowing us the time necessary for completing this challenging exercise of writing a monograph on an important topic.

Dr G Athithan
Dr Saibal K Pal

CHAPTER 1

Introduction

'Man is the measure of all things: of things which are, that they are, and of things which are not, that they are not'

- Protagoras (c 490 BCE–420 BCE)

Of the things that we as humans encounter in our personal and professional lives, most owe their existence to natural sources and processes. The rest owe their origin to the imagination and enterprise of us as creators in our own right. Indeed, the proportion of the latter category, namely man-made things has been continuously on the rise vis-a-vis the former, nature-made things. Man may be the measure of all things as famously proclaimed by Protagoras and echoed by Eli Naptha, one of the characters in 'The Magic Mountain'[1]. Indeed, man can surely claim to be the measure of the list of his own artefacts. Since the dawn of civilisation, this list has been growing, sometimes steadily and sometimes dramatically. A far-reaching recent addition to this list is what goes by the name of 'cyberspace'.

When Norbert Wiener coined the word 'Cybernetics' in 1948[2,3], he might not have imagined that this word would be later adopted to convey the notion of the space where the activities of today's computers and communication networks play out. He proposed it to mean the science of control and communication in animals and machines. Later AN Kolmogorov generalised it to mean 'a science concerned with the study of systems of any nature which are capable of receiving, storing, and processing information so as to use it for control'[4]. The key word in Kolmogorov's definition is information, and the question arose concerning the space where it is received, stored, and processed. Taking the prefix from Wiener's coinage, this space has been labelled as cyberspace.

Thus, cyberspace is today understood to be an integral part of the information processing and communicating systems that we use every day. When we check our e-mails, chat, browse the Internet for information, pay our bills online, book our tickets on portals, update our status on social media sites, etc., we interact with this space. We do this either in our personal capacity or as the representative of an organisation, public or private, often on behalf of our employer. In both cases, much of the information handled might be confidential or private, requiring protection from unauthorised access or modification. In fact, our information and activities in the cyberspace define us today more objectively than our own words or perceptions can. Therefore, our wellbeing and success in our personal and professional lives are dependent upon the security of our information and activities in the cyberspace.

The case for the security of information and activities of organisations in the cyberspace has an even more serious dimension. Whether an organisation is a business enterprise, or a nation's military, or the nation-state itself, it needs to endure and prevail against its competitors and adversaries. As computerisation and networking in organisations inevitably increase, the battles for prevailing against competitors and adversaries are increasingly to be fought in the cyberspace. Therefore, the security of the cyberspace of organisations becomes paramount.

The target of security measures is the information housed in the cyberspace. On the one hand, information may be viewed as mere data in cyberspace needing a human reader to discern its meaning. On the other hand, some of this information may be factual or time-invariant tending to be knowledge. To address the security requirements appropriately, the nature of information and its relationship to data and knowledge has to be understood clearly. While information is the focus of protection mechanisms, the security of tools and platforms for processing information is equally important. In this context, the foundational concepts of information processing need to be understood and appreciated. The different types of information processing systems need to be understood as well. Finally, following the Cartesian approach of breaking down the complex to simple, the basic layers of cyberspace need to be identified and accounted for in their role in information processing. These aspects are elaborated in an introductory manner in the following sections.

DRDO MONOGRAPHS/SPECIAL PUBLICATIONS SERIES

About the Monograph

This book is borne out of the experiential learning of its two authors during their long careers in public service. While the objective is to address the compelling need for cyber security awareness in the age of information systems, the focus is on both theory and practice. In an evolving domain such as the cyber security, an understanding of its fundamentals is vital. Keeping this in view, the book starts with the basic concepts behind the development and operation of information systems. As is necessary for a book on security, it highlights threats to information systems next. Guidelines for formulation of cyber security policies and the means for their implementation and operation constitute the middle core of the book. Incorporating cyber security during the many stages of a system development cycle is given due coverage next, followed by a discussion on applicable standards. The penultimate chapter gives an overview of the emerging domain of quantum information technology and its impact on cyber security. The treatment of the subject is at a level accessible to the middle-level managers in public and private organisations. At the same time, experts in the domain too would find something to reflect upon and to evolve new solutions to the persisting problems of cyber security.

About the Authors

Dr G Athithan received his BE (Hons) degree in Electronics and Communications from the Coimbatore Institute of Technology, India in 1981. He received his PhD in Physics (of Neural Networks) from the Indian Institute of Technology, Mumbai, India in 1997. After a stint of seven years in the Department of Atomic Energy (DAE) of India, he joined the Defence Research and Development Organisation (DRDO) of India in 1988, from where he retired in 2018. At present, he is appointed as a DRDO Chair in the Centre for Artificial Intelligence and Robotics, Bengaluru, India. His work in DAE was mostly on computer graphics, computer-aided design, and modelling of Penrose patterns and crystal structures. Later, in DRDO, he contributed to the development of parallel computing technology, scientific data visualisation, and information security solutions. He was a Distinguished Scientist and one of the Director Generals of DRDO at the time of his retirement. His current research interests are artificial intelligence, network data mining, and cyber security technologies. He has published about 25 papers in peer-reviewed journals, about 30 papers in conference proceedings, and has co-authored a book. He is a senior member of IEEE.

Dr Saibal K Pal completed his Post-graduation in Computer Science in 1991 from the University of Allahabad and PhD in the area of Information Security from the University of Delhi. He joined DRDO in 1991 and is presently working as Scientist 'G' and Divisional Head at Scientific Analysis Group, Delhi. He has contributed to several R&D projects and international collaborations. He has also served as the Chief Information Security Officer of DRDO during the period 2017-19. His areas of interest are cryptology, cyber security, computational intelligence and information systems. He has authored three books on electronic governance and data science and more than 250 research publications in peer-reviewed journals and conference proceedings.

978-93-94166-07-3

9 789394 166073

Price: ₹ 1500
US $ 35
UK £ 30

Defence Scientific Information & Documentation Centre
Defence Research & Development Organisation
Ministry of Defence, Metcalfe House, Delhi - 110 054