Cyber Security and the Role of Intelligent Systems in Addressing its Challenges

YANIV HAREL and IRAD BEN GAL, Tel Aviv University
YUVAL ELOVICI, Ben-Gurion University of the Negev

CCS Concepts: • **Security and privacy** → *Security requirements*; *Social aspects of security and privacy*; Systems security; File system security; • **Computing methodologies** → **Artificial intelligence**; *Machine learning*; • **General and reference** → *General literature*; • **Social and professional topics** → Computing industry; Theory of computation

Additional Key Words and Phrases: Cyber security, cyber definition, autonomous systems, internet of things, cyber technology trends, artificial intelligence, machine learning, cyber collaboration, intelligent systems, cyber phenomenon, cyber challenges

ACM Reference Format:
Yaniv Harel, Irad Ben Gal, and Yuval Elovici. 2017. Cyber security and the role of intelligent systems in addressing its challenges. ACM Trans. Intell. Syst. Technol. 8, 4, Article 49 (May 2017), 12 pages.
DOI: http://dx.doi.org/10.1145/3057729

1. INTRODUCTION

We are living in a unique period of history, and the current technology revolution will be among the most dramatic societal transformations remembered by humanity. The important changes associated with the invention of the engine, electricity, and the printing press gradually transformed society in the western world over a period of over a hundred years. The changes accompanying the current revolution have significantly altered the lives of average citizens across the globe in less than a generation. This is unprecedented.

In the past, revolutions spanned decades, enabling the establishment of processes and systems. For example, a language that supports the new revolution evolves, and leaders emerge, with the fresh perspective required by the revolutionary changes. New disciplines are created and new occupations are developed to support the changes. The present revolution is taking place at such a high speed that such enabling processes and systems have not yet been established, let alone developed or matured, and they will continue to be created well into the future.

Over the past three decades, an important new vector of the technology revolution has emerged: the cyber domain. In particular, the technological aspects of cyber—such as computer technologies, access to information and systems, greater connectivity among subsystems, and the combined effect of all these aspects on a growing list of diverse spheres—expose the world to unprecedented risks. Academia and the intellectual

Authors' addresses: Y. Harel; email: yaniv.c.harel@gmail.com; I. Ben-Gal; email: bengal@tau.ac.il; Y. Elovici; email: elovici@bgu.ac.il.

DOI: http://dx.doi.org/10.1145/3057729

infrastructure associated with the cyber domain are struggling to keep up with the domain's rapid pace.

Cryptography is a mature discipline, with strong connections to mathematics and computer science, which have helped the discipline evolve and develop over the years. Traditionally, it has been the cyber area most rooted in the academic world. However, many other technological subjects should also be part of the cyber academic discussion. Each month, as the cyber effect expands, new aspects of this arena become part of the cyber theoretical discipline. For example, the autonomous car came on the scene in recent years [Coppola and Morisio 2016], and it did not take long before a cyber threat associated with the autonomous car was identified. The immaturity of the discipline is reflected by the fact that cyber is currently being discussed on many stages and studied by researchers from diverse disciplines and perspectives. The issue of whether cyber is a pure discipline or a topic that relates to several disciplines will continue to be discussed in the coming years. The following special issue includes a collection of selected papers that cover the diverse cyber domain and how it interfaces with intelligent systems. The topics were presented at the Tel Aviv Academic Conference over two successive years. The scope of this special issue is relatively broad, yet there are many cyber issues that have not been addressed in this edition.

2. CYBER DEFINITION

Despite the increasing presence of the cyber domain in our daily routine, a clear definition of cyber security is elusive. Von Sloms and Van Niekerk [2013] describe how the notion of cyber security has evolved from securing information (e.g., defending against malware) to the more general integration of physical and digital domains (e.g., in urban infrastructure). Based on their ideas, we propose a broader definition of cyber security. We propose that the concept of cyber be related both to *Cyber Security* and a larger *Cyber Phenomenon*. Based on this broad definition of the cyber concept, cyber security pertains to all actions that can take place on a computerized platform, with or without the knowledge of the owner of the platform, as well as all of the technologies, products, and efforts that can be used to defend against such actions. The Cyber Phenomenon refers to a wide phenomenon encompassing all of the technological aspects of cyber (such as computer technologies, access to information and systems, and greater connectivity among subsystems) and their effects on a growing list of diverse spheres (including the societal, economic, political, judicial, and cultural spheres).

Our broader definition of cyber directly addresses its multidisciplinary nature. In the past decade, scientific research has increasingly focused on diverse aspects of cyber security, moving away from traditional malware and cryptology analysis [Jang-Jaccard and Nepal 2014]. Topics include the security of vehicles and implantable medical devices such as pacemakers [Rushanan et al. 2014]. These examples are part of the Internet of Things (IoT), a rapidly emerging trend with serious cyber security implications. The IoT is connecting an increasing amount of physical objects (such as cars, electronic devices, and buildings) and enabling them to "communicate" with other entities by collecting and sending data [Whitmore et al. 2014]. This is an exciting technological development that brings the physical and cyber dimensions closer; the bridging of the two dimensions holds great potential and opportunity but also creates new and complex privacy, trust, and security issues [Sicari et al. 2015]. Another developing area of cyber security focuses on the security issues associated with smart cities, cyber-physical systems, and critical infrastructure [Elmaghraby and Losavio 2014]. This area of research develops tools to identify and protect sensitive infrastructure, ranging from the national to the local level. The need for such tools is based on our increasing dependence on computer systems, the growing convergence between physical and cyber systems discussed earlier, and recent events that demonstrate how nations use cyber warfare against

each other. This, of course, does not disregard the advances in more traditional areas of cyber security, such as malware research, cryptography [Ganeshkumar et al. 2014], early detection and intervention [Fernandes et al. 2015], and privacy [Jentzsch 2015].

With regard to the cyber phenomenon, issues in cyber technologies are also examined in the social and humanities contexts. A wide range of topics are addressed, including issues pertaining to the political, criminal, and economic aspects of cyber security and more generally to the cyber ecosystem [Choucri 2013]. In these areas, cyber security is expanding and considering classic issues in economic domains, such as economical models based on the financial aspects of cyber security, cyber insurance, commercial cyber security issues, and cyber currencies [Jentzsch 2016]; judicial domains, such as issues of cyber intellectual properties [Svantesson 2016] and the development of cyber law, cyber contracts, methods to monitor and uphold cyber laws, and privacy protection laws; international domains, such as government accountability regarding cyber attacks, international cyber treaties, cyber deterrence, the development of cyber weapons and cyber offenses, cyber trade monitoring, and cyber crime [Aggarwal et al. 2014]; social domains, such as societal response to cyber, privacy issues, and the future effects of cyber on society [Kral 2014]; and cultural domains, such as cyber-inspired poetry, music, film, and theater.

3. THE MAIN CYBER SECURITY INDUSTRY TRENDS

The cyber security industry follows the major technological trends in modern society and builds its response accordingly. Thus, it is influenced by current trends that reflect the characteristics of the threats and challenges. After gaining increased understanding of the main vectors, and challenges, a response is often developed with the aim of strengthening society's ability to cope. We identify six main trends that will affect and shape cyber security development in the near future: automation, collaboration, virtual and shared resources, fighting the unknown, the Internet of Things, and the move toward an autonomous world.

Automation. Over the last decade, the cyber defense industry has focused on creating a mechanism [Dobson et al. 2006] involving sensors capable of providing alerts and current situational updates to organizations' cyber operation centers. On the one hand, this method was successful at both providing a centralized point of information for cyber command centers and the identification of problems and anomalies [Ramuhalli et al. 2013]. On the other hand, new problems were caused by overloading organizational cyber operation centers with more data than humans could efficiently process [Mancuso et al. 2015]. Better training, improved skills, and additional personnel were not enough to keep pace with the growing amount of data. In the next decade, the cyber industry will focus on establishing automatic systems to support the organization's Security Operation Center (SOC). Computerized systems will process and analyze data and even make simple decisions, while complex decisions will remain in the hands of the SOC's human resources.

Collaboration. Although there are a few collaboration platforms and shared commercial capabilities that have created a broad approach regarding cyber threats, most organizations in the world today faces cyber threats independently and respond accordingly. In contrast, cyber criminals have collaborated in many cases of cyber crime attacks. While such collaboration has benefited attackers, cooperation in cyber defense among organizations has been very limited – as collaboration can expose organizations to reputational damage. In addition, there is a danger of information leaks that can damage and threaten the organization's ability to defend itself. There are many reasons not to share information; this can be illustrated by the fact that large companies have a lack of motivation to share information. In contrast, small and medium-sized businesses often act differently and are eager to share information. Despite this, there are

advantages to collaboration and it will be an important trend going forward. Sectorial similarity among companies from the same industry underpins and fosters important collaboration [Zuiderwijk et al. 2015]. In the coming years, the industry will invest in the creation of new platforms for cooperation against cyber crimes [Peters 2015]. Currently, some corporations have developed platforms and solutions to protect themselves against the negative aspects of cooperation. Others focus on optimizing the process to establish a basis for new industry standards. This is imperative and will be integrated with governmental regulations and cyber security norms of conduct.

Virtual and Shared Resources. The revolution that began a decade ago with the creation of virtual servers and dynamic allocation of processing power has been developed in recent years. It expands the software-defined trend and other organizational information technology (IT) components, including the Internet and storage resources [Tang et al. 2016]. Central computing resources are being developed to provide quick operational response and maximize IT capabilities and resources. Shared resources can be cost-effective, because the average amount of resources needed to meet the demands of different systems is considerably less than the maximum value required.

This new world has brought cloud capabilities (vast IT resources and necessary applications and software infrastructure) to organizations around the world. The situation in which an organization transfers many capabilities to the cloud or consumes services provided on the cloud [Guo et al. 2014] is the essence of the revolution. Gradually, infrastructure, IT, and software qualifications are consumed as shared services. This perception is effective and efficient, but it also poses a significant challenge to the cyber world in which segregation between different processes can be critical [Majhi and Bera 2015]. At the same time, these shared capabilities challenge the world of privacy, reliability, and continuity [Sgandurra and Lupu 2016], bringing rise to the issue of the cyber defense abilities of small organizations in comparison to large organizations that provide shared services on a huge scale.

Fighting the Unknown. For many years, the efforts of the IT security industry were based on the assumptions that attacks were conducted on a large scale and major threats spread before arriving at a specific network or computer. Solutions were created on the basis of these assumptions and addressed as follows. A typical threat was identified as a virus, which was investigated by IT security company labs that identified the virus signature and sent this information to endpoints installed with the leading antivirus software. The endpoint then sent an alert that updated the user and provided instructions about removing the threat (according to the user IT security policy).

In recent years, with the development of new and advanced threats and attack methods, attackers have better understanding of how to adjust dedicated attack tools for their specific requirements. Such polymorphism [Li et al. 2010] is similar to painting in different shades and has created a situation in which one cannot assume that the threats are known and there is a need to provide an effective response to the threat when it is initially encountered. This change represents a transition in the area of cyber defense. The world is facing the change with the development of solutions such as anomaly detection [Chandola et al. 2009], behavior analysis (which creates a white list of behavior parameters), simulation (to identify risks before attacks happen and shorten response time), the use of honey pots, and so on. This trend will continue in the coming years, leading to the development of sophisticated techniques to expose threats and build efficient responses that are capable of stopping attacks when an organization first encounters them.

Internet of Things. In the past, most Internet interactions were interactions between humans that communicated via different platforms over the global network.

Communications between humans, as the primary users of online communications, will change dramatically with the evolution of the IoT realm [Ko et al. 2016]. Most of the entities that will communicate on the Web in the future will be machines [Schaffers et al. 2011], and they will be used to initiate reports, make contact, or respond to requests. The means to facilitate this is characterized by easy access to the Web and the ability for mass distribution. For example, there is a possibility to turn households into smart homes with intercommunicative technology instead of investing in designing a supporting infrastructure. Even scattering sensors along oil fields is the result of technological developments that led to a decrease in the price of materials [Chen et al. 2017], easy logistical operation, and resistant products that meet industrial standards. On the one hand, the IoT revolution makes mass distribution possible and mainstream; on the other hand, the cyber world is challenged by IoT in a dramatic way. Take, for example, the issue of dealing with cyber threats on IT products. The cyber threat for an inexpensive IoT product is, in many cases, not any different than a threat for a luxury IoT product; however, the ability and motivation to provide protection for a cheap IoT product is very low and cuts into the profit margin. The cyber world needs to rethink and shape new methods to provide a response to challenges such as these. The last distributed denial-of-service attack on the DYN Company illustrates that, although the IoT revolution has just begun, new threats are just around the corner.

The Move Toward an Autonomous World. For years, the cyber defense field has dealt with information security based on mitigating the risk that information would get into the wrong hands, get lost, would not be available, or would be modified maliciously. All of these are significant risks, with the ability to cause great damage, and damage with regard to information can have economic, political, and personal impact. The Snowden affair, Ashley Madison, Sony, and other examples show the harm that can be caused by cyber attacks. The danger increases significantly when machines operate autonomously. Robots are being integrated into society [Doumanoglou et al. 2016] and will gradually take on an increasing number of tasks currently handled by humans. Within this new reality, the ability of cyber attacks to cause damage, including harm to human life, is increasing. This could radically change our perspective of attacks to the point that threats resulting only in IT damages are considered minor.

The cyber world has barely begun to focus on new types of dangers such as the autonomous world, since this process has just started [Li et al. 2016]. However, the severity level of the threat is clear. In the coming years, the cyber defense community will be called upon to develop new and effective technologies to meet the challenges posed by our changing and increasingly autonomous world.

4. THE CONTRIBUTION OF INTELLIGENT SYSTEMS TO CYBER SECURITY

In recent years, a large amount of research addressing the contribution of intelligent systems to cyber security has been conducted. One can hear more and more about *artificial intelligence* (AI), *machine learning,* and *deep learning* systems in cyber security. As often happens with buzz words, nonexperts tend to use them casually and loosely. Despite the fact that the borderlines between such terms are not always clear and these borderlines become even fuzzier with new practical and theoretical developments, it is important to try to characterize the focus of these systems in the field.

Artificial intelligence (AI), which was officially established in the late 1950s by scholars such as Marvin Minsky, is used as a generic name representing a wide variety of methods, tools, and techniques that mimic "cognitive" functions or tasks that people associate with the human mind, such as "learning," "planning," "reasoning," or "problem solving" [Russell et al. 1995]. The importance of AI in cyber security is twofold and related to two opposing directions. The first direction focuses on AI-controlled

systems as potential targets of cyber attacks, mainly due to their increasing role in controlling vital and complex systems. There are numerous examples of cyber risks related to AI-controlled systems, such as smart vehicles [Berger and Iniewski 2012], smart grids [Yan et al. 2012], and smart cities [Elmaghraby and Losavio 2014]. The second direction addresses AI as an important set of *tools* that can help identify cyber breaches and cyber risks. This direction contains most of the engineering and computer science–related papers, including most of the papers that are published in this special issue.

Knowledge-based systems and *machine learning* methods are two well-known classes of AI methods that contain valuable tools used in cyber security. In *knowledge-based systems*, a huge amount of (experts') knowledge is uploaded to the computer memory (thus, it is also called *expert systems* [Feigenbaum 1977]). The learning part in these systems is based on the reasoning related to this large body of knowledge, which is often obtained by programmed rules (such as "if–then" and "inference logic rules"). Antivirus and antispam software packages [Blanzieri and Bryl 2008] represent straightforward implementations of expert systems in cyber security. In this case, expert knowledge (accumulated based on a large amount of transactions) regarding the procedures used—such as applied protocols, network traffic (e.g., HTTP, HTTPS, VoIP, or email), and I/O interactions with the operating system—is organized systematically to protect the users from cyber breaches. There are several papers in this issue that serve as good examples of such expert systems [Maltinsky et al. 2017; Kolman and Pinkas 2017; Hirschprung et al. 2017].

Machine-learning methods, unlike knowledge-based systems, usually refer to applications in which the learning component is performed by the computers "themselves." This is often done by extracting relevant patterns from the data and using them to derive predictions and smart recommendations. In other words, machine-learning algorithms are improved "automatically" through experience with the data, while giving the computers "the ability to learn without being explicitly programmed," as suggested long before the field of cyber security was formally established [Samuel 1959]. There are many examples of cyber-security tasks that can be addressed by machine learning, including user monitoring, spam filtering, zero-day attack identification, risk analysis, and many more.

It is well known that machine-learning methods are divided into two main classes (and a hybrid class of methods that combines the two). The first class contains *unsupervised learning* methods, in which untagged data samples are introduced to the system in order to find significant patterns. Fraud detection in financial systems, anomaly detection in communication protocols, and segmentation of both users and software packages according to their risk potential are good examples of *unsupervised machine-learning methods* that apply techniques, such as anomaly detection and clustering, to identify both "positive" or "negative" deviations from the norm. These deviations are then mapped into actions that include, for example, risk assessment of new software packages, blacklisted websites, or blocking Internet connections with high rates of suspicious users. Two papers published in this issue are introduced in this section, which serve as good examples of unsupervised machine-learning methods [Maltinsky et al. 2017; Ben Neria et al. 2017].

The second class of methods belongs to *supervised learning*, in which the data samples that are introduced to the system are tagged *a priori*. In other words, the sample data inputs are coupled with their desired outputs (thus the term *supervised*). The goal is to learn a general rule that maps inputs to outputs. Some examples from the cyber security domain are users' risk scores [Ben Neria et al. 2017], for which descriptive features of users—such as the communication volume, time, and the type of interaction—are

tagged either as "risky" or "nonrisky" and are then learned by the system to predict high-risk users in advance [Gruber and Ben-Gal 2017].

Within the class of *supervised-learning* methods (that contain many other tools, such as decision trees, support vector machines, and regression models), there is a unique group of *artificial neural networks*, which are models that were inspired by the structure and functional aspects of biological neural networks in the human brain. Layers of nodes ("neurons") are connected to each other via weighted edges that are fine-tuned by mapping inputs to tagged outputs. These models are often used to represent complex (nonlinear) relationships between inputs and outputs; they were considered to be very successful and got another boost recently from the deep-learning revolution. *Deep-learning* models initially emerged from this subset of methods, consisting of neural networks with multiple processing layers. These highly complex models require both high-speed processing units and a large amount of data, which became more available with the development of big-data technologies and cyber-security techniques. Deep-learning models also evolved to address *unsupervised learning* and were found to be extremely successful in signal processing (for which a lot of tagged data exists), specifically in *image processing,* which supports computer vision, and in *speech recognition* [He et al. 2016; Hinton et al. 2012], for which it has the primary task of identifying the user and providing the user with the correct authorization level. These models gained quite a bit of attention recently when leading global companies decided to invest significantly in these models in order to develop new applications; examples include Apple (e.g., Siri), Alphabet/Google (e.g., self-driving cars), and Facebook (automated image processing). These models have been shown to generate excellent results with specific tasks, yet this performance is not always guaranteed, especially in noncontinuity cases [Schmidhuber 2015]. Moreover, these models are not as descriptive as other analytic models, such as closed-form regression models, decision trees, or graphical networks. Therefore, their outputs pose challenges in terms of their interpretation or intuitive understanding by cyber security analysts (that play a vital role in cyber defense) [Ganesan et al. 2017] and by other decision makers (e.g., the Chief Information Officer) in cyber security. Thus, *deep learning* is a subset of *machine learning*, which is a central branch of AI. Deep learning should be viewed as an important tool in the cyber security toolkit, specifically when the analytic tasks involved require modeling a large amount of data by complex, often nonlinear, relations between the system's input and output.

To summarize, we believe that the role of *intelligent systems* in cyber security will continue to grow, while the development of these systems, like any other scientific development, poses both negative and positive effects on cyber security.

5. CASE STUDY: INTELLIGENT SYSTEM FOR THE DETECTION OF UNAUTHORIZED INTERNET OF THINGS DEVICES

IoT devices are widely deployed in the IT infrastructure of many organizations, a trend that is expected to continue in the coming years. The risks that IoT devices pose to organizations have been demonstrated by security experts [Singh and Singh 2015; Zhao and Ge 2013]. Given these risks and the increasing popularity and widespread adoption of such devices, their inherent mobility and diversity, and standardization obstacles, organizations require new forms of protection based on the ability to detect unauthorized IoT devices connected to their networks.

An intelligent system capable of detecting suspicious IoT devices, particularly those that are not part of the organization's *white list* of trustworthy IoT devices, provides a solution. In such a system, supervised machine-learning algorithms are applied on network traffic in order to accurately identify IoT devices listed on the approved white list. Any device that is not identified will raise a security alert. The task of device identification can be treated as a multiclass classification problem, based on a set of

authorized devices D (white list) and a structured set of traffic data and the assumption that each device Di on the white list D is represented sufficiently in the labeled dataset. Supervised learning, which captures the behavior of all of the authorized devices on the white list, is used to induce classifier C, and the classifier is used for device identification on new streams of (unlabeled) network traffic data.

In a system evaluation experiment conducted at Ben-Gurion University of the Negev, data was collected from eight different IoT devices and their network traffic was manually labelled. This data was used to train the multiclass classifier-based system, and 274 features were extracted from each network session [Bekerman et al. 2015]. The comprehensive evaluation demonstrated the classifier's ability to correctly classify the white-listed devices as trustworthy and the unlisted devices as suspicious [Bohadana 2017].

Eight multiclass classifiers were induced during the evaluation. In each case, the classifier C was induced by withholding one IoT device, which was used to represent an unknown device; the other devices represent the devices on the white list D. Accuracy, based on correctly classifying each device that is part of the white list and identifying the withheld device, guided the parameter optimization process.

After experimenting with XGBoost, GBM, and Random Forest, and various threshold levels, the Random Forest model was found to yield the best results: $tr = 0.75$. The evaluation process concluded by utilizing the optimal parameters (majority vote on the classification results of 247 sessions, and classification threshold $tr = 0.75$); in this case, the system was able to accurately detect (with 100% accuracy) all of the devices on the white list as well as each of the unauthorized devices.

This intelligent system demonstrates how machine-learning techniques can be employed to solve new cyber security threats (particularly IoT security, in this case). Additional information regarding this research can be found in Bohadana [2017].

6. THE SPECIAL ISSUE TOPICS

The special issue includes topics that were presented during the technical sessions of the academic conference that is held every year in Tel Aviv as part of Cyber Week. The topics were selected to address a variety of important issues spanning the cyber technology domain.

Cyber defense is based on understanding the network and its behavior. Whereas in the past mechanisms were developed that provided effective protection, there is currently a need to understand the infrastructure and communication issues in order to prevent potential attacks. The article entitled "On Network Neutrality Measurements" [Maltinsky et al. 2017] covers these aspects and the ability to identify attacks based on this information. Anomaly detection became part of the cyber domain when the ability to know about potential threats in advance seemed impossible. Creating the white list of behavior served as a way to identify the exception that may be malicious. Coping with cyber threats in the industrial world, which historically was among the most stable and defined settings, is one of the most important challenges of the cyber world today. The areas of anomaly detection and the industrial world are combined and analyzed for a defined issue in the article entitled "Automatic Construction of State chart-Based Anomaly Detection Models for Multi-Threaded Industrial Control Systems" [Kleinmann and Wool 2017].

One of the important key elements that still drives sensitive asset protection is the ability to ensure network isolation. The mobile revolution brought new challenges to the cyber arena that existing cyber security techniques were unable to cope with. The abilities of the smartphone were as advanced as any other organizational endpoints, yet defense systems have had difficulty including them in the organizational defense strategy. The article entitled "Bridging the Air Gap between Isolated Networks and

Mobile Phones in a Practical Cyber Attack" [Guri et al. 2017] brings together mobile devices and the network isolation requirement. This research is unique due to the proposed methodology, in which a single case of possible breach to an environment that was considered safe was demonstrated, thereby raising an important issue to the academic cyber community.

The users' role in cyber defense and the user as a point of vulnerability within the organizational structure has been the focus of much discussion in recent years. The user's behavior was also recognized as fundamental in differentiating between the normal and the irregular flow of actions. The article entitled "Understanding the Relationship between Human Behavior and Susceptibility to Cyber-Attacks: A Data-Driven Approach" [Ovelgonne et al. 2017] provides an in-depth investigation of the behavior side. This work leverages the data held by organizations in order to develop methodologies that analyze the data and reach relevant defense conclusions. Due to the range of potential attacks on diverse and vast amounts of assets with different levels of severity and organizational impact, the discipline of managing risks has evolved in recent years. This also reflects the inclusion of cyber as part of other organizational risks. The article entitled "A Risk-Scoring Feedback Model for Webpages and Web Users Based on Browsing Behavior" [Ben Neria et al. 2017] takes the risk discussion to the level of naïve users in the context of webpages and malware.

A significant part of the analysis tasks and operational roles will transform into smart systems in upcoming years. Conversely, specific tasks will continue to be handled by skilled individuals with the experience and knowledge to define algorithms for the unique cases. The article entitled "Optimal Scheduling of Cybersecurity Analysts for Minimizing Risk" [Ganesan et al. 2017] takes the topic of optimizing the asset of analysts and improves the contribution of this asset to organizational protection effectiveness. The question of sharing information becomes a factor when dealing with the challenge of defending entities with a wider scope within the cyber arena. Concepts and techniques that allow for the derivation of results and insights based on users' data may be valuable. The article entitled "Securely Computing a Ground Speed Model" [Kolman and Pinkas 2017] proposes a unique theory that incorporates these concepts in risk computing in the fraud industry.

While assuming that there are objective and defined truths in the cyber discipline, we realize that often the user's decisions and opinions are based on many other parameters. The paper entitled "Analyzing and Optimizing Access Control Choice Architectures in Online Social Networks" [Hirschprung et al. 2017] uses theoretical and empirical approaches for addressing the question in the evolving environment of social networks.

The cyber discipline is multidisciplinary and encompasses many domains. In this special issue, we aimed to cover a broad cross-section of topics and address some of the many important issues, challenges, and methodologies that make up the current cyber landscape. Future research in these and other areas will result in additional questions and answers, and will contribute to the evolving cyber domain.

We would like to thank the Editor in Chief Prof. Yu Zheng and the supportive special issue team. We also extend our thanks to Prof. Subramanian, who proposed the initiative, and we would like to express our deep appreciation to the reviewers for their professional contribution. Last, but not least, we extend our thanks to the authors for their collaboration and efforts.

REFERENCES

L. T. Berger and K. Iniewski. 2012. *Smart Grid: Applications, Communications, and Security*, Wiley, Hoboken, NJ, 488 pages.

R. Coppola and M. Morisio. 2016. Connected car: Technologies, issues, future trends. *ACM Computing Surveys* 49, 3, Article 46, 1–36.

R. Von Solms and J. Van Niekerk. 2013. From information security to cyber security. *Computers and Security* 38, 97–102.

J. Jang-Jaccard and S. Nepal. 2014. A. Survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences* 80, 5, 973–993.

M. Rushanan, A. Rubin, D. F. Kune, and C. M. Swanson. 2014. SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks. In *Proceedings of the 2014 IEEE Symposium on Security and Privacy*, Berkeley, CA. May 18–21, 2014. IEEE Computer Society.

A. Whitmore, A. Agarwal, and L. Xu. 2014. The Internet of Things—a survey of topics and trends. *Information Systems Frontiers* 17, 2, 261–274.

S. Sicari, A. Rizzardi, A. Grieco, and A. Coen-Porisini. 2015. Security, privacy and trust in Internet of Things: the road ahead. *Computer Networks* 76, 146–164.

A. S. Elmaghraby and M. M. Losavio. 2014. Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research* 5, 4, 491–497.

K. Ganeshkumar, D. Arivazhagan, and S. Sundaram. 2014. Advance cryptography algorithm for symmetric image encryption and decryption scheme for improving data security. *Journal of Academia and Industrial Research* 10, 2, 563.

G. Fernandes, J. J. Rodrigues, and M. L. Proenca. 2015. Autonomous profile-based anomaly detection system using principal component analysis and flow analysis. *Applied Soft Computing* 34, 513–525.

N. Jentzsch. 2015. *Horizontal and Vertical Analysis of Privacy and Cyber-Security Markets*. IPACSO White Paper Series.

N. Choucri. 2015. Explorations in Cyber International Relations: A Research Collaboration of MIT and Harvard University. MIT Political Science Department Research Paper No. 2016–1.

N. Jentzsch. 2016. State-of-the-art of the economics of cyber-security and privacy. IPACSO.

D. J. B. Svantesson. 2016. The new phenomenon of cyber law. In *Air Law, Space Law, Cyber Law—the Institute of Air and Space Law at Age,* S. Hobe (Ed.) *90* (123–135). Cologne, Germany: Carl Heymanns Verlag.

P. Aggarwal, P. Arora, and R. Ghai. 2014. Review on cyber crime and security. *International Journal of Research in Engineering and Applied Sciences* 2, 1, 48–51.

I. Kral. 2014. Shifting perceptions, shifting identities: Communication technologies and the altered social, cultural and linguistic ecology in a remote indigenous context. *The Australian Journal of Anthropology* 25, 2, 171–189.

S. Dobson, S. Denazis, A. Fernández, D. Gaïti, E. Gelenbe, F. Massacci, P. Nixon, F. Saffre, N. Schmidt and F. Zambonelli. 2006. A survey of autonomic communications. *ACM Transactions on Autonomous and Adaptive Systems* 1, 2, 226.

P. Ramuhalli, M. Halappanavar, J. Coble, and M. Dixit. 2013. *Towards a Theory of Autonomous Reconstitution of Compromised Cyber-system*s. In *IEEE International Conference on Technologies for Homeland Security*, Waltham, MA, November 12–14, 2013.

V. Mancuso, F. Funke, G. Stran, and A. Eckold. 2015. Capturing Performance in Cyber Human Supervisory Control. In *Proceedings of the Human Factors and Ergonomics Society 59th Annual Meeting*, Oak Ridge Institute for Science and Education, Air Force Research Laboratory, 321.

A. Zuiderwijk, M. Janssen, K. Poulis, and G. V. D. Kaa. 2015. Open Data for Competitive Advantage: Insights from Open Data Use by Companies. In *Proceedings of the 16th Annual International Conference on Digital Government Research*, Phoenix, AZ, May 27–30, 2015 (79–88). ACM.

W. Peters. 2015. Integrated Adaptive Cyber Defense: Integration Spiral Results. In *SafeConfig'15 Proceedings of the Workshop on Automated Decision Making for Active Cyber Defense*, October 12–16, 2015, Denver, CO, ACM.

J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, and R. Buyya. 2016. Ensuring security and privacy preservation for cloud data services. *ACM Computing Surveys* 49, 1, Article 13, 1–39.

T. Guo, U. Sharma, P. Shenoy, T. Wood, and S. Sahu. 2014. Cost-aware cloud bursting for enterprise applications. *ACM Transactions on Internet Technology* 13, 3, 10:4.

S. K. Majhi and P. Bera. 2015. A Security Enforcement Framework for Virtual Machine Migration Auction. In *SafeConfig'15 Proceedings of the Workshop on Automated Decision Making for Active Cyber Defense*, October 12–16, 2015, Denver, CO, 47–53, ACM.

D. Sgandurra and E. Lupu. 2016. Evolution of attacks, threat models, and solutions for virtualized systems, *ACM Computing Surveys* 48, 3, Article 46, 1–38.

Z. Li, W. Luo, L. Yue, and X. Wang. 2010. On the completeness of the polymorphic gate set. *ACM Transactions on Design Automation of Electronic Systems*, 15, 4 Article 32.

V. Chandola, A. Banerjee, and V. Kumar. 2009. Anomaly detection: a survey. *ACM Computing Surveys* 41, 3, Article 15, 1–58.

I. Y. Ko, H. G. Ko, A. J. Molina, and J. H. Kwon. 2016. SoIoT: toward a user-centric IoT-based service framework. *ACM Transactions on Internet Technology* 16, 2, 8:2.

H. Schaffers, Komninos Pallot, Trousse Nilsson, and Oliveira. 2011. Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation. In *Future Internet—Future Internet Assembly 2011: Achievements and Technological Promises*, Springer, New York, NY.

X. Chen, D. Zhang, L. Wang, N. Jia, Z. Kang, Y. Zhang, and H. Shiyan. 2017. Design automation for interwell connectivity estimation in petroleum cyber-physical systems. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 36, 2, 255–264.

A. Doumanoglou, J. Stria, G. Peleka, I. Mariolis, V. Petrík, A. Kargakos, and L. Wagner. 2016. Folding clothes autonomously: a complete pipeline. *IEEE Transactions on Robotics*. 32, 6.

Y. Li, K. P. Tee, R. Yan, W. L. Chan, and Y. Wu. 2016. A framework of human–robot coordination based on game theory and policy iteration. *IEEE Transactions on Robotics* 32, 6, 1408.

S. Russell, P. Norvig, and A. Intelligence. 1995. *A Modern Approach: Artificial Intelligence*. Prentice-Hall, Upper Saddle River, NJ.

Y. Yan, Y. Qian, H. Sharif, and D. Tipper. 2012. A survey on cyber security for smart grid communications. *IEEE Communications Surveys and Tutorials* 14, 4, 998–1010.

E. A. Feigenbaum. 1977. *The Art of Artificial Intelligence*. 1. Themes and case studies of knowledge engineering (No. STAN-CS-77-621). Department of Computer Science, Stanford University, Stanford, CA.

E. Blanzieri and A. Bryl. 2008. A survey of learning-based techniques of email spam filtering. *Artificial Intelligence Review* 29, 1, 63–92.

A. Maltinsky, R. Giladi, and Y. Shavitt. 2017. On network neutrality measurements. *ACM Transactions on Intelligent Systems and Technology: Special Issue on Cyber Security.* 8, 4.

E. Kolman and B. Pinkas. 2017. Securely computing a ground speed model. *ACM Transactions on Intelligent Systems and Technology: Special Issue on Cyber Security.* 8, 4.

R. Hirschprung, E. Toch, H. Schwartz-Chassidim, T. Mendel, and O. Maimon. 2017. Analyzing and optimizing access control choice architectures in online social networks, *ACM Transactions on Intelligent Systems and Technology: Special Issue on Cyber Security.* 8, 4.

A. L. Samuel. 1959. Some studies in machine learning using the game of checkers. *IBM Journal of Research and Development* 3, 3, 210–229.

M. Ben Neria, N. S. Yacovzada, and I. Ben-Gal. 2017. A risk-scoring feedback model for webpages and web users based on Browsing behavior. In *ACM Transactions on Intelligent Systems and Technology: Special Issue on Cyber Security.* 8, 4.

A. Gruber and I. Ben-Gal. 2017. Using targeted Bayesian network learning for suspect identification in communication network. *International Journal Information Security* doi:10.1007/s10207-017-0362-4.

K. He, X. Zhang, S. Ren, and J. Sun. 2016. Deep residual learning for image recognition. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, Seattle, WA, June 27–30, 2016. 770–778.

G. Hinton, L. Deng, D. Yu, G. E. Dahl, A. R. Mohamed, N. Jaitly, and B. Kingsbury. 2012. Deep neural networks for acoustic modeling in speech recognition: the shared views of four research groups. *IEEE Signal Processing Magazine*, 29, 6, 82–97.

J. Schmidhuber. 2015. Deep learning in neural networks: An overview. *Neural networks* 61, 85–117.

R. Ganesan, S. Jajodia, and H. Cam. 2017. Optimal scheduling of cybersecurity analysis for minimizing risk. *ACM Transactions on Intelligent Systems and Technology: Special Issue on Cyber Security.* 8, 4.

S. Singh and N. Singh. 2015. Internet of Things (IoT): Security Challenges, Business Opportunities & Reference Architecture for E-Commerce. In *IEEE International Conference on Green Computing and Internet of Things*, Delhi, India, October 8–10, 2015. 1577–1581.

K. Zhao and L. Ge. 2013. A survey on the Internet of Things Security. In *IEEE International Conference on Computational Intelligence and Security*, Leshan, China, December 13–15, 2013. 663–667.

D. Bekerman, B. Shapira, L. Rokach, and A. Bar. 2015. Unknown malware detection using network traffic classification. In *IEEE Conference on Communications and Network Security*, Florence, Italy, September 28–30, 2015. 134–142.

M. Bohadana, Y. Median, A. Shabtai, and Y. Elovici. 2017. Detection of unauthorized IoT devices using machine learning techniques. (Working paper).

A. Kleinmann and A. Wool. 2017. Automatic construction of statechart-based anomaly detection models for multi-threaded industrial control systems. In *ACM Transactions on Intelligent Systems and Technology: Special Issue on Cyber Security* 8, 4, 1–22.

M. Guri, M. Munitz, and Y. Elovici. 2017. Bridging the air gap between isolated networks and mobile phones in a practical cyber attack, *ACM Transactions on Intelligent Systems and Technology: Special Issue on Cyber Security.* 8, 4.

M. Ovelgonne, A. Prakash, V. S. Subrrahmanian, T. Dumitras, and B. Wang. 2017. Understanding the relationship between human behavior and susceptibility to cyber-attacks: a data-driven approach. *ACM Transactions on Intelligent Systems and Technology: Special Issue on Cyber Security.* 8, 4.

Received January 2017; revised March 2017; accepted April 2017