COMPLEX SYSTEM MODELING AND SIMULATION
ISSN 2096-9929 04/06 pp 327–342
Volume 3, Number 4, December 2023
DOI: 10.23919/CSMS.2023.0018

Complexity Science and Cyber Operations: A Literature Survey

Briant Becote* and Bhaskar Prasad Rimal

Abstract: Complexity science is an interdisciplinary scientific field that analyzes systems as holistic entities consisting of characteristics beyond the sum of a system's individual elements. This paper presents current research across the literature promoting cyber security as a complex adaptive system. We introduce complex systems concepts and fields of study, and deliver historical context, main themes, and current research relevant to cyber operations. Examples of cyber operations research leveraging agent-based modeling demonstrate the power of computational modeling grounded in complex systems principles. We discuss cyber operations as a scientific field, define current shortfalls for scientific rigor, and provide examples of how a complexity science foundation can further research and practice across a variety of cyber-based efforts. We propose standard definitions applicable to complex systems for cyber professionals and conclude with recommendations for future cyber operations research.

Key words: cybersecurity; cyberwarfare; modeling; simulation; agent-based modeling (ABM)

1 Introduction

Cyberspace is without question the battlefield of the twenty-first century, but unlike any previous war, its combatants include more than four billion civilian internet users. Cybersecurity is the ongoing effort to defend internet users and protect sensitive data. Cybersecurity researchers and practitioners develop procedures and implement patches in an effort to thwart malicious actors, but to what end? These dedicated and well-trained professionals generally operate on the defensive. The paradigm of cybersecurity is analogous to a dam that, despite best efforts, continues to spring leaks. While cybersecurity experts develop solutions for today's botnet, ransomware, and rootkit, attackers continue to create and exploit software features that become tomorrow's zero-day exploits. Given the current paradigm of playing catch up to keep up, cybersecurity will remain a responsive approach to malicious attacks unless a radical change occurs in the current approach to understanding network, information, and computer security.

This proposal is not a silver bullet solution. However, an effort must be made to establish a better foothold in combating cyber-attacks. Part of the challenge lies in the incredibly diverse and seemingly unpredictable nature of cyberspace. To better understand and, at some level, control cyberspace, researchers have begun examining cyber operations from a complexity science perspective.

The study of complexity science is a growing interdisciplinary field of research. While complexity science lacks a formal or universal definition, its key concepts include emergent phenomenon, dynamics, evolution and adaptation, collective non-deterministic behavior, and self-organization. Researchers of complex systems often find it necessary to develop simulations and models to understand and communicate the nature of a complex system effectively. Such complex systems span nearly all domains, including ecology, psychology, mathematics,

• Briant Becote is with the Technology Department, Florida State College at Jacksonville, Jacksonville, FL 32202, USA. E-mail: briant.becote@fscj.edu.
• Bhaskar Prasad Rimal is with the Department of Computer Science, University of Idaho, Moscow, ID 83844, USA. E-mail: bhaskar.rimal@ieee.org.
* To whom correspondence should be addressed.
※ This article was recommended by Associate Editor Qingshan Jia.
Manuscript received: 2023-03-16; revised: 2023-08-04; accepted: 2023-08-11

economics, and computer science. Given that the internet is a complex system and the nature of cybersecurity to safeguard its use, we believe that examining cyber operations with a complexity science perspective is an important and necessary step to producing a safe and secure internet.

There are many survey papers within the literature regarding cyber operations focused on malware attacks and analysis[1, 2], vehicle intrusion[3, 4], financial technology[5], big data[6], and industrial control systems[7] to name a limited few. To the best of our knowledge, there is no survey article dedicated to a comprehensive analysis of literature focused on complexity science and cyber operations. The aim of this paper is to fill that gap by presenting a sweeping overview of the current literary landscape. Examples across various fields are presented to illustrate complexity science principles and practices, but the primary focus is on cyber operations. We present cyber operations aligned with the principles of complexity science to achieve two critical goals: (1) to reinforce an approach to cyber operations based on a scientific paradigm, improving future research and innovation, and (2) to produce increased and actionable insight leading to a more proactive approach to securing computer networks.

A systematic literature review of text, journal, and online materials was conducted to ensure a thorough presentation of available sources. The following paragraphs present a narrative-style, general literature review, as defined by Ref. [8]. Critical analysis through cross-checking assertions and references was completed to ensure confidence.

Cyber operation is defined by a radically diverse field of both theoretical and practical applications across largely all facets of life. The following examples should be framed that considering each cyber operation is an independent complex adaptive system. It is important to observe that complexity science represents fundamental principles that are true across all complex adaptive systems. While the literature cross-section of cyber operations and complexity science is fractionally small in comparison, the examples presented below represent an essential effort to usher in increased cyber research based on complexity science principles.

The paper is structured as follows: Section 2 introduces cyber operations and complexity science, including history and terminology. Section 3 presents complexity science fields of study and tools with examples related to cyber operations. Section 4 discusses the current state of cyber operations as a science. Section 5 discusses the future of complexity science and cyber operations, and Section 6 presents our conclusion.

2 Overview of Cyber and Complexity Science

2.1 Cyber early history

Given the wide variety of contexts that broadly define cyber operations, we align the origin of cyber operations with that of the internet. Concepts of the internet evolved throughout the twentieth century, beginning with its development by the United States Department of Defense's Advanced Research Projects Agency in the 1960s. Leveraging the Transmission Control Protocol/Internet Protocol (TCP/IP) provided a common language for computer-to-computer connectivity, facilitating computer data transfer. As such, the officially recognized birthday of the internet is January 1, 1983, when Advanced Research Projects Agency Network (ARPANET) and the Defense Data Network adopted the TCP/IP protocol. Through Domain Name System (DNS), which converts IP addresses into alphabetical website addresses, the growth of internet use expanded exponentially throughout the late twentieth century. Coincidentally, home computer ownership likewise grew due to reduced costs and increased availability. But with added availability and access, greater threats and a new form of warfare arrived.

2.2 Cyber warfare

Cyber warfare is the offensive and defensive postures and actions based on securing or exploiting a cyber target. The domain encompasses the technology, networks, and tactical or strategic plans and operations designed to exploit, disrupt, or destroy information systems and the active efforts to present these attacks. Attacks can originate from a nation, state, or non-state sponsored group and continue to evolve as new threats are discovered and new techniques to eliminate threats are implemented. Cyber warfare techniques will generally follow under the following approaches:

- Espionage;
- Cyberattacks;
- Information warfare;
- Cyber sabotage;
- Cyber counterintelligence.

In addition to politically motivated attacks,

cybercriminals may exploit networks for political change or financial gain. Through the development of computer malware, rootkits, and specialized network attacks, a bad actor can exploit a software or hardware vulnerability and expose an individual or organization to loss of data, privacy, or network capability. While motivations, techniques, and objectives vary, the need for effective defense of network assets and information remains.

Like complexity science, there is often a great deal of variation in terminology across cyber research. Within the literature, offensive cyber appears synonymous with terms including cyber warfare, pen-tester, and red teaming. Additionally, there are multiple areas of study, such as network connectivity, cloud computing, communications, cyber-physical systems, cybercrime, application security, and information security (to name a few), that we assert also fall under cyber operations as a formal domain, though we recognize not exclusively. Conversely, there are fields of research that rely heavily on cyber functionality, such as artificial intelligence, social network analysis, blockchain security, and smart cities (a small few) that fall in a gray space of domain identity. We defer to experts in those fields to clearly define an appropriate primary domain for these research areas. Throughout this article, we define cyber operations as inclusive of offensive cyber, cybersecurity, and applicable internet and network-based activity.

2.3 Complexity early history

The formal study of complex systems as a modern scientific endeavor took root in the twentieth century and was established as a recognizable field of study in the 1980s[9]. Prior to that, complexity science evolved from contributions across multiple disciplines. Five areas of early study are cited as fundamental to the current state of complexity science: (1) mathematics of complexity, (2) general systems theory, (3) complex systems theory, (4) cybernetics, and (5) artificial intelligence[10]. Each of these areas has impacted the understanding of complex systems both independently and interdependently, which continues to result in definitions and applications of complexity theory that vary from one domain to the next.

The development of General System Theory (GST), founded by Austrian biologist Ludwig Von Bertalanffy was an early contributor to generalizing system analysis[11]. In the mid-20th century, Von Bertalanffy[11] identified the increased isolation of scientific fields. He also noted that despite little communication across these evolving boundaries, researchers from different domains were independently tackling challenges derived from the chaotic nature of nonlinear systems[11]. First proposed in the 1940s and then published in 1968, Von Bertalanffy's general system theory suggested that complex systems share fundamental universal principles across all domains that can be understood and mathematically modeled. His theory was rooted in examining systems characterized by autonomy, creativity, and dynamism, and has produced theoretical developments across multiple fields, including complexity, cybernetics, systems theory, and systems engineering.

Building on similar principles at the time, cybernetics and artificial intelligence produced important contributions to studying complex systems. Wiener, using the term cybernetics in his 1948 text on the subject[12], proposed that feedback loops are fundamental to learning and that such dynamic systems could be leveraged in developing machine learning. Walter Pitts, the founder of artificial intelligence, was a student of Wiener at Massachusetts Institute of Technology (MIT). Working with Wiener and Warren McCulloch, a neurophysiologist, Pitts developed computational models forwarding the concept of neural networks[13].

Through the efforts of the Santa Fe Institute (SFI) established in 1984, complexity science exposure grew across scientific domains and international borders. SFI founders and early contributors, many from the Los Alamos Laboratory, represented a swath of scientific fields, including economics, physics, biology, and chemistry. Hosting international conferences for discussion and collaboration, complex systems research quickly expanded. Notable figures such as George Cowan, Murray Gell-Mann, and David Pines laid the groundwork for the evolution of complexity science into the groundbreaking scientific field it has become today[14].

2.4 Complexity terminology

Complexity science continues to be an interdisciplinary field of research, and its definitions and applications vary from one domain to the next. Across each research field vested in understanding complexity, different terms are used to underscore the principles of complexity science, including complexity theory, complex systems analysis, system of a system, system dynamics, chaos theory, systems thinking, complex

networks, and complex adaptive systems. Nonetheless, the significance of complex systems analysis is so profound that the scientific method itself has been refined to account for the insights provided through our increased understanding of complexity science.

As a baseline for cyber operations research, we provide the following definitions to clarify complex systems terms for current and future research. The field of complexity science, or complex systems science, encompasses the entirety of complexity research and represents the domain as a whole. A complex system is a system in which interdependent elements interact to produce characteristics that define the system beyond the characteristics present when analyzing the individual elements independently. This phenomenon, known as emergence, underlines the distinction between complex systems and simple systems (elements and the system characteristics are consistent, and behavior/relationship of elements are fixed) or disparate systems (the behavior/relationship of elements within the system are not related or truly random). Regarding cyber security, Ref. [15] asserted: "A security property of a cybersystem exhibits emergent behavior if the property is not possessed by the underlying lower-level components of the cybersystem." Complex systems analysis provides a means of understanding systems beyond classical mathematical tools, such as differential equations and statistics, emphasizing the complexity and correlation of elements within the system.

Self-organization, the rise of emergence spontaneously over time, can be observed in complex adaptive systems when analyzing the element's interdependent effects on the system as a form of non-directed system evolution over time. These systems will typically adapt as their interdependent elements develop new responses based on changes within the system. Often, a complex system will be referred to as dynamic, highlighting the sometimes radical changes observed within a complex system when its nonlinear nature becomes apparent. A simple example is that of the double pendulum, the motion of which is bound by differential equations, resulting in a dynamic and chaotic track of movement.

3 Cyber Operation and Complexity Science

3.1 Fields of study

Within the scope of complexity science are different areas of study that represent the various disciplines from which they evolved. Sayama[16], director of the Center for Collective Dynamics of Complex Systems at Binghamton University, defined seven areas of focus within complexity science as topical clusters: (1) game theory, (2) nonlinear dynamics, (3) systems theory, (4) pattern formation, (5) evolution and adaptation, (6) networks, and (7) collective behavior. Adopted from Ref. [16], Fig. 1 provides a visual perspective of the various research fields related to Sayama's topical areas. The following paragraphs outline a concise introduction and correlation of the topical areas related to cyber research examples.

Behavioral game theory is a multidisciplinary field based on mathematical models representing rational or irrational decision-making across human populations. Cyber researchers utilize game theory to simulate cyber operations dynamics[17−19], adapt machine learning for cyber security[20], and as a tool for creating cybersecurity assessments[21]. Findings from Ref. [17] demonstrated the utility of a complexity science perspective in cyber research to quantify the impact of network misconfiguration across attacker types and network setups. Reference [21] highlighted the advantage of decision support gained through cyber operations complexity analysis. Recent cyber-based research contributions[22, 23] provide excellent continued reading beyond this initial introduction.

Nonlinear dynamics, popularly known as chaos theory, focuses on systems in which a change of input is not mathematically proportional to the output. Related research has aimed at understanding cyber incident frequency to improve short-term incident prediction[24], managing cyber-emergencies[25], and interpreting cyber warfare law[26]. As early as 2006, researchers positioned chaos theory to predict the outcome of cyber operations through the recognition that the average of hundreds of simulations can normalize results[25].

Systems theory research is the application of understanding and problem-solving complex systems challenges. Given this is the broadest of the complexity science areas, it can be applied across all domains; though the term is commonly used in social sciences research such as psychology, business management, and organizational behavior. Research directly related to system homeostasis (a system's steady state of equilibrium), feedback (or cybernetics, when a system's output influences the inputs), and system dynamics

Fig. 1 Complex systems topics.

(measurement of a system's change over time) are based on systems theory. Fundamentally, this is the foundation for research regarding solutions dedicated to Cyber-Physical Systems (CPS) and the Internet of Things (IoT).

Pattern formation is the recognition and research of complex systems based on self-organization into naturally occurring identifiable patterns. From pattern—formation evolved the study of cellular automata, popularized by John Conway and his "game of life" study[27]. A cellular automaton is a cellular grid bound by explicit rules defining a finite set of states and how states update over time. Cyber research has used cellular automata to calculate cybersecurity risk based on CPS[28], smart grids[29], and cascading failures[30]. The area of complex evolution and adaptation is dedicated to understanding how adaptation occurs in biological and technological systems. Specific areas tangent to cyber operations includes artificial intelligence, artificial life, and machine learning. Given the current popularity of artificial intelligence and machine learning, examples of relevant cyber research are ubiquitous throughout the literature.

The study of networks is fundamental to cyber operations; however, not all networks are complex networks. Specific areas of complex networks include dynamic networks, adaptive networks, scaling, and graph theory. A great deal of research regarding complex networks is found throughout the literature based on cyber-attacks[31, 32] as well as various areas of cybersecurity[33, 34].

The final topical cluster is collective behavior. In addition to social dynamics, collective intelligence, and synchronization, agent-based modeling is a key research area of complexity science and underlines

many cyber research articles based on complexity science. Agent-Based Modeling (ABM) simulates dynamic systems through the use of interdependent agents who influence one another and the system according to a set of predetermined rules. Agent-based modeling provides three considerable benefits: it illustrates emergent phenomena associated with complex systems, models are relatively simple to design and observe, and results can be gained quickly across many runs of the simulation. Cyber-related research includes both offensive and defensive models, which will be discussed in detail below.

3.2 Complex systems tool

Given the breadth and depth of complex systems subject matter, developing a meaningful appreciation can be aided through familiarization with the field's tools. Shalizi[35] presented a comprehensive approach to organizing complexity science tools by categorizing them into three areas based on purpose: building and understanding models, measuring complexity, and analyzing data (Fig. 2). The remainder of this section is dedicated to reviewing complex systems tools that can be leveraged in cyber operations research and performance.

Artificial Intelligence (AI) continues to experience significant growth and development across all domains, including cyber operations. Statistical learning theory is a framework for developing and evaluating algorithms and models fundamental to the prediction required for systematic learning. Although modeling complex systems may reveal system phenomena not evident with statistical analysis, statistics can still provide meaningful insight in data analysis relevant to complexity science[36].

Due to the complicated nature and number of variables in many complex systems, a valid and reliable approach to analyzing output causality can provide significant insight into the system's operations.

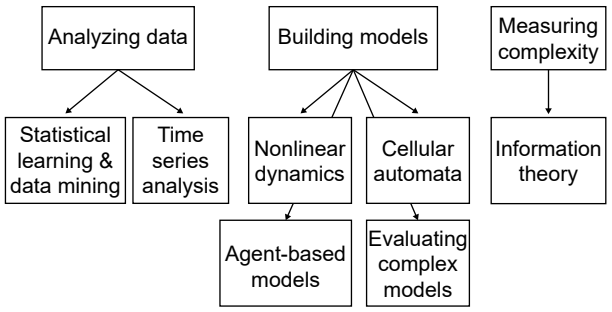

Fig. 2 Complex systems tools.

Research by Razak and Jensen[37] demonstrated the use of transfer entropy, a time series statistical model designed to analyze complex systems, as a means to infer causation from correlations that accurately forecast future values. Through the use of applicable models and tools, complex systems can be visually displayed through graphs and measured using probability models to facilitate interpreting system characteristics. As each of these areas of analysis is a field of research unto itself, we present recently published research applicable to cyber operations as a foundation for discussion.

Naturally, statistical learning is inherent in cyber research based on artificial intelligence. Throughout the literature, there are notable cyber research examples dedicated to statistical learning theory including fake website detection[38], cybersecurity and biometrics[39], and cyber threat detection[40, 41]. These examples each explicitly identify the relevant contribution statistical learning provided to developing an effective framework within a cyber context.

While there are variations on modeling complex systems, the most prominent are cellular automata, complex network models, and agent-based models. Agent-based modeling represents the most common approach of the three within the cyber literature and has significantly increased in popularity over the last twenty years as a reliable tool for analyzing and presenting complex phenomena. Based on agents that are autonomous and interactive, ABMs enable observing the complexity within a system that would otherwise be difficult to extract and understand. This approach is used in modeling phenomena across a wide range of fields including political science[42], sociology[43], economics[44], epidemiology[45, 46], biology[47], and chemistry[48]. Specific to each system and phenomenon being studied, agents may take the form of individual people, infections, fire, flooding, or independent systems[49]. Agents within an ABM may vary from a few to millions, and while initial programming defines basic agents with identical characteristics and learning rules, the variations experienced due to interactions with one another, and the environment often results in a wide variety of agent actions and system adaptation.

Information theory, specifically information fluctuation, provides a quantitative measure of complexity within a given system[50]. While an in-depth analysis is beyond the scope of this paper, a cursory introduction will help provide context to

further applicable measurements on a macroscopic scale. As presented in Ref. [51], complexity is a matter of probability, and its presence can be measured based on the states of information available, depicted in Eqs. (1) and (2):

$$I = \log N = -\log P \tag{1}$$

$$P = 1/N \tag{2}$$

where N is the number of instances, I is information, P is probability, and log is a logarithmic operation, symbolic of the reverse exponential function defined by the probability equation that represents the content of information in a complex system. The negative log P produces increased information through decreasing probability. Equation (1) can then be simplified into Eq. (2). In a complex system, order and chaos occur in variations of alternating states producing a system that at times may be either predictable or unpredictable. Reference [51] illustrated these states within a system using a diagram similar to that presented in Fig. 3. Arrows converge on the circles representing stability and order. When arrows diverge from the circle, it represents chaos. The numbers within the circles represent various potential states within the system. The arrows then have a forward conditional probability $P_{i\to j}$ and a reverse conditional probability $P_{i\leftarrow j}$ (not displayed) indicating the probability of the current state and future or past state, respectively[51].

Once the probability of a state is defined, net gain information Γ represents transitions from the present to the next state, and when balanced against the weighted mean or average using standard deviation $\langle\Gamma\rangle$ and calculated for multiple transitions, the complexity of a system can be measured using Eq. (3):

$$\Gamma_{ij} = \log P_i - \log P_j = I_j - I_i \tag{3}$$

The above introduction is only a summary based on Refs. [50, 51]. Interested readers are encouraged to review these papers for a detailed examination and illustrated examples.

3.3 Cybersecurity dynamics framework

Across the cyber-complex literature landscape, a notable and prominent contribution emerged: Xu's cybersecurity dynamics framework[52]. The following subsection outlines specifics regarding cybersecurity dynamics and its potential influence on cyber research. Recognizing the need for a formal scientific foundation in cyber research, Xu developed cybersecurity dynamics[52−54]. While the name implies a strict focus on cybersecurity, its principles and applications apply to both offensive and defensive cyber. Based on a macroscopic perspective, or macroscopic cybersecurity, Xu[52−54] applied many of the principles of complexity science including a system-level analysis, acknowledging the emergent, adaptive and dynamic nature of cyber systems, and leveraging applicable models to interpret system-level characteristics.

Within Xu's cybersecurity dynamics framework, two core principles define the scope of cybersecurity dynamics: core research objectives and the triple research axis (Fig. 4). The core research objectives are based on understanding, managing, and forecasting cyber phenomena[53]. As such, cyber dynamics drives researchers to develop descriptive, prescriptive, and predictive models. When examined holistically, each of these objectives supports and ultimately drives forward one another, providing a means to interpret and validate data observed across cyber systems. Descriptive modeling provides an abstraction and simplification of model characteristics to better grasp agent-level influences and system adaptation. Often these models are preliminary simulations designed to ensure the simplest approach to modeling system functionality. Cyber descriptive models can be used to understand attack-defense scenarios in a variety of instances including botnets[55], mobile networks[56], and organizational manufacturing[21]. Descriptive models

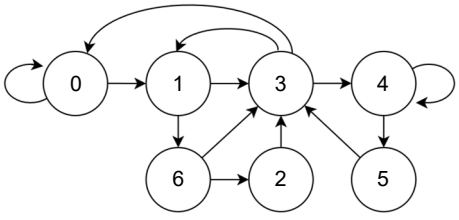

Fig. 3 Illustration of a complexity state diagram.

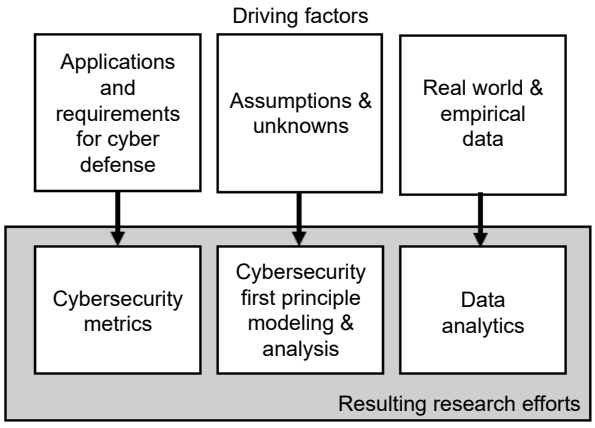

Fig. 4 Triple axis of cybersecurity dynamics research[53].

progress into prescriptive and predictive models. Prescriptive models involve the analysis of cyber datasets to assess cyber operations, and they are frequently applied in team simulations[57] and security assessments[17]. Predictive models extrapolate cyber datasets to forecast the impact that threats and security measures make on cyber operations. Through the use of prescriptive and predictive modeling, researchers can evaluate policy and validate assumptions posed through the descriptive modeling process[53].

3.4 Cyber agent-based modeling

As early as 1999, Fred Cohen, the father of computer virus defense and pioneer of network modeling[58], identified the lack of research regarding complex systems and cyber, despite applicable advantages in modeling and simulation already determined for cyber operations[58]. Citing challenges such as the complexity of cyberspace, lack of quality data, inconsistency in practice and research, and the rate of evolving technology, Cohen[58] recognized hurdles that remain true to this day. Furthering the point, Cohen[58] emphasized the shortfalls of statistical analysis, the standard modeling and simulation tool of the time, for its inability to demonstrate attacks in parallel or simulate attacks based on timing. To improve on the few previously published models simulating cyber operations, Cohen[58] actively balanced accuracy in complexity with computational performance limitations. Leveraging a cause and effect approach, Cohen[58] developed a novel model simulating attack and defense of a cyber environment approximating the time to attack and defend as a prominent characteristic. Although the model is not explicitly agent-based, attackers and defenders (or agents) are defined by various characteristics, and the cause and effect and timing-based nature of the model produce an emergent quality of the system/model in which elements of the cyber environment become more or less exposed to attack throughout the simulation. Through analysis and multiple simulations, the researchers identified a critical point within the system in which the defense of a system increases radically despite minimal increase in defender ability. They also recognized that a perfect defender does not always succeed, allowing an organization to fall victim to attacks when certain time and ability thresholds of attackers are met. Ultimately, they presented the nonlinear results of attacker success, implicitly highlighting the applicability of cyber operations to complex systems analysis and demonstrating its power through modeling and simulation.

Building from Cohen et al.'s model, cyber research applying formal agent-based modeling techniques began to grow, including influential contributions by Kotenko to include examining various attack and defense scenarios and simulating cyber-wars across the internet[59−62].

Kotenko et al.[57] followed up this research with agent-based modeling approaches to defending against botnet attacks and analyzing cooperation versus competition of teams[63] to determine how best to simulate their actions and an analysis of cyber-attack and defense for homeland security[62]. Additional agent-based modeling research analyzing cyber operation teams of note includes Refs. [64, 65].

In 2011, Grunewald et al.[66] introduced NeSSi2, an agent-based network security simulation framework designed to illustrate various attack vectors versus security solutions. Built on a three-component architecture, the framework consists of a Graphical User Interface (GUI), agent-based simulation back-end, and results' database. The framework adopted three context models: the network, attacker, and related interdependencies, and simulated attacker intent, opportunity, capability, and preferences demonstrated through attacker actions. The researchers reported successful findings when leveraging NeSSi2 to determine effective intrusion detection strategies versus malicious worm propagation. While recognizing the lack of real-world validation, the results provide insight beyond historical reference and enabled cybersecurity professionals to assess security strengths beyond the ubiquitous threat assessment frameworks solely relied on by many organizations. Further research highlighted NeSSi2's scalability, fidelity, and extendable nature[67], in addition to research on specific cyber threats such as large-scale Distributed Denial of Service (DDoS) attacks[68].

Following an analysis of the current state of cybersecurity illustrated through application whitelisting, Norman and Koehler[69] aptly illustrated the importance of applying complex scientific principles to cybersecurity to analyze and solve cyber challenges. Through the use of a fictional government, the researchers used agent-based modeling to run simulations of a fictional government conducting cybersecurity via whitelisting applications from a top-down (all programs are whitelisted with the exception of those approved for network use) versus bottom-up

(programs are whitelisted once a known vulnerability is identified) perspective. Despite expecting a top-down approach to significantly bottleneck operational productivity, the agent-based model demonstrated that the two approaches had very similar time throughput measuring organizational success via application processing times. While an exceptionally simple model, it grounded organizational decision-making regarding cybersecurity through empirical evidence rather than simply leaning on common sense or existing precedent.

Across the literary landscape, a single cyber-based performance model was identified, the Cyber-Forces Interaction Terrain (FIT) simulation framework[70]. The Cyber-FIT model is designed specifically to support military operations, modeling military forces and terrain (computer systems). Using NetLogo, an agent-based modeling software, the authors simulated three terrain types (military base, tactical, or industrial location) and cross-threaded them against three terrains (analogous to computer systems) to define three vulnerability rates (Table 1).

To implement the agents, Dobson and Carley[70] defined offensive and defensive forces. Defensive forces take action to update vulnerable terrain to secure terrain. Offensive forces conduct one of four attack standards associated with one of the terrain types (1) random - attacks all types, (2) routing protocol attack - attacks Type 1 (networking systems), (3) denial of service - attacks Type 2 (server systems), and (4) phishing - attacks Type 3 (user systems)[70]. Through running simulations, the researchers answered a series of questions regarding operational logistics such as ideal force allocation for cyber defense and impact on network security based on changes to attack scenarios.

The Cyber-FIT simulation framework represents an important significant step forward in performance modeling for cyber operations. As noted by Dobson and Carley[70], it lacks rigorous validity via empirical data (inputs do not reflect real-world values), and while the model demonstrates proof of concept, it is unable to be applied to real-world applications. Becote's cyber operations performance framework[71] builds on these developments by applying input from the Cyber Operations Self-Efficacy Scale (COSES) to reflect cyber operator behavioral characteristics while also accepting inputs regarding real-world network status and operator skills and capabilities.

Table 1 Cyber-FIT vulnerability matrix.

Terrain type	Base	Tactical	Industrial
Type 1 (networking)	Low	Medium	High
Type 2 (servers)	Low	High	Medium
Type 3 (users)	High	Medium	Low

As noted by Wilensky and Rand[72], agent-based models may be employed for the following eight use cases: (1) description, (2) explanation, (3) experimentation, (4) providing sources of analogy, (5) communication/education, (6) providing focal objects or centerpieces for scientific dialogue, (7) thought experiments, or (8) prediction. As seen across the cyber literature, each of these use cases are applicable to examining and understanding the cyber environment.

While not the only modeling and simulation framework for demonstrating complex systems, the ease with which researchers can develop, observe, and experiment with emergence compared to alternatives cannot be overstated. Researchers with little programming experience can develop agent-based models with free open-source software including NetLogo[73], Repast Suite[74], and StarLogo Nova[75]. These and additional software options with varying strengths and learning curves are available to examine and simulate cyber operations across all Operating System (OS) platforms. With a combination of community support, in-depth online tutorials, and resources such as https://www.comses.net, readers are encouraged to explore the incredible potential of computational modeling beyond the scope of this article.

3.5 Trends in research

Despite the clear applicability, cyber operations represent only a fraction of the literature based on agent-based modeling. We conducted a trends analysis through Dimensions.ai, a site dedicated to providing comprehensive data on published research. To establish context, we begin with the key phrase "complex systems" (quotes applied), where there were approximately 38 000 articles filtering for "complex systems" within the title and abstract. Figure 5 presents our findings across each year of the last decade of research (see Fig. 5a).

Due to the nature of complexity science jargon across its various domains of applied research, this surely represents a small sample of all research reflective of the subject matter. Despite this, the number of publications and applicable citations has grown on average over the last ten years, as depicted in Fig. 5.

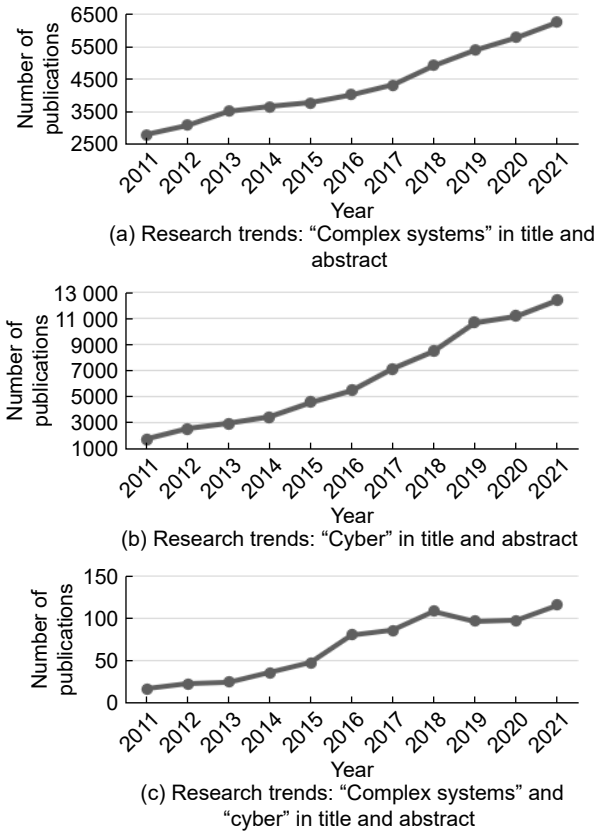

Fig. 5 Research trends across the literature. Source: Dimensions.ai.

During the same period, the term “cyber” appears in the title and abstract of just over 76 000 journal articles (Fig. 5b).

Conducting the search inclusive of both “complex systems” and “cyber”, we discovered 736 publications across the decade of research with both our terms (Fig. 5c), a small fraction of the overall literature. As was identified by reviewing the terms independently, the trend reflects a general increase in publications year over year. It is also important to note that not every article within our combined search is specific to cyber operations applied through a complexity science perspective. Ultimately, the findings indicate thousands of research articles in which either concept is central but relatively few at the intersection of both fields. When analyzing the publication source classifications, a majority of the research articles are related to artificial intelligence and information systems, with only a small fraction represented by distributed computing.

4 Cyber Operations as a Science

While modern textbooks introduce cyber operations as an applied science[76], there are notable concerns that justify arguments suggesting that cyber operation is not a science[77], or more specifically, is a proto-science[78]. Of the characteristics that define a field as scientifically rigorous, we assert that “clearly defined terminology”, “highly controlled experimental conditions”, and “reproducibility” are all elements cyber operations as a field lacks in both research and practice. Without complexity science, the overwhelming scope, scale, and variability of factors presenting across the cyber landscape make producing truly scientific experimentation incredibly challenging.

While we acknowledge that models and simulations represent only an approximation of reality, reliance on models and simulations is critical to ensuring the long-term success of cyber security, both as a means to assess current vulnerabilities and to develop and optimize cyber systems against future attacks[79].

In addition to rigorous testing and empirical evidence, science must be based on a universally agreed-upon metric for measurement. To be viable, the measurement must be both reliable and valid. Reliability ensures consistency. Validity is the degree of accuracy in specifically measuring the desired phenomenon. While numerous efforts have been made to define metrics at a microscopic scale applicable to specific research efforts, Ref. [52] produced a systemic set of metrics as part of the cybersecurity dynamics framework that represents key measurements applicable to the whole of cyber operations. Though there remains additional work to establish a comprehensive set of standardized measurements applied across the field, this research, based on key complexity science principles, establishes an important step in moving cyber operations forward as a legitimate scientific field.

5 Future of Complexity Science and Cyber

Due to the breadth of applications in research and practice in both cyber operations and complexity science, the areas for future research are plentiful. Current research based on a complexity science perspective examining cyber operations continues to grow and impact all practical applications of offensive and defensive cyber. Future research in cyber modeling and simulation will improve foresight regarding cyber-attacks. Artificial intelligence will develop new avenues for simplifying network protection and automating the identification of vulnerabilities. For

those interested in the most recent influential research and future work, Table 2 presents current advances in cyber complexity research focused within the last 12 months and broken out by the most dominant research areas. As an honorable mention a few years older, Couretas[94] provided a wealth of knowledge and examples of tools and technologies currently available for performing cyber modeling and simulation. Additionally, two more recent publications have proven meaningful in providing fresh avenues for future research opportunities. A newly published text from Pawlick and Zhu[95] outlined game theory principles specific to cyber operations and provided recommendations regarding open challenges across the field. Also, *Game Theory and Machine Learning for Cyber Security*[20], provides case study and formula-based guidance in developing a foundation in game theory and machine learning principles applicable to cyber operations. These texts, like the many others cited throughout this paper, deliver the fundamentals required to begin developing cyber tools and models while recognizing future research needs in developing solutions for current computational and incomplete information limitations.

Complexity science is not without areas for further research. As a scientific framework, it is an evolutionary leap forward in understanding system adaptation and evolution, but a variety of challenges remain, including validity and reliability testing, stakeholder understanding of model implications, and

Table 2 Recent cyber complexity research by cyber topic.

Research area	Author	Title	Year	Source	ISBN/DOI
Game theory	Chethana et al.[80]	Deep learning technique based intrusion detection in cyber-security networks	2022	*2022 IEEE 2nd Mysore Sub Section International Conference*	10.1109/MysuruCon55714.2022.9972350
	Ishii and Zhu[81] (editors)	*Security and Resilience of Control Systems: Theory and Applications*	2022	Springer, Switzerland	978-3030832353
	Benaddi et al.[82]	Robust enhancement of intrusion detection systems using deep reinforcement learning and stochastic game	2022	*IEEE Transactions on Vehicular Technology*	10.1109/TVT.2022.3186834
	Rose et al.[83]	IDERES: Intrusion detection and response system using machine learning and attack graphs	2022	*Journal of Systems Architecture*	10.1016/j.sysarc.2022.102722
Artificial intelligence	Dash et al.[84]	Threats and opportunities with AI-based cyber security intrusion detection: A review	2022	*International Journal of Software Engineering & Applications*	10.5121/ijsea.2022.13502
	Sarker et al.[85]	Internet of Things (IoT) security intelligence: A comprehensive overview, machine learning solutions and research directions	2022	*Mobile Networks and Applications*	10.1007/s11036-022-01937-3
	Aldhyani and Alkahtani[86]	Attacks to automatous vehicles: A deep learning algorithm for cybersecurity	2022	*Sensors*	10.3390/s22010360
	Alohali et al.[87]	Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment	2022	*Cognitive Neurodynamics*	10.1007/s11571-022-09780-8
	Ahmed et al.[88]	A bolckchain- and artificial intelligence-enabled smart IoT framework for sustainable city	2022	*International Journal of Intelligent systems*	10.1002/int.22852

(to be continued)

Table 2 Recent cyber complexity research by cyber topic.

(continued)

Research area	Author	Title	Year	Source	ISBN/DOI
Modeling	Ghiasi et al.[89]	A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future	2023	*Electric Power Systems Research*	10.1016/j.epsr.2022.108975
	Apruzzese et al.[90]	Modeling realistic adversarial attacks against network intrusion detection systems	2022	*Digital Threats: Research and Practice*	10.1145/3469659
	Best[91] (chapter author), Masys (editor)	Modeling and simulation for security: An overview	2022	*Handbook of Security Science*	10.1007/978-3-319-91875-4_53
	Poursoltan et al.[92]	A new modeling framework for cyber-physical and human systems	2022	*Annual Modeling and Simulation Conference*	10.23919/annsim55834.2022.9859402
	Kianpour et al.[93]	Advancing the concept of cybersecurity as a public good	2022	*Simulation Modelling Practice and Theory*	10.1016/j.simpat.2022.102493

the application of data science on large-scale models. Each of these areas directly impacts cyber operations research and practice, and dedicated efforts across both fields can help bridge current challenges and gaps in knowledge.

6 Conclusion

Given the extensive variety of topics across cyber and complexity research, the selection and breadth of references throughout this article were intentional to provide readers with avenues for additional research based on the specific area of complexity science or cyber research sought.

Though relatively young as a field, complexity science has proven a revolutionary force in understanding and interpreting the world around us. Cyber operations research and practice can employ complexity models, including time series analysis and agent-based modeling, to interpret and predict cyber operations. Cybersecurity dynamics framework[53] provides key guidance to leveraging appropriate metrics reinforcing a scientific foundation for cyber operations. The very nature of cyberspace as a dynamic and continuously evolving environment will no doubt challenge researchers to create controlled conditions for experimentation or leverage modeling to simulate real-world systems. The way forward will combine the power and capability of complex systems modeling while continuing to build a foundation for effective research and policy-making through a formal association with complexity science.

References

[1] A. D. Raju, I. Y. Abualhaol, R. S. Giagone, Y. Zhou, and S. Huang, A survey on cross-architectural IoT malware threat hunting, *IEEE Access*, vol. 9, pp. 91686–91709, 2021.

[2] M. Husák, J. Komárková, E. Bou-Harb, and P. Čeleda, Survey of attack projection, prediction, and forecasting in cyber security, *IEEE Commun. Surv. Tutor.*, vol. 21, no. 1, pp. 640–660, 2019.

[3] W. Wu, R. Li, G. Xie, J. An, Y. Bai, J. Zhou, and K. Li, A survey of intrusion detection for in-vehicle networks, *IEEE Trans. Intell. Transport. Syst.*, vol. 21, no. 3, pp. 919–933, 2020.

[4] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, and R. Das, Attacks on self-driving cars and their countermeasures: A survey, *IEEE Access*, vol. 8, pp. 207308–207342, 2020.

[5] S. Mehrban, M. W. Nadeem, M. Hussain, M. M. Ahmed, O. Hakeem, S. Saqib, M. L. M. Kiah, F. Abbas, M. Hassan, and M. A. Khan, Towards secure FinTech: A survey, taxonomy, and open research challenges, *IEEE Access*, vol. 8, pp. 23391–23406, 2020.

[6] R. Atat, L. Liu, J. Wu, G. Li, C. Ye, and Y. Yang, Big data meet cyber-physical systems: A panoramic survey, *IEEE Access*, vol. 6, pp. 73603–73636, 2018.

[7] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan,

and N. Meskin, Cybersecurity for industrial control systems: A survey, *Comput. Secur.*, vol. 89, p. 101677, 2020.

[8] A. J. Onwuegbuzie and R. Frels, *Seven Steps to a Comprehensive Literature Review: A Multimodal and Cultural Approach*. Los Angeles, CA, USA: SAGE Publications Ltd, 2016.

[9] A. B. Downey, *Think Complexity: Complexity Science and Computational Modeling, 2nd edition*. Boston, MA, USA: O'Reilly Media, 2018.

[10] B. Castellani and F. W. Hafferty, *Sociology and Complexity Science: A New Field of Inquiry*. Berlin, Germany: Springer Berlin Heidelberg, 2009.

[11] L. Von Bertalanffy, *General System Theory: Foundations, Development, Applications, Revised edition*. New York, NY, USA: George Braziller Inc., 1968.

[12] N. Wiener, *Cybernetics: Or Control and Communication in the Animal and the Machine* (*Second Edition*). Cambridge, MA, USA: MIT Press, 1948.

[13] B. Macukow, Neural networks–State of art, brief history, basic models and architecture, https://doi.org/10.1007/978-3-319-45378-1_1, 2016.

[14] G. A. Cowan, *Manhattan Project to the Santa Fe Institute: The Memoirs of George A. Cowan*. Albuquerque, NM, USA: University of New Mexico Press, 2010.

[15] S. Xu, Emergent behavior in cybersecurity, in *Proc. 2014 Symp. and Bootcamp on the Science of Security*, Raleigh, NC, USA, 2014, pp. 1–2.

[16] H. Sayama, *Introduction to the Modeling and Analysis of Complex Systems*. Albany, NY, USA: Open SUNY Textbooks, 2015.

[17] S. Moskal, S. J. Yang, and M. E. Kuhl, Cyber threat assessment via attack scenario simulation using an integrated adversary and network modeling approach, *J. Def. Model. Simul. Appl. Methodol. Technol.*, vol. 15, no. 1, pp. 13–29, 2018.

[18] A. Attiah, M. Chatterjee, and C. C. Zou, A game theoretic approach to model cyber attack and defense strategies, in *Proc. 2018 IEEE Int. Conf. Communications* (*ICC*), Kansas City, MO, USA, 2018, pp. 1–7.

[19] R. Mitchell and B. Healy, A game theoretic model of computer network exploitation campaigns, in *Proc. 2018 IEEE 8th Annual Computing and Communication Workshop and Conference* (*CCWC*), Las Vegas, NV, USA, 2018, pp. 431–438.

[20] C. A. Kamhoua, C. D. Kiekintveld, F. Fang, and Q. Zhu, eds., *Game Theory and Machine Learning for Cyber Security*. Hoboken, NJ, USA: Wiley, 2021.

[21] A. Zarreh, C. Saygin, H. Wan, Y. Lee, and A. Bracho, A game theory based cybersecurity assessment model for advanced manufacturing systems, *Procedia Manuf.*, vol. 26, pp. 1255–1264, 2018.

[22] A. Iqbal, L. J. Gunn, M. Guo, M. Ali Babar, and D. Abbott, Game theoretical modelling of network/ cybersecurity, *IEEE Access*, vol. 7, pp. 154167–154179, 2019.

[23] A. E. Chukwudi, E. Udoka, and I. Charles, Game theory basics and its application in cyber security, *Adv. Wirel. Commun. Netw.*, vol. 3, no. 4, pp. 45–49, 2017.

[24] A. Mcleod, C. A. Dorantes, and G. B. Dietrich, Modeling security vulnerabilities using chaos theory: Discovering order, structure and patterns from chaotic behavior in complex systems, presented at the 7th Annual Security Conference, Las Vegas, NV, USA, 2008.

[25] C. A. Dorantes, A. J. McLeod, and G. B. Dietrich, Cyber-emergencies: What managers can learn from complex systems and chaos theory, in *Proc. 12th Americas Conference on Information Systems* (*AMCIS 2006*), Acapulco, Mexico, 2006, pp. 1563–1573.

[26] D. Garrie and M. Simonova, A keystroke causes a tornado: Applying chaos theory to international cyber warfare law, *Brooklyn Journal of International Law*, vol. 45, no. 2, p. 497, 2020.

[27] M. Gardner, Mathematical games—The fantastic combinations of John Conway's new solitaire game "life", *Sci. Am.*, vol. 223, no. 4, pp. 120–123, 1970.

[28] H. Qin, D. Liu, and J. Weng, Cellular automata based cyber risk conduction mechanism of cyber physical power systems, in *Proc. 2020 IEEE Sustainable Power and Energy Conference* (*iSPEC*), Chengdu, China, 2020, pp. 1672–1677.

[29] G. Cisotto and L. Badia, Cyber security of smart grids modeled through epidemic models in cellular automata, in *Proc. 2016 IEEE 17th Int. Symp. on A World of Wireless, Mobile and Multimedia Networks* (*WoWMoM*), Coimbra, Portugal, 2016, pp. 1–6.

[30] J. Zhang, X. Xiong, Y. Wang, and J. Zhang, Simulation model for cascading failure in complex network: A cellular automata approach, in *Proc. 2nd World Symp. on Software Engineering*, Chengdu, China, 2020, pp. 274–277.

[31] K. Shi, J. Wang, S. Zhong, Y. Tang, and J. Cheng, Hybrid-driven finite-time H_∞ sampling synchronization control for coupling memory complex networks with stochastic cyber attacks, *Neurocomputing*, vol. 387, pp. 241–254, 2020.

[32] R. Pan, Y. Tan, D. Du, and S. Fei, Adaptive event-triggered synchronization control for complex networks with quantization and cyber-attacks, *Neurocomputing*, vol. 382, pp. 249–258, 2020.

[33] D. Ionică, N. Popescu, D. Popescu, and F. Pop, Cyber defence capabilities in complex networks, in *Internet of Everything*, B. Di Martino, K. C. Li, L. T. Yang, and A. Esposito, eds. Singapore: Springer, 2018, pp. 217–231.

[34] G. Wen, W. Yu, X. Yu, and J. Lü, Complex cyber-physical networks: From cybersecurity to security control, *J. Syst. Sci. Complex.*, vol. 30, no. 1, pp. 46–67, 2017.

[35] C. R. Shalizi, Methods and techniques of complex systems science: An overview, in *Complex Systems Science in Biomedicine*, T. S. Deisboeck and J. Y. Kresh, eds. Boston, MA, USA: Springer, 2006, pp. 33–114.

[36] T. Mary-Huard and S. Robin, Introduction to statistical methods for complex systems, in *Handbook of Statistical Systems Biology*, M. P. H. Stumpf, D. J. Balding, and M. Girolami, eds. Chichester, UK: John Wiley & Sons, Ltd,

2011, pp. 15–38.

[37] F. A. Razak and H. J. Jensen, Quantifying 'causality' in complex systems: Understanding transfer entropy, *PLoS One*, vol. 9, no. 6, p. e99462, 2014.

[38] A. Abbasi, Z. Zhang, D. Zimbra, H. Chen, and J. F. Nunamaker, Detecting fake websites: The contribution of statistical learning theory, *MIS Q.*, vol. 34, no. 3, pp. 435–461, 2010.

[39] J. Kour, M. Hanmandlu, and A. Q. Ansari, Biometrics in cyber security, *Def. Sc. J.*, vol. 66, no. 6, pp. 600–604, 2016.

[40] J. Ashraf, M. Keshk, N. Moustafa, M. Abdel-Basset, H. Khurshid, A. D. Bakhshi, and R. R. Mostafa, IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities, *Sustain. Cities Soc.*, vol. 72, p. 103041, 2021.

[41] K. Pei, Bridging statistical learning and formal reasoning for cyber-attack detection, MS dissertation, Department of Computer Science, Purdue University, West Lafayette, IN, USA, 2016.

[42] S. de Marchi and S. E. Page, Agent-based models, *Annu. Rev. Polit. Sci.*, vol. 17, pp. 1–20, 2014.

[43] M. W. Macy and R. Willer, From factors to actors: Computational sociology and agent-based modeling, *Annu. Rev. Sociol.*, vol. 28, pp. 143–166, 2002.

[44] F. Chávez-Juárez, On the role of agent-based modeling in the theory of development economics, *Rev. Dev. Econ.*, vol. 21, no. 3, pp. 713–730, 2017.

[45] A. M. El-Sayed, P. Scarborough, L. Seemann, and S. Galea, Social network analysis and agent-based modeling in social epidemiology, *Epidemiol. Perspect. Innov.*, vol. 9, no. 1, p. 1, 2012.

[46] S. Galea, M. Riddle, and G. A. Kaplan, Causal thinking and complex system approaches in epidemiology, *Int. J. Epidemiol.*, vol. 39, no. 1, pp. 97–106, 2010.

[47] Ş. Bora and S. Emek, Agent-based modeling and simulation of biological systems, in *Modeling and Computer Simulation*, D. Cvetković, ed. London, UK: IntechOpen, 2018, pp. 29−43.

[48] A. Troisi, V. Wong, and M. A. Ratner, An agent-based approach for modeling molecular self-organization, *Proc. Natl. Acad. Sci. USA*, vol. 102, no. 2, pp. 255–260, 2005.

[49] CoMSES, Computational model library, https://www.comses.net/codebases/, 2021.

[50] J. E. Bates and H. K. Shepard, Measuring complexity using information fluctuation, *Phys. Lett. A*, vol. 172, no. 6, pp. 416–425, 1993.

[51] J. Bates, Measuring complexity using information fluctuation: A tutorial, https://www.researchgate.net/publication/340284677_Measuring_complexity_using_information_fluctuation_a_tutorial, 2020.

[52] S. Xu, Cybersecurity dynamics: A foundation for the science of cybersecurity, in *Proactive and Dynamic Network Defense*, C. Wang and Z. Lu, eds. Cham, Switzerland: Springer, 2019, pp. 1–31.

[53] S. Xu, The cybersecurity dynamics way of thinking and landscape, in *Proc. 7th ACM Workshop on Moving Target Defense*, Virtual Event, USA, 2020, pp. 69–80.

[54] S. Xu, Cybersecurity dynamics, in *Proc. 2014 Symp. and Bootcamp on the Science of Security*, Raleigh, NC, USA, 2014, pp. 1–2.

[55] I. Kotenko, A. Konovalov, and A. Shorov, Simulation of botnets: Agent-based approach, in *Intelligent Distributed Computing IV*, M. Essaaidi, M. Malgeri, and C. Badica, eds. Berlin, Germany: Springer, 2010, pp. 247–252.

[56] B. Thompson and J. Morris-King, An agent-based modeling framework for cybersecurity in mobile tactical networks, *J. Def. Model. Simul. Appl. Methodol. Technol.*, vol. 15, no. 2, pp. 205–218, 2018.

[57] I. Kotenko, Simulation of agent teams: Application of a domain independent framework to computer network security, in *Proc. 23rd European Conference on Modelling and Simulation* (*ECMS 2009*), Mondragon, Spain, 2009, pp. 1–7.

[58] F. Cohen, Simulating cyber attacks, defences, and consequences, *Comput. Secur.*, vol. 18, no. 6, pp. 479–518, 1999.

[59] I. Kotenko and E. Man'kov, Experiments with simulation of attacks against computer networks, in *Computer Network Security*, V. Gorodetsky, L. Popyack, and V. Skormin, eds. Berlin, Germany: Springer, 2003, pp. 183–194.

[60] I. Kotenko, Teamwork of hackers-agents: Modeling and simulation of coordinated distributed attacks on computer networks, in *Multi-Agent Systems and Applications III*, V. Mařík, M. Pěchouček, and J. Müller, eds. Berlin, Germany: Springer, 2003, pp. 464–474.

[61] I. Kotenko, Agent-based modeling and simulation of cyber-warfare between malefactors and security agents in Internet, in *Proc. Simul. Wider Eur. - 19th Eur. Conf. Model. Simul. ECMS 2005*, Riga, Latvia, 2005, pp. 533–543.

[62] I. Kotenko, Multi-agent modelling and simulation of cyber-attacks and cyber-defense for homeland security, in *Proc. 2007 4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, Dortmund, Germany, 2007, pp. 614–619.

[63] A. M. Konovalov, I. V. Kotenko, and A. V. Shorov, Simulation-based study of botnets and defense mechanisms against them, *J. Comput. Syst. Sci. Int.*, vol. 52, no. 1, pp. 43–65, 2013.

[64] K. Sycara and M. Lewis, Agent-based approaches to dynamic team simulation, in *Navy Personnel Research, Studies, and Technology Division Bureau of Naval Personnel*, https://apps.dtic.mil/sti/pdfs/ADA487741.pdf, 2008.

[65] P. Rajivan, M. A. Janssen, and N. J. Cooke, Agent-based model of a cyber security defense analyst team, *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 57, no. 1, pp. 314–318, 2013.

[66] D. Grunewald, M. Lützenberger, J. Chinnow, R. Bye, K. Bsufka, and S. Albayrak, Agent-based network security simulation, in *Proc. 10th Int. Conf. Autonomous Agents*

and Multiagent Systems, Taipei, China, 2011, pp. 1325–1326.

[67] Y. Zhao, Y. Wang, H. Zhang, C. Zhang, and C. Yang, Agent-based network security simulator Nessi2, https://api.semanticscholar.org/CorpusID:61933384, 2015.

[68] A. Kosowski and V. Mosorov, Nessi2 simulator for large-scale DDoS attack analysis, in *Proc. Perspective Technologies and Methods in MEMS Design*, Polyana, Ukraine, 2011, pp. 157–159.

[69] M. D. Norman and M. T. K. Koehler, Cyber defense as a complex adaptive system: A model-based approach to strategic policy design, in *Proc. 2017 Int. Conf. The Computational Social Science Society of the Americas*, Santa Fe, NM, USA, 2017, p. 17.

[70] G. B. Dobson and K. M. Carley, Cyber-FIT: An agent-based modelling approach to simulating cyber warfare, in *Social, Cultural, and Behavioral Modeling*, D. Lee, Y. Lin, N. Osgood, and R. Thomson, eds. Cham, Switzerland: Springer International Publishing, 2017, pp. 139–148.

[71] B. Becote, Defining a cyber operations performance framework via computational modeling, PhD dissertation, Department of Computer and Cyber Sciences, Dakota State University, Madison, SD, USA, 2023.

[72] U. Wilensky and W. Rand, *An Introduction to Agent-Based Modeling: Modeling Natural, Social, and Engineered Complex Systems with NetLogo*. Cambridge, MA, USA: MIT Press, 2015.

[73] NetLogo home page, http://ccl.northwestern.edu/netlogo, 2016.

[74] Repast Suite documentation, https://repast.github.io/index.html, 2021.

[75] StarLogo Nova, https://www.slnova.org/, 2022.

[76] J. Dykstra, *Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems*. Sebastopol, CA, USA: O'Reilly Media, 2016.

[77] A. Kott, Towards fundamental science of cyber security, in *Network Science and Cybersecurity*, R. E. Pino, ed. New York, NY, USA: Springer, 2013, pp. 1–13.

[78] E. N. Hatleback, The protoscience of cybersecurity, *J. Def. Model. Simul. Appl. Methodol. Technol.*, vol. 15, no. 1, pp. 5–12, 2018.

[79] A. Kott, The significance of model-driven paradigms in cyber security: An introduction, *J. Def. Model. Simul. Appl. Methodol. Technol.*, vol. 15, no. 1, pp. 3–4, 2018.

[80] C. Chethana, P. K. Pareek, V. H. Costa de Albuquerque, A. Khanna, and D. Gupta, Deep learning technique based intrusion detection in cyber-security networks, in *Proc. 2022 IEEE 2nd Mysore Sub Section Int. Conference* (*MysuruCon*), Mysuru, India, 2022, pp. 1–7.

[81] H. Ishii and Q. Zhu, *Security and Resilience of Control Systems*: *Theory and Applications*. Cham, Switzerland: Springer, 2022.

[82] H. Benaddi, K. Ibrahimi, A. Benslimane, M. Jouhari, and J. Qadir, Robust enhancement of intrusion detection systems using deep reinforcement learning and stochastic game, *IEEE Trans. Veh. Technol.*, vol. 71, no. 10, pp. 11089–11102, 2022.

[83] J. R. Rose, M. Swann, K. P. Grammatikakis, I. Koufos, G. Bendiab, S. Shiaeles, and N. Kolokotronis, IDERES: Intrusion detection and response system using machine learning and attack graphs, *J. Syst. Archit.*, vol. 131, p. 102722, 2022.

[84] B. Dash, M. F. Ansari, P. Sharma, and A. Ali, Threats and opportunities with AI-based cyber security intrusion detection: A review, *Int. J. Softw. Eng. Appl.*, vol. 13, no. 5, pp. 13–21, 2022.

[85] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, Internet of Things (IoT) security intelligence: A comprehensive overview, machine learning solutions and research directions, *Mob. Netw. Appl.*, doi: 10.1007/s11036-022-01937-3.

[86] T. H. H. Aldhyani and H. Alkahtani, Attacks to automatous vehicles: A deep learning algorithm for cybersecurity, *Sensors*, vol. 22, no. 1, p. 360, 2022.

[87] M. A. Alohali, F. N. Al-Wesabi, A. M. Hilal, S. Goel, D. Gupta, and A. Khanna, Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment, *Cogn. Neurodyn.*, vol. 16, no. 5, pp. 1045–1057, 2022.

[88] I. Ahmed, Y. Zhang, G. Jeon, W. Lin, M. R. Khosravi, and L. Qi, A blockchain- and artificial intelligence-enabled smart IoT framework for sustainable city, *Int. J. Intell. Syst.*, vol. 37, no. 9, pp. 6493–6507, 2022.

[89] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future, *Electr. Power Syst. Res.*, vol. 215, p. 108975, 2023.

[90] G. Apruzzese, M. Andreolini, L. Ferretti, M. Marchetti, and M. Colajanni, Modeling realistic adversarial attacks against network intrusion detection systems, *Digit. Threats Res. Pract.*, vol. 3, no. 3, p. 31, 2022.

[91] E. Best, Modeling and simulation for security: An overview, in *Handbook of Security Science*, A. J. Masys, ed. Cham, Switzerland: Springer International Publishing, 2022, pp. 447–458.

[92] M. Poursoltan, N. Pinède, B. Vallespir, and M. K. Traore, A new modeling framework for cyber-physical and human systems, in *Proc. 2022 Annual Modeling and Simulation Conference* (*ANNSIM*), San Diego, CA, USA, 2022, pp. 90–101.

[93] M. Kianpour, S. J. Kowalski, and H. Øverby, Advancing the concept of cybersecurity as a public good, *Simul. Model. Pract. Theory*, vol. 116, p. 102493, 2022.

[94] J. M. Couretas, *An Introduction to Cyber Modeling and Simulation*. Hoboken, NJ, USA: Wiley, 2018.

[95] J. Pawlick and Q. Zhu, *Game Theory for Cyber Deception: From Theory to Applications*. Cham, Switzerland: Springer International Publishing, 2021.

Briant Becote received the MS degree in computer science from DePaul University, Chicago, IL, USA in 2017, the Master of Arts (MA) degree in industrial organization psychology from Northcentral University, Scottsdale, AZ, USA in 2010, and the PhD degree in cyber operations from Dakota State University, Madison, SD, USA in 2023. He is an adjunct professor at Florida State College at Jacksonville, USA, while serving as a naval officer in the United States Navy. His research interests are in cyberpsychology and complexity science.

Bhaskar Prasad Rimal received the PhD degree in telecommunications engineering from University of Quebec, Quebec City, Canada, in 2017. He is an assistant professor at University of Idaho, Moscow, USA. He was previously an assistant professor of computer and cyber sciences at Dakota State University, Madison, SD, USA. He currently serves as a technical editor for the *IEEE Network* and an associate editor for the *IEEE Access* journals. He is a senior member of IEEE and ACM.