Advances in Information Security 61

Robinson E. Pino
Alexander Kott
Michael Shevenell *Editors*

Cybersecurity Systems for Human Cognition Augmentation

Springer

Advances in Information Security

Volume 61

Series Editor

Sushil Jajodia, Center for Secure Information Systems, George Mason University, Fairfax, VA 22030-4444, USA

For further volumes:
http://www.springer.com/series/5576

Robinson E. Pino • Alexander Kott
Michael Shevenell
Editors

Cybersecurity Systems for Human Cognition Augmentation

Springer

Editors
Robinson E. Pino
ICF International
Fairfax, VA, USA

Michael Shevenell
ICF International
Darlington, MD, USA

Alexander Kott
Network Science Division
U.S. Army Research Laboratory
Adelphi, MD, USA

ISSN 1568-2633
ISBN 978-3-319-10373-0 ISBN 978-3-319-10374-7 (eBook)
DOI 10.1007/978-3-319-10374-7
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014952036

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

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 Robinson E. Pino
Adelphi, MD, USA Alexander Kott
Darlington, MD, USA Michael Shevenell

Contents

Contributors

James B. Aimone Cybersecurity Systems for Human Cognition Augmentation, Sandia National Laboratories, Albuquerque, New Mexico, USA

Massimiliano Albanese Center for Secure Information Systems, George Mason University, Fairfax, VA, USA

Gustave W. Anderson MacAulay-Brown, Inc. (MacB), Roanoke, VA, USA

Simon Berkovich Department of Computer Science, The George Washington University, Washington, DC, USA

Misty Blowers Air Force Research Laboratory, Information Directorate, Rome, NY, USA

Hasan Cam Network Science Division, U.S. Army Research Laboratory, Adelphi, MD, USA

Kristy A. Campbell Department of Electrical and Computer Engineering, Boise State University, Boise, ID, USA

George Corbin BAE Systems, Rome, NY, USA

Erik P. Debenedictis Cybersecurity Systems for Human Cognition Augmentation, Sandia National Laboratories, Albuquerque, New Mexico, USA

Arthur Edwards U.S. Air Force Research Laboratory, Kirtland, NM, USA

Stefan Fernandez Air Force Research Laboratory, Information Directorate, Rome, NY, USA

Brandon Froberg Air Force Research Laboratory, Information Directorate, Rome, NY, USA

Xinwen Fu Department of Computer Science, University of Massachusetts, Lowell, MA, USA

Linqiang Ge Department of Computer & Information Sciences, Towson University, Towson, MD, USA

Raqibul Hasan University of Dayton, Dayton, OH, USA

Sushil Jajodia Center for Secure Information Systems, George Mason University, Fairfax, VA, USA

Alexander Kott Network Science Division, U.S. Army Research Laboratory, Adelphi, MD, USA

Andrew J. Lohn Cybersecurity Systems for Human Cognition Augmentation, Sandia National Laboratories, Albuquerque, New Mexico, USA

James Lyke U.S. Air Force Research Laboratory, Kirtland, NM, USA

Matthew J. Marinella Cybersecurity Systems for Human Cognition Augmentation, Sandia National Laboratories, Albuquerque, New Mexico, USA

Mark R. McLean Center for Exceptional Computing, Baltimore, MD, USA

Patrick R. Mickel Cybersecurity Systems for Human Cognition Augmentation, Sandia National Laboratories, Albuquerque, New Mexico, USA

Kevin Nelson BAE Systems, Rome, NY, USA

Antonio S. Oblea Department of Electrical and Computer Engineering, Boise State University, Boise, ID, USA

Leonid Perlovsky LP Information Technology & Harvard University, Cambridge, MA, USA

Youngok K. Pino Information Sciences Institute, University of Southern California, Arlington, VA, USA

Robinson E. Pino U.S. Department of Energy, Office of Science, Washington, DC, USA

Olexander Shevchenko LP Information Technology, Cambridge, MA, USA

Tarek M. Taha University of Dayton, Dayton, OH, USA

Jonathan Williams Air Force Research Laboratory, Information Directorate, Rome, NY, USA

Guobin Xu Department of Computer & Information Sciences, Towson University, Towson, MD, USA

Chris Yakopcic University of Dayton, Dayton, OH, USA

Wei Yu Department of Computer & Information Sciences, Towson University, Towson, MD, USA

Yan Yufik Institute of Medical Cybernetics, Inc., Potomac, MD, USA

About the Editors

Robinson E. Pino is a visionary thinker and technology leader in cybersecurity, computational intelligence, computing architectures and development with the current role of Program Manager for the Advanced Scientific Computing Research (ASCR) program office in the Department of Energy's (DOE) Office of Science. In his portfolio, Dr. Pino focuses on revolutionary basic research and development efforts for high performance computing, cybersecurity, and applications that will enable our continued leadership through exascale and beyond computing and energy efficient technologies. Dr. Pino has deep and broad expertise within technology development, program management, government, industry, and academia. He previously worked as Director of Cyber Research at ICF International advancing the state of the art in cybersecurity by applying autonomous concepts from computational intelligence and neuromorphic computing for the U.S. Department of Defense (DoD) Army Research Laboratory (ARL) and various DoD and U.S. Department of Energy (DoE) collaborators, industry and academia. Dr. Pino's research and development program focused on the development of intelligent, autonomous, and cognitive applications toward network, host, and mobile security solutions. In addition, Dr. Pino was a Senior Electronics Engineer at the U.S. Air Force Research Laboratory (AFRL) where he was a program manager and principle scientist for the computational intelligence and neuromorphic computing research efforts. He also worked at IBM as an advisory scientist/engineer development enabling advanced CMOS technologies and as a business analyst within IBM's photomask business unit. Dr. Pino served as an adjunct professor at the University of Vermont where he taught electrical engineering courses. Dr. Pino has a Ph.D. and M.Sc. degrees in Electrical Engineering with honors from the Rensselaer Polytechnic Institute and a B.E. in Electrical Engineering with honors from the City University of New York, City College. He is the recipient of numerous awards and professional distinctions; has published more than 50 technical papers, including four books; and holds six patents, three pending.

Alexander Kott is responsible for fundamental research and applied development in performance and security of tactical mobile and strategic networks. He oversees projects in network performance and security, intrusion detection, and network emulation. Research under his direction brings together government, industry, and academic institutions working toward a fundamental understanding of interactions, interdependencies, and common underlying science among social/cognitive, information, and communications networks, including science for cyber. Previously, Dr. Kott served as a program manager for the Defense Advanced Research Programs Agency (DARPA), and earlier positions included technical director with BBN Technologies, director of R&D at Logica Carnegie Group, and IT research department manager at AlliedSignal, Inc. In 2008, he received the Secretary of Defense Exceptional Public Service Award and accompanying Exceptional Public Service Medal. Dr. Kott has a Ph.D. from the University of Pittsburgh. He has published more than 70 technical papers and coauthored and edited six technical books.

Michael Shevenell has over 25 years of experience managing and implementing the development of network applications using several technologies, including Python, Java, C++, Perl, PHP, CORBA, and C. He is also experienced in database development (Greenplum, PostgreSQL, Oracle, and MYSQL). Mr. Shevenell has led and managed teams of software developers and researchers that design and implement cybersecurity research, development, and applications. He has experience in the development of applications that take advantage of various types of Linux file-systems, cluster environments, and network emulation systems. Mr. Shevenell has played a major role in the research, design, and development of advanced Intrusion Detection System (IDS).

Chapter 1
Situational Awareness, Sensemaking, and Situation Understanding in Cyber Warfare

Yan Yufik

1.1 Introduction

The notions of situational awareness, sensemaking, and situation understanding are used in the literature to denote different components in the repertoire of cognitive activities exercised by analysts in the prosecution of cyber warfare. This 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 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 six brief sections: Sects. 1.1–1.4 develop a framework and set the stage for design suggestions in Sect. 1.5. Section 1.6 considers the future of intelligent support is cyber warfare predicting transition from "machine learning" to "machine understanding." (Throughout the chapter, the terms "situation comprehension" and "situation understanding" will be used interchangeably).

1.2 Discussing the Terms

Review [2] postulates that situational awareness (SA) for cyber defense encompasses the following seven aspects:

"1. Be aware of the current situation.
2. Be aware of the impact of the attack.

Y. Yufik (✉)
Institute of Medical Cybernetics, Inc., Potomac, MD 20854, USA
e-mail: imc.yufik@att.net

R.E. Pino et al. (eds.), *Cybersecurity Systems for Human Cognition Augmentation*, Advances in Information Security 61,
DOI 10.1007/978-3-319-10374-7_1

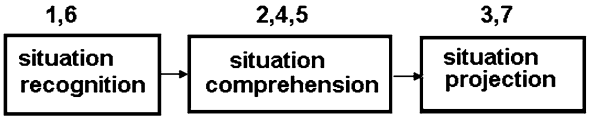

Fig. 1.1 The SA situation recognition (including Aspects 1 and 6), situation comprehension (including aspects 2, 4, and 5), and situation projection (including aspects 3 and 7) (adopted from [2])

3. Be aware of how situations evolve.
4. Be aware of actor (adversary) behavior.
5. Be aware of why and how the current situation is caused.
6. Be aware of the quality (and trustworthiness) of the collected situation awareness information items and the knowledge-intelligence-decisions derived from these information items.
7. Assess plausible futures of the current situation" (Barford et al. [2], pp. 3–4).

These aspects combine into three stages of SA, as shown in Fig. 1.1.

According to Fig. 1.1, comprehending a situation involves awareness of the perpetrator, the cause, the means and the impact. An extensive quote below presents a less general and more technical definition of comprehension tailored to the cyber domain:

> *SA Stage 2*: *Comprehension*. During the second cognitive fusion stage (situation assessment), an analyst performing escalation analysis first reviews the suspicious activity (perception). The analyst then combines and integrates his knowledge and experience with additional data sources to determine whether the suspicious activity represents an actual incident. He refines the mental model of the attacker's identity and threat level as he traces the attacker's path through the network back in time. Also in this stage, an analyst performing correlation analysis identifies and reports on patterns of suspicious and anomalous behavior; the reports serve to cue other analysts. This escalation and correlation analysis represents the comprehension aspect of SA. SA Stage 2 also involves limited projection. Escalation analysis includes some postulating about an attacker's actions if left unblocked. Incident responders, in choosing a course of action, project what future actions an unblocked attacker could take and what actions an attacker might take if he realizes he has been discovered ([4], pp. 229–233).

Per that definition, comprehending a situation in the cyber battlespace boils down to escalation and correlation analysis. Figure 1.2 places situation comprehension within a decision loop.

The process in Fig. 1.2 is, to an extent, consistent with the following definition of sensemaking:

> Sensemaking, as in to make sense, suggests an active processing of information to achieve understanding (as opposed to the achievement of some state of the world), and this is sense in which we mean it here: Sensemaking involves not only finding information but also requires learning about new domains, solving ill-structured problems, acquiring situation awareness, and participating in social exchanges of knowledge. In particular, the term encompasses the entire gamut of behavior surrounding collecting and organizing information for deeper understanding ([22]).

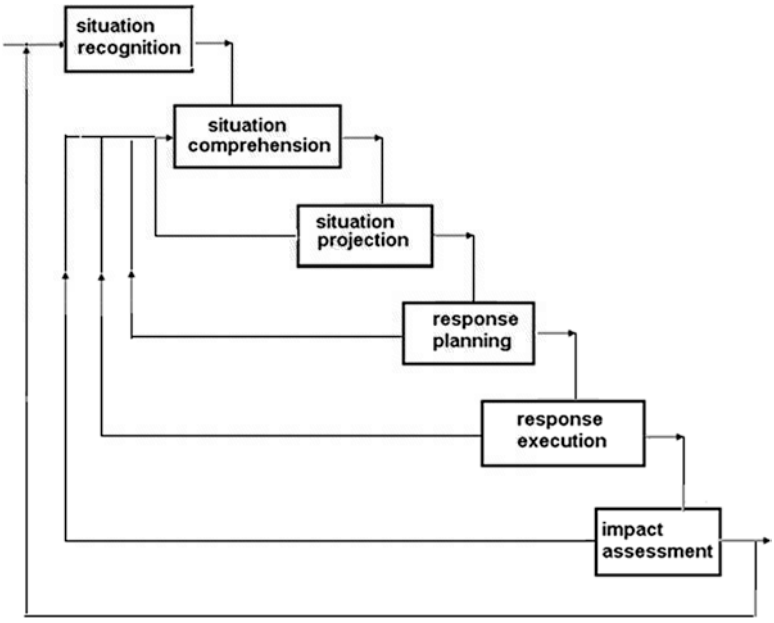

Fig. 1.2 Envisioning how the situation can evolve and formulating appropriate responses are predicated on reaching an adequate level of situation comprehension. The diagram emphasizes that the process is not linear: Comprehension can improve in the course of cognitive activities in every stage, which, in turn, can lead to adjustments in those activities. Arrival of new data might or might not change the way the analyst views the current situation

According to the definition, "sensemaking" denotes cognitive activities directed towards and preparing the stage for the onset and subsequent improvement of understanding. (Note discrepancies in the interpretations of the concepts: Situational awareness can be viewed as a constituent of sensemaking [22, 16] or the other way around [2]. This chapter adheres to the former interpretation). Collecting and organizing information culminates in achieving understanding, as illustrated in Fig. 1.3.

Figure 1.3 connotes several ideas:

1. Information processing necessary for reaching understating, is a laborious activity.
2. The fruits of the labor include fast and streamlined action planning.
3. The apex of understanding might never be reached (or reached too late, in the fashion of Monday-morning quarterbacking).

Reaching the apex (grasp) is accompanied by the emergence of cohesive cognitive structures (mental models) amenable to cognitive operations not available on the sets of disjointed information elements. Efficient decision making is the product of such operations (for more on this subject, please see [27–32]).

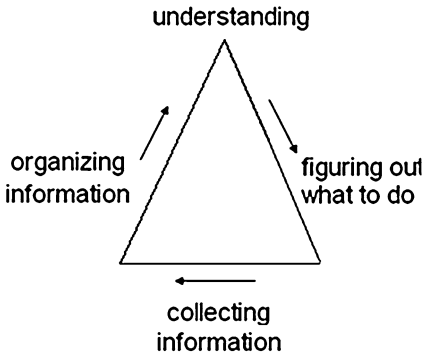

Fig. 1.3 Situation understanding mediates between information gathering and action planning

1.3 What is "Understanding"?

Webster's Collegiate Dictionary defines understanding as

> 1: a mental grasp …2a: the power of comprehension, *esp*: the capacity to apprehend general relations of particulars.

Apprehending general relations of particulars is the hallmark of human cognition (e.g., the Latin *cogito* derives from *coagitare*, to shake together ([13], p. 183)). "Shaking together" some disjointed information elements can result in either piling them into a heap or creating a well-organized, cohesive cognitive structure (mental model). Figure 1.4 illustrates the distinction.

The job of climbing the pyramid (as in Fig. 1.3), from the bottom of information gathering to the summit of understanding, is the sole responsibility of the decision-maker. Assume that the driver takes the trouble of collecting information beyond the minimum needed for reaching the destination from the current location and then organizing this information into a coherent model, what would such an effort afford? The results include, but are not limited, to the following:

1. Ability to figure out and flexibly adjust routes between any points (as opposed to learning some fixed routes and rigidly adhering to them).
2. Ability to retain different routes in one's memory and retrieve them on demand.
3. Ability to reverse one's mental steps (i.e., going back from B to A in one's mind) and trace possible alternative routes, without having those traces interfere with each other.
4. Ability to deal efficiently with unforeseeable obstacles such as a street that is closed off because of an accident.
5. Ability to determine whether novel inputs or, at least, some of them are relevant (salient) or irrelevant to the task at hand (e.g., the sign "street is closed" is relevant if the street happens to be on the current route and irrelevant if otherwise).
6. Ability to foresee the forthcoming inputs (or, at least, some of them, as in "a second roundabout will have to come up shortly after passing the first one").

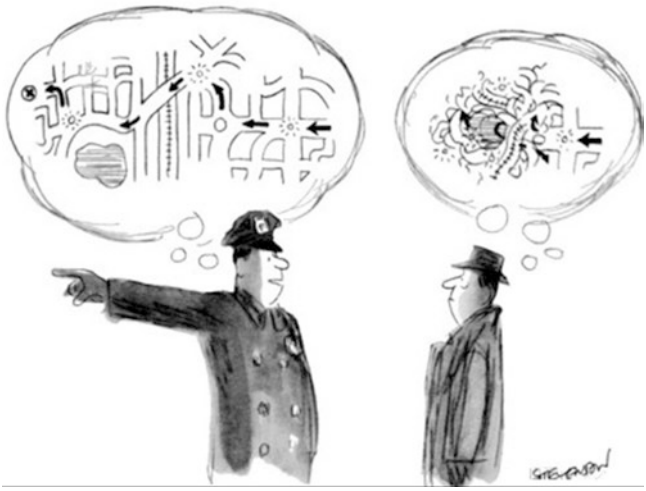

Fig. 1.4 Driving in the pre-GPS era. The officer understands the situation (holds a well-organized mental model) while the driver does not. Instructions can make the driver aware of the relevant information elements (the "particulars") but cannot do the job of pulling those elements together into an actionable model. (Drawing by Stevenson, 1976, The New Yorker Magazine, Inc.)

Fig. 1.5 An organized structure (image of a bearded man) might or might not emerge from the aggregation of shapeless blobs. It was found that some people fail to grasp the image, however hard and for however long they try

The latter three abilities become crucial when time is of the essence. Since in real-life situations time is always of the essence, albeit with different degrees of urgency, the key dilemma facing decision-makers consists of choosing between (a) expending time and effort in hope of reaching situation understanding thereby enabling robust performance and (b) avoiding such expenditures and thus increasing the risk of performance breakdown. Two factors exist that can bias a decision-maker toward the latter choice: Expenditures can be steep and success is never certain. An image in Fig. 1.5 ubiquitous in psychology textbooks will help to appreciate these factors.

In difficult tasks, the temptation is to constrain oneself to seeking local relations and abandon looking for the global ones, as in Fig. 1.6.

Fig. 1.6 The effort of organizing information can be extended to a few available information elements while ignoring the rest (e.g., some people are quick to see a fig. of a person throwing an object with the right hand)

1.4 Anatomy of Grasp

Two transformations appear to occur simultaneously at the apex in Fig. 1.4: The previously disjointed information elements (the "particulars") form distinct groups and, at the same time, different levels of significance (weights) are attributed to the groups and the elements. It is helpful to recognize that these transformations are expressed in two strategies of machine learning: unsupervised and supervised learning, correspondingly. Figure 1.7 illustrates the notion.

Grouping and significance attribution are inseparable facets of the grasping phenomenon that create the foundation for mental models and enable complex cognitive functions (operations on the models). Two examples—similarity judgment and classification/forecasting—will help to substantiate these contentions.

One of the best validated theories in psychology determines similarity S (A, B) of two objects A and B as a function F of the number of shared attributes (features) minus the number of distinctive attributes, as follows:

$$\mathrm{S}(\mathrm{A},\mathrm{B}) = \mathrm{V}_1\mathrm{F}(a \cap b) - \mathrm{V}_2\mathrm{F}(\mathrm{a}-\mathrm{b}) - \mathrm{V}_3\mathrm{F}(\mathrm{b}-\mathrm{a})$$

Here a and b are lists of features of A and B, $(a \cap b)$ is the overlap, (a-b) and (b-a) are the features of A and B identified as distinctive when comparing A to B and B to A, correspondingly (similarity determinations are not symmetrical), and V_1, V_2 and V_3 are parameters (weights) reflecting subjective significance attributed to various features [26]. Besides accounting for subjective significance, the theory postulates prior extraction of relevant features ("…the representation of an object as a collection of features is viewed as a product of a prior process of extraction and compilation" ([26], p. 329). That is, the number of features one can associate with an object