

Preface

This book argues that neuromorphic computing, and particularly the recently emerging efficient hardware architectures for neuromorphic computing, are of particular significance to cyber defense in austere environments and to the continued evolution of any technological roadmap. In this overall volume, we bring examples from government, industry, and academic domains to illustrate special challenges of cyber defense where size, weight, and power (both electric and computing) of devices are tightly constrained. Of special importance are cognitive challenges of cyber users and defenders in austere environments, and to this end we review prior work on augmentation of related cognitive processes, such as visualization and algorithms that attempt to provide context and advice to the human. The state of the art in neuromorphic approaches (such as artificial neural networks) to cyber defense, and their successes and limitations, are discussed along with the emergence of new hardware such as memristor-based computing architectures that opens new opportunities for neuromorphic techniques in cyber defense. This effort sought to pursue, tactical, algorithmic, and hardware approaches currently being pursued within multiple disciplines to advance the state of the art in cybersecurity in particular to human cognition augmentation.

Chapter 1 covers the notion of cyber situational awareness, sensemaking, and situation understanding that are used in the literature to denote different components in the repertoire of cognitive activities exercised by analysts in the prosecution of cyber warfare. The chapter discusses the relative role of these components in cyber analysis and the nature of cognitive challenges they present, focusing on situation understanding. The purpose here is threefold: to clarify the notions, to elevate the role of understanding to that of the key determinant of successful performance, and to offer suggestions for the design of decision aids that are likely to facilitate situation understanding. These issues are tackled from a number of different perspectives. Accordingly, the text is divided into several brief sections that develop a

framework and set the stage for design suggestions, and consider the future of intelligent support for cyber warfare predicting transition from “machine learning” to “machine understanding.”

In Chap. 2, we present a newly developed in-house neural network learning algorithm called Adaptive Locally Influenced Estimation Network (ALIEN). The aim of this new learning algorithm is to reduce mathematical complexity and electronic overhead in contrast to existing neural network learning models for direct application within physical embedded hardware such as the emerging memristor-, more mature FPGA- or GPU-based technologies for network security applications such as network intrusion detection. In this work, we demonstrate two applications. The first application was to perform malicious network traffic classification within network flows utilizing the often-cited intrusion detection data set from the International Knowledge Discovery and Data Mining Tools Competition. The second application was in the classification of network packets containing DNS queries as A or MX requests. During our experiments, we were able to achieve a 98 % accurate classification of malicious network traffic utilizing only six fields of information and to perfectly classify 20,000 DNS A and MX packets when the training set of only two packets was used (containing one A request and one MX request).

In Chap. 3, we highlight the importance of developing automated tools and models to support the work of security analysts for cyber situation awareness. Current processes are mostly manual and ad-hoc, therefore they are extremely time-consuming and error-prone, and force analysts to seek through large amounts of fine-grained monitoring data, rather than focusing on the big picture of the cyber situation. To address this limitation, we show how an integrated set of automated tools can be used to perform a number of highly repetitive and otherwise time-consuming tasks in a highly efficient and effective way. The result of this type of automated analysis is the generation of a set of higher-level attack scenarios that can be used by analysts to assess the current situation as well as to project it in the near future. We believe this is an important step toward future generations of self-aware and self-protecting systems, but more work needs to be done in this direction to achieve this vision.

In Chap. 4, we focus on data mining in particular to application in modern cyber operations. Defending cyberspace is a complex and largely scoped challenge which considers emerging threats to security in space, land, and sea. Cyberspace is defined as a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. And, cyberspace operations are defined as the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. The global cyber infrastructure presents many challenges because of the complexity and massive amounts of information transferred across the global network daily. To this end, we seek to understand the role and practical functionality of data mining.

In Chap. 5, we describe how supply chain threats have invalidated the assumption that one may move critical software out of band of an attacker through the use

of secure hardware root of trust. Many systems consist of COTS hardware, which, through supply chain exploitations, may contain trojans. It is no longer valid to assume that an adversary has no reasonable avenue of attack even if the software protections are structured properly and augmented with secure hardware. In today's cyber-attack environment, one must assume that a subset of systems are, or will be, eventually compromised. With this new mindset development of next generation systems should focus on architectures that are capable of supporting design separation for high reliability and information assurance. Furthermore, these systems must be capable of continued operation while under attack and maintain protection of critical intellectual property. By leveraging a hybrid fault model with multiple, parallel execution paths and resultant execution trace comparison, in this chapter, we discuss a distributed architecture where algorithms and applications are fractionated across a cloud computation system to achieve desired security constraints assuring trusted execution. Furthermore, the model architecture can be scaled through proactive thread diversity for additional assurance during threat escalation. The solution provides dynamic protection through distributing critical information across federated cloud resources that adopt a metamorphic topology, redundant execution, and the ability to break command and control of malicious agents.

In Chap. 6, we discuss the future of cybersecurity as a warfare between machine learning techniques of attackers and defenders. As attackers will learn to evolve new camouflaging methods for evading better and better defenses, defense techniques will in turn learn new attacker's tricks to defend against. The better technology will win. Here we discuss the theory of machine learning based on dynamic logic that is mathematically provable to learn with the fastest possible speed. We also discuss cognitive functions of dynamic logic and related experimental proofs. This new mathematical theory, in addition to being provably fastest machine learning technique, is also an adequate model for several fundamental mechanisms of the mind.

In Chap. 7, we focus on malware threats on mobile devices. To address this critical issue, we developed an Artificial Neural Network (ANN)-based malware detection system to detect unknown malware. In our system, we consider both permissions requested by applications and system calls associated with the execution of applications to distinguish between benign applications and malware. We used ANN, a representative machine learning technique, to understand the anomaly behavior of malware by learning the characteristic permissions and system calls used by applications. We then used the trained ANN to detect malware. Using real-world malware and benign applications, we conducted experiments on Android devices and evaluated the effectiveness of our developed system.

In Chap. 8, we describe how the sustainable progress of modern society raises many environmental and organizational issues. Most obvious concerns are related to the problems of energy, as there is no adequate substitute for the depleting hydrocarbons. Especial significance bear energy developments for reliability and security of operational networks. Beyond cyber attacks, the apparent vulnerabilities of the physical integrity of the electrical power grid could be obviated by a decentralized generation of energy. Also, a dependable autonomous supply of energy is decisive for vast distributed networks of sensors and actuators. This chapter reveals a new yet not

recognized type of energy in the physical world. Such a possibility could be suspected from many paradoxical observations and experiments where involvement of regular sources of energy is not evident. The surmised new energy is extracted from impetuses of information-processing clocking pulses, the so-called “hot-clocking” effect, which drive the mechanism of the Holographic Universe. Most clearly, this mechanism transpires through the otherwise incomprehensible property of Universe’s nonlocality. The considered concept can explain the perplexing “excess heat” effect promising to provide clean abundant energy. This effect had been uneasily attributed to a kind of a nuclear process notoriously dubbed “Cold Fusion” that later on had been largely substituted by a milder term Low Energy Nuclear Reactions (LENR). Proper scientific understanding of the “excess heat” effect would remove the major stumbling block on the way of its reducing to practice.

In Chap. 9, we focus on how the memristor formalism provided by Leon Chua and promoted by Hewlett-Packard Labs has provided a compelling analogy to biological synapses and has led to very rapid progress in the field but it misses much of the complexity that is present in resistive switches. Examining this complexity, it is clear that these devices are in fact much more similar to biological synapses than was previously imagined and a variety of biomimetic opportunities exist for designing neural networks. By leveraging these advanced biomimetic functionalities, the use of memristors in neural networks (and other neuromorphic architectures) shows strong potential as an adaptive and accurate cyberthreat identification solution.

In Chap. 10, we describe how deploying intrusion detection systems (IDS) across all devices in a network can help increase resilience to cyber attacks. Such deployment will require extreme low power hardware to minimize the impact on the power consumption of mobile devices. Several studies have proposed neural network-based IDS. Additionally several other studies have proposed mapping traditional computer algorithms to neural network form to reduce power. This chapter examines the design of several novel specialized multicore neural processors. Such systems could enable pervasive deployment of IDS algorithms. Systems based on SRAM cores and memristor devices were examined. Detailed circuit simulations were used to ensure that the systems could be compared accurately. Two types of memristor cores were examined: digital and analog cores. Novel circuits were designed for both of these memristor systems. Additionally full system evaluation of multicore processors based on these cores and specialized routing circuits were developed. Our results show that the memristor systems yield the highest throughput and lowest power. Our results indicate that the specialized systems can be between two and five orders of magnitude more energy efficient compared to the traditional HPC systems. Additionally the specialized cores take up much less die area—allowing in some cases a reduction from 179 Xeon six-core processor chips to 1 memristor-based multicore chip and a corresponding reduction in power from 17 kW down to 0.07 W.

In Chap. 11, we present a memristor SPICE model and simulation for chalcogenide-based ion-conductor devices. As memristor-based technologies mature, it is important to be able to simulate large numbers of devices within the integrated circuit architecture in order to speed up reliably the development process

within the industry standard SPICE simulation environment. Our compact model replicates the characteristic hysteresis behavior through single-valued equations without requiring the need for recursive or numerically intensive solutions. The SPICE model netlist and fitting parameters are presented.

In Chap. 12, we describe the design and operation of a scalable distributed reconfigurable memristor-based computing logic architecture. From a Boolean logic point of view, any computing element functionality can be represented as a truth table that shows completely the validity of the computing logic function. Thus, we have designed and demonstrated the ability to use memristor devices to describe the operation of a distributed functional logic computing architecture. Given that memristor devices are reconfigurable devices whose impedance states are bounded by a maximum and minimum resistance values. Then, with the use of a digital decoder, we can select the distributed memristor device elements which contain the output value of the logic function whose inputs are the digital inputs to the decoder. With this computing architecture scheme any multiple input/output Boolean logic function can be designed and implemented.

In Chap. 13, we talk about how the class of reconfigurable systems, which include the digital field programmable gate array (FPGA) and emerging new technologies such as neuromorphic computation and memristive devices, represents a type of frontier for cyber security. In this chapter, we provide a brief sketch of the field of reconfigurable systems, introduce a few basic ideas about cyber security, and consider the implications of cyber security as it applies to present and future devices. We also attempt to provide some insights on how to add robustness to reconfigurable systems technologies.

Fairfax, VA, USA
Adelphi, MD, USA
Darlington, MD, USA

Robinson E. Pino
Alexander Kott
Michael Shevenell

Cybersecurity Systems for Human Cognition
Augmentation

Pino, R.E.; Kott, A.; Shevenell, M. (Eds.)

2014, XVI, 209 p. 113 illus., Hardcover

ISBN: 978-3-319-10373-0