Artificial Intelligence in Cybersecurity

Nadine Wirkuttis and Hadas Klein

Cybersecurity arguably is the discipline that could benefit most from the introduction of artificial intelligence (AI). Where conventional security systems might be slow and insufficient, artificial intelligence techniques can improve their overall security performance and provide better protection from an increasing number of sophisticated cyber threats. Beside the great opportunities attributed to AI within cybersecurity, its use has justified risks and concerns. To further increase the maturity of cybersecurity, a holistic view of organizations' cyber environment is required in which AI is combined with human insight, since neither people nor AI alone has proven overall success in this sphere. Thus, socially responsible use of AI techniques will be essential to further mitigate related risks and concerns.

Keywords: cybersecurity, artificial intelligence (AI), security intelligence, Integrated Security Approach (ISA), cyber kill chain

Introduction

Since 1988, when the first denial-of-service (DoS) attack was launched,[1] the sophistication, number, and impact of cyberattacks have increased significantly. As cyberattacks have become more targeted and powerful so have cybersecurity countermeasures. While the first security tool was limited to spotting signatures of viruses and preventing their execution, today we find solutions that are designed to provide holistic protection against a wide range

Nadine Wirkuttis is a PhD candidate at the Okinawa Institute of Science and Technology Graduate University and former research intern in the Cyber Security Program at the Institute for National Security Studies. Hadas Klein is the Cyber Security Program Manager at the Institute for National Security Studies.

of attack types and a variety of target systems; nevertheless, it has become increasingly challenging to protect information assets in the virtual world.

To implement resilient and continuous protection, security systems need to constantly adjust to changing environments, threats, and actors involved in the cyber play. Cyber reality, however, appears somewhat different. Security approaches are regularly tailored to known attacks, and due to a lack of flexibility and robustness, security systems typically are unable to adapt automatically to changes in their surroundings. Even with human interaction, adaption processes are likely to be slow and insufficient.[2]

Due to their flexible and adaptable system behavior, artificial intelligence (AI) techniques can help overcome various shortcomings of today's cybersecurity tools.[3] Although AI has already greatly improved cybersecurity,[4] there are also serious concerns. Some view AI as an emerging existential risk for humanity.[5] Accordingly, scientists and legal experts have expressed alarm at the increasing role that autonomous AI entities are playing in cyberspace and have raised concerns about their ethical justifiability.[6]

The purpose of this work is to highlight the shortcomings of traditional security measures as well as the progress that has been made so far by applying AI techniques to cybersecurity. In addition, this work summarizes the risks and concerns linked to this development, by exploring AI's status quo, addressing present concerns, and outlining directions for the future.

Challenges of Today's Cybersecurity

Although awareness of cyber threats has increased; large amounts of money has been invested; and efforts are being made to fight cybercrimes, the ability of organizations to sufficiently protect their own virtual assets is not yet known.[7] The involved parties in cyberspace range from single individuals, private organizations, non-state actors to governmental organizations, all aiming to protect their cyber assets, attack those of others, or both. In addition, the sources of cyber threats are manifold: cyber threats basically arise from potential malicious acts due to financial, political, or military reasons.[8]

However heterogeneous and dynamic the nature of cyberspace might be, certain similarities of attacks and their countermeasures can be used to describe and allow for a holistic security framework. Most cyberattacks follow certain attack phases that can be described as a **cyber kill chain**.[9] This framework assumes that every attack sequence starts with a **reconnaissance** phase**,** in

which an attacker tries to locate gaps and vulnerabilities of a target system. The **weaponizing** phase follows, during which the uncovered weaknesses are used to develop targeted malicious code. This is followed by the **delivery** phase when the malware is transferred to the potential target. After the malware is delivered successfully, the **exploit** phase occurs during which the malware triggers the installation of an intruder's code. Afterwards, the compromised host system allows the establishment of a command and control channel so that the attacker can initiate malicious actions. Counteractions can be determined depending upon where a malicious action appears in the cyber kill chain.

The **integrated security approach**[10] (ISA) provides key ideas for a holistic view on cyber defense and a framework for such categorization. The main aim of the ISA is to generate **early warnings**, or alarms, preferably before the attack is launched (before the exploit phase**)**. The alarm is supposed to generate a relevant warning message that translates newly gathered threat data into actionable tasks. By this means, the message further supports the selection of countermeasures or already contains dedicated counteractions to prevent organizations from being victims of an attack. If an intrusion can not be prevented in advance, the extent of the attack must be detected, followed respectively by reaction and response. These measures should include actions to stop or counterattack the invader, in addition to defining recovery procedures to quickly rollback the system to its initial state.

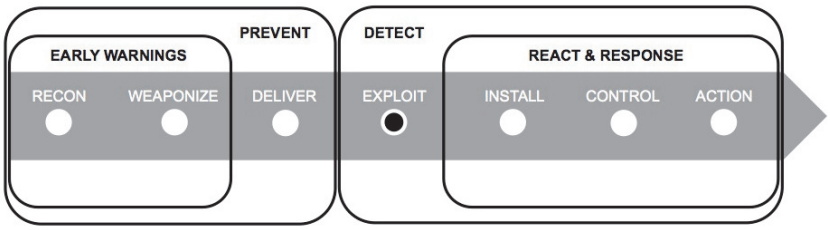

Figure 1: Cyber kill chain phases encapsulated in countermeasures of the integrated security approach

Figure 1 above depicts the interconnection of cyberattacks, described by the cyber kill chain, with their countermeasures, covered by the ISA. The diagram depicts the cyber kill chain, here visualized as the gray arrow in the center, encapsulated by the ISA. The cyber kill chain includes the seven

phases of a cyberattack, whereas the ISA consists of four counteraction phases. For detecting and blocking attacks as early as possible, all attack phases of the cyber kill chain need to be considered within the comprehensive ISA framework.[11] As stated above, the emphasis is on preventing attack and detecting malicious activities during the first three phases of an intrusion, here visualized as recon, weaponize, and deliver on the left side of the diagram within the gray arrow. After the attack—depicted as exploit in the center of the arrow—the ISA measures detection, reaction, and response necessary to interfere with the compromising malicious activities.

The complex and dynamic nature of cyberspace leads to various strategic and technological challenges that hinder and complicate an organization's ability to protect itself sufficiently in this virtual environment. These challenges comprise data acquisition, technology driven matters, as well as shortcomings in regulation and process management.

Challenges in Gathering Cyber Intelligence

The fact that perpetrators leave tracks when attempting to attack a potential target system is the key to better understanding an attacker. Consequently, an ISA with its holistic view of an organization's security requires gathering and analysis of a range of information for gaining cyber intelligence.[12] There are challenges, however, in acquiring relevant data as well as in processing, analyzing, and using it. Therefore, related efforts to effectively prevent, detect, and respond to malicious intrusions are regularly aided by security tools that aim to automate supporting security processes. The main **challenges in acquiring relevant data tracks** are:[13]

a. Amount of data: The amount of data has increased exponentially since electronic devices and their use has become ubiquitous in our work and daily lives. For the implementation of an ISA, data from all systems across entire organizations may need to be considered.
b. Heterogeneity of data and their sources: The variance in data and its sources makes it difficult to identify and collect those data; moreover, both are spread across organizational and national borders. Even if the relevant heterogeneity within the cyber environment is identified, topology and behavior of systems and networks may change and, thus, require constant adaption.

c. High data velocity: The high rate at which data is produced and processed within its sources leads to challenges in data storing and processing, which, in turn, is essential for subsequent analysis.

When it comes to processing, analyzing, and using the acquired date, **intrusion detection prevention systems** (IDPS) have proved to be an invaluable tool for cybersecurity,[14] one of many in today's cybersecurity arsenal. An IDPS is either software or hardware configured to protect single systems or entire networks. There are two main principles for IDPSs: the **misuse detection** approach, which identifies malicious activities by defining patterns of abnormal network and/or system behavior, and the **anomaly detection** approach, which is based on defining patterns of normal network and/or system behavior. Security experts define both patterns, mainly based on their experiences plus their prior knowledge of cyber threats.[15]

Cyber reality, however, is a highly complex and dynamic nature; new threats appear constantly, and attacks are specifically tailored to circumvent known protection scenarios. While the desired characteristics of IDPSs are optimized performance, maximum protection, and minimum error,[16] traditional security systems are no longer able to fully fulfill these requirements. The most **critical technological weaknesses** are:[17]

a. Low detection rate: Any inaccuracy in defining patterns of abnormal or normal network and/or system behavior may affect the IDPS's detection rate. The continuously changing network environment makes this task even more challenging. Errors in defining abnormal patterns can lead to high false negative detection rates. Here, the malicious network activities of attempted attacks are not detected in advance because a non-malicious network behavior was assumed instead. By contrast, erroneous definition of normal patterns can cause high false positive rates, causing non-malicious network activities to be categorized as malicious.
b. Slow throughput: IDPSs can show limitations in processing and analyzing gigabits of data per second. Mechanisms that address this issue are based mainly on the distribution of data processing and, thus, can further affect the system's operation, maintenance, and related costs.
c. Lack of scalability and resilience: Cyber environments are dynamic. Infrastructures and network traffic change and expand constantly, and vast amounts of heterogeneous data needs to be processed and analyzed. These dynamics further lead to performance issues and a loss of efficiency,

as IDPSs might be not able to provide and maintain their functionalities when coping with these dynamics.

d. Lack of automation: IDPSs are not yet able to adapt automatically to changes in their environment. This can result in the need for individual analysis of log data; the manual readjustment of systems to changes in the network environment; or for experts to determine the appropriate reaction for every individual warning message. This lack of automation results in a constant need for human supervision, and causes delays as well as an overhead in costs and resources.

Due to the technological challenges, organizations may face security deficits at some point; they may use several security systems or purchase security intelligence, in terms of security consulting, through third-party providers.[18]

Additional Challenges

Besides the comprehensive acquisition of data and the use of solid security technologies for protecting the full range of information in a timely manner, supporting processes also need to be considered. The establishment and maintenance of these processes is as important as data acquisition and the use of appropriate security technologies. Inter-organizational as well as intra-organizational processes can help to further improve and maintain organizations' ISAs, in addition to increasing their cybersecurity maturity level.[19] Furthermore, the creation of a so-called **cyber ecosystem**[20] encourages partnerships between diverse actors across the cyber landscape that aim to address and share security threats, experience, or resources.

Organizations operating in different sectors also tend to have inconsistent demands of cybersecurity. These differences can correspond to heterogeneous security requirements as well as varying responses when facing similar cyberattacks.[21] In cases where organizations need to protect critical infrastructures, such as water treatment or nuclear power plants, they focus on increased security rather than on financial aspects. In comparison, private organizations tend to focus on financial losses and do not give too much importance to endangering public safety.[22]

These are only some of the challenges that trouble organizations when setting up their security strategy. Given the important role of security systems in this context, the following section will focus on the technological measures.

Intelligent Techniques to Facilitate Security Measures

In tackling intelligence-gathering issues for cybersecurity, intelligent machines show promise of improving today's security measures. Intelligent machines can perform some human cognitive abilities (ability to learn or reason) as well as having sensory functions (ability to hear or see). These machines exhibit what we could call **intelligence**.[23] Such artificial intelligence enables machines to behave intelligently and imitate human intelligence—albeit to a limited extent.

The development of intelligent systems, either software or hardware, provides methods to solve complex problems—problems that could not be solved without applying some intelligence.[24] Whereas traditional computer systems are based on fixed algorithms[25] and require known data formats for decision making, the computer science discipline of AI developed flexible techniques, such as the recently revived approach of deep neural networks, that enables machines to learn[26] and adapt automatically to the dynamics of their environment. In cyberspace, this may include the automatic adaption to heterogeneous data formats, changing data sources, or noise[27] in cyber activities.

In the realm of AI, cybersecurity arguably is the industry that could benefit most from the introduction of machine intelligence; furthermore, the challenges of conventional security systems are supposed to be overcome by using autonomous AI systems.[28] Consequently, the issues in data acquisition (amount, heterogeneity, and velocity of data) as well as the problems of the related tools (low detection rate, slow throughput, a lack of scalability and resilience, and a lack of automation) could be mitigated through AI. Thus, efficiency and the effectiveness of cybersecurity and its respective tools could be improved.

The field of AI has developed and is still developing numerous techniques to address intelligent system behavior, and many have been established already in the field of cybersecurity. These systems can therefore handle and analyze vast amounts of information within a reasonable time frame and in the event of an attempted attack, can analyze the information and select dedicated counteractions. Possible scenarios, where AI techniques are applied to security issues related to the four categories within the ISA, can demonstrate the vast possibilities of the various branches of AI.

Interacting Intelligent Cyber Police Agents to Monitor Entire Networks

The paradigm of **intelligent agents** is a branch of AI that arose from the idea that knowledge in general and, especially, knowledge to solve problems ought to be shared between different entities. A single agent is an autonomous cognitive entity,[29] with its own internal decision-making system and an individual goal. To achieve its goal, an agent acts proactively within its environment and with other agents. In addition, agents have a reactive behavior; they understand and respond to changes in their environment and interact with it and other decentralized agents. Over time, agents self-adapt to dynamic changes in their environments, given their own accumulated experiences.[30]

Due to their decentralized and interacting nature, intelligent agents are predestined to gather information on entire networks and surrounding systems. It appears that this favorable characteristic has been used not only in terms of defense measures, but also for reconnaissance and exploitation (see the cyber kill chain discussed above) of potential target systems.[31] Since the behavior of every agent is formed by its experiences within its own personal environment, it is quite challenging to protect against such individualized threats.

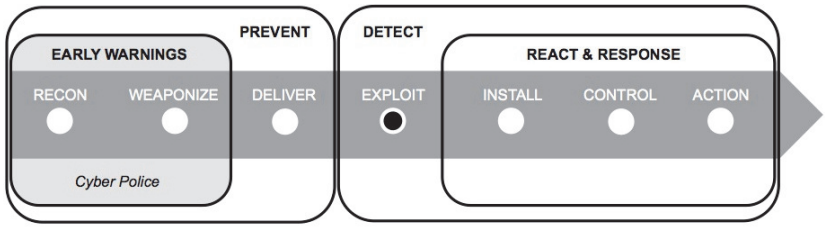

Figure 2: Intelligent Cyber Police Agents for Early Warnings in an Integrated Security Approach

A powerful way to utilize agents against distributed cyberattacks is by building up an intelligent agent's cyber police. This approach pursues the idea of artificial **police agents** in a defined cyber environment to detect malicious activities in a decentralized way.[32] As visualized in Figure 2 above, such police agents can facilitate protection already in the earliest stages of a cyberattack.

Intelligent agents can also be found in human-inspired artificial immune systems (AISs). By using two different types of agents, detection and counterattack agents, the beneficial characteristics of the human immune system is imitated. Detection agents monitor cyber environments and try to detect abnormal activities. When these agents spot malicious activities, they proactively send out decentralized instructions to counterattack agents, which are then activated to prevent, mitigate or even counterattack network intruders.[33]

Artificial Neural Networks to Prevent Malicious Intrusions

Another technique that emerged from the field of AI is the **artificial neural network** (ANN). ANNs are statistical learning models imitating the structure and the function of the human brain. They can help to learn and solve problems, especially in environments where algorithms or rules for solving a problem are difficult to express or are unknown. Since ANNs' system behavior is kind of elusive, they are considered undefined black-box models.[34]

In cybersecurity, ANNs have been used successfully within all stages of ISAs and, hence, can encapsulate all phases of the cyber kill chain. Integrated in cybersecurity, ANNs can be used for monitoring network traffic. As depicted in Figure 3 below, malicious intrusions can be detected already during the delivery phase and before an actual attack occurs.[35] This is a desired goal of cybersecurity, and it is a great achievement when cyberattacks can be hindered before they take place, thus, elaborating upon the main idea of perimeter defense.[36] ANNs can be successfully used to learn from past network activities and attacks in order to prevent future attacks from actually transpiring.

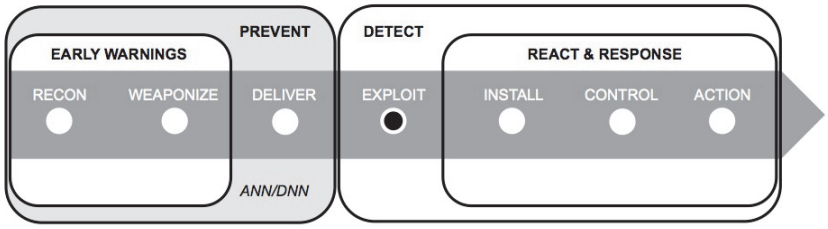

Figure 3: Artificial Neural Networks to Prevent Attacks within an Integrated Security Approach

Compared to conventional techniques used for cyber defense, the great advantage of using ANNs is their learning ability. As mentioned above, patterns that describe normal and abnormal network activities are traditionally defined manually by security professionals based on their expert knowledge. ANNs, however, can be trained to identify such patterns automatically by using previous data that has been transferred over the network.

Within an anomaly-based IDPS approach, it was shown that ANNs can be successfully utilized to evaluate header information[37] of network data packages to *learn* patterns for normal network behavior.[38] In a first preparatory step, the ANN was trained to identify and learn patterns of header attributes that belonged to normal network traffic. Every future data packet that was transferred over the monitored network was compared afterwards with these pre-learned patterns. When attributes of packet headers matched the *normal* pattern, they were transferred as usual. Irregularities in a data packet's header information that mismatched the learned pattern were classified as malicious and rejected by the IDPS. This dedicated approach has shown that the overall detection rate of attempted intrusions has improved without generating any false positive or false negative alarms. While traditional IDPSs, both signature-based and anomaly-based, work mostly against known intrusions, this ANN approach has successfully protected against instances of intrusions that were previously unknown. In summary, ANNs are said to support a viable approach to building robust, adaptable, and accurate IDPS.[39]

ANN monitoring is not limited to the use within IDPSs; it can be established in every system that monitors network activities. Firewalls, intrusion detection systems, or network hubs use ANNs to scan incoming as well as outgoing network traffic. In malware detection, an ANN-based experimental simulation demonstrated that even with quite a small computational effort, 90 percent of malware could be detected in advance.[40]

Deep neural networks (DNN), a more elaborate and computationally expensive form of ANNs,[41] have been used recently not only to protect organizations from cyberattacks, but also to predict these attacks. Improvements in hardware have led to advancements in data processing within network infrastructures and have enhanced storage capacities; thus, DNN technologies have become more popular and applicable. A dedicated AI-based security platform that used a DNN approach successfully demonstrated that it could predict cyberattacks 85 percent of the time.[42] With this development, we

see traditional approaches of cybersecurity shifting from attack detection to attack prevention. DNN techniques can now possibly lead in a new phase of cybersecurity—namely cyberattack prediction.

Expert Systems to Provide Decision Support for Security Professionals

Expert systems are computer programs designed to provide decision support for complex problems in a domain; these are the most widely used AI application. Conceptually, an expert system consists of a knowledge base, which stores the expert knowledge, and an inference engine, which is used for reasoning about predefined knowledge as well as finding answers to given problems.[43]

Depending on the way of reasoning, expert systems apply to different problem classes. A case-based reasoning (CBR) approach allows solving problems by recalling previous similar cases, assuming the solution of a past case can be adapted and applied to a new problem case. Subsequently, newly proposed solutions are evaluated and, if necessary, revised, thus leading to continual improvements of accuracy and ability to learn new problems over time. Rule-based systems (RBS) solve problems using rules defined by experts. Rules consist of two parts: a condition and an action. Problems are analyzed stepwise: first, the condition is evaluated and then the action that should be taken next is determined. Unlike CBR systems, RBSs are not able to learn new rules or automatically modify existing rules. This fact refers to the "knowledge acquisition problem," which is crucial in adapting to dynamic environments.[44]

Security professionals widely use expert systems for decision support in cyber environments. In general, evaluating security systems' audit data can determine whether a network or system activity is malicious or not. Due to the large amount of data, security experts regularly use statistical reports to scan and analyze the whole audit information in a reasonable time span. AI-based expert systems have successfully demonstrated that they could support these efforts by performing real-time monitoring in cyber environments, even on numerous or heterogeneous systems.[45] In cases where a malicious intrusion was spotted, a warning message was generated. It provided relevant information, upon which security professionals could select appropriate security measures more efficiently (cf. react & respond in Figure 4 below).

At this point, it is crucial to recall that expert systems so far solely assist decision makers, but are not able to substitute for them.[46]

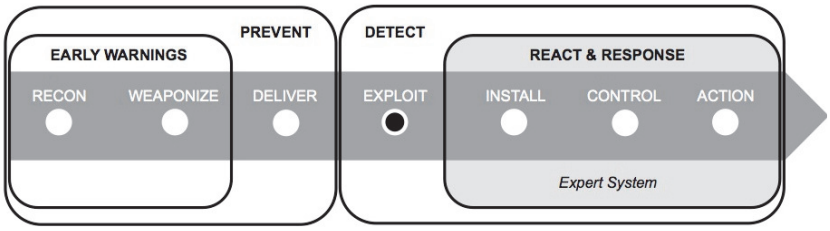

Figure 4: Expert Systems to Support React & Response Measures in an Integrated Security Approach

Drawbacks of Artificial Intelligence within Cybersecurity

The previous section discussed the benefits of AI as well as the various techniques that can address significant technological issues in today's cybersecurity domain. Despite these positive aspects, the concerns and risks from using AI within cybersecurity are as follows:

a. Inability to maintain cybersecurity autonomously: Although there have been huge advances in adapting AI techniques to cybersecurity, security systems are not yet fully autonomous. Since they are not yet able to completely replace human decisions, there are still tasks that require human intervention.[47]
b. Data privacy: AI techniques, like ANNs and DNNs, are becoming more advanced and new techniques emerge regularly—thanks to advances in hardware. The growing need, however, for big data can have a negative side when it comes to data privacy. The analysis of huge amounts of data may cause private as well as public organizations to be concerned about the privacy of their personal data, and some are even unwilling to share this data at all.[48] What personal data is used, why it is used, and how conclusions are reached within AI-based solutions may remain unanswered and may not be transparent for affected organizations.
c. Lack of regulation: Although there are various legal concerns about AI, the one concern that is most prevalent is the loss of human control over the consequences of AI's autonomy. Due to the unique and unforeseeable nature of AI, existing legal frameworks do not necessarily apply to this discipline.[49]

d. Ethical concerns: AI-based security systems increasingly make decisions for human individuals or assist them to do so (e.g., as discussed above in the case of Expert Systems). Considering this development, it is particularly worrisome that these systems do not currently have a moral code. Consequently, the decisions that are made for us are not necessarily the ones that a person would take.[50]

Conclusions

AI is considered as one of the most promising developments in the information age, and cybersecurity arguably is the discipline that could benefit most from it. New algorithms, techniques, tools, and enterprises offering AI-based services are constantly emerging on the global security market. Compared to conventional cybersecurity solutions, these systems are more flexible, adaptable, and robust, thus helping to improve security performance and better protect systems from an increasing number of sophisticated cyberthreats. Currently, deep learning techniques are possibly the most promising and powerful tools in the realm of AI. DNNs can predict cyberattacks in advance, instead of solely preventing them, and might lead to a new phase of cybersecurity.

Despite the promising nature of AI, it has emerged as a global risk for human civilization, while the risks and concerns for its use in cyberspace are justified. Here, four major issues can be identified: the lack of AI's full autonomy, concerns about data privacy, the absence of sufficient legal frameworks, in addition to ethical concerns originating from a missing moral code of autonomous decision-making systems. Due to the fast-growing nature of AI, it is necessary to resolve these related risks and concerns as early as possible. But, given these concerns and that sustainable solutions are not in sight, a socially responsible use of AI within cybersecurity is highly recommended. This could help to mitigate at least some related risks and concerns.

Until now, neither people nor AI alone have proven overall success in cyber protection. Despite the great improvements that AI has brought to the realm of cybersecurity, related systems are not yet able to adjust fully and automatically to changes in their environment; learn all the threats and attack types; and choose and autonomously apply dedicated countermeasures to protect against these attacks. Therefore, at this technological stage, a

strong interdependence between AI systems and human factors is necessary for augmenting cybersecurity's maturity. Moreover, a holistic view on the cyber environment of organizations is required. Cybersecurity is not only a technological issue; it is also about regulation and the way that security risks are dealt with. It is necessary to integrate any technical solutions, relevant processes, and people into an ISA framework to achieve optimal security performance. In the end, it is still the human factor that matters—not (only) the tools.

Notes

1 In 1988, Robert Tappen Morris, a graduate student in computer science, wrote the first computer program, which was distributed via the internet: the Morris Worm. The program was not designed to cause damage, but rather to gauge the size of the internet; a critical error, however, transformed the program, causing it to launch the first denial-of-service attack.

2 About the IDPS weaknesses, see Amjad Rehman and Tanzila Saba, "Evaluation of Artificial Intelligent Techniques to Secure Information in Enterprises," *Artificial Intelligence Review* 42, no. 4 (2014): 1029–1044, especially the section "Performance issues: IDS."

3 Selma Dilek, Hüseyin Çakır, and Mustafa Aydın, "Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review," *International Journal of Artificial Intelligence & Applications* 6, no. 1 (2015): 21–39.

4 Enn Tyugu, "Artificial Intelligence in Cyber Defense," in *Proceedings of 3rd International Conference on Cyber Conflict [ICCC], 7–10 June, 2011 Tallinn Estonia*, eds. C. Czosseck, E. Tyugu, and T. Wingfield (Tallinn, Estonia: CCD COE, 2011), pp. 95–105; Xiao-bin Wang, Guang-yuan Yang, Yi-chao Li, and Dan Liu, "Review on the Application of Artificial Intelligence in Antivirus Detection System," *Cybernetics and Intelligent Systems* (2008): 506–509.

5 The Global Challenges Foundation states AI as one of two emerging risks that might threaten mankind in the future. For more, see Dennis Pamlin and Stuart Armstrong, "Global Challenges—Twelve risks that threaten human civilisation," (Global Challenges Foundation: 2015), http://globalchallenges.org/wp-content/uploads/12-Risks-with-infinite-impact.pdf.

6 Stuart Russell, Tom Dietterich, Eric Horvitz, Bart Selman, Francesca Rossi, Demis Hassabis, Shane Legg, Mustafa Suleyman, Dileep George, and Scott Phoenix, "Research Priorities for Robust and Beneficial Artificial Intelligence: An Open Letter," *AI Magazine* 36, no. 4 (2015): 105–114.

7 My Digital Shield, "A History of Cybersecurity: How Cybersecurity Has Changed in the Last 5 Years," October 5, 2015, http://www.mydigitalshield.com/history-cyber-security-cyber-security-changed-last-5-years/.

8 Rehman and Saba, "Evaluation of Artificial Intelligent Techniques."

9 There are various approaches to describe the different stages of a cyberattack. This article refers to the *Cyber Kill Chain*® by Lockheed Martin, which has been widely used by the security community. For more, see www.lockheedmartin.com.
10 Gabi Siboni, "An Integrated Security Approach: The Key to Cyber Defense," *Georgetown Journal of International Affairs*, May 7, 2015, http://journal.georgetown.edu/an-integrated-security-approach-the-key-to-cyber-defense/.
11 Tony Sager, "Killing Advanced Threats in Their Tracks: An Intelligent Approach to Attack Prevention," A SANS Analyst Whitepaper (2014), https://www.sans.org/reading-room/whitepapers/analyst/killing-advanced-threats-tracks-intelligent-approach-attack-prevention-35302.
12 Cyber intelligence is more than the availability of raw data; rather, it provides actionable information of pre-sorted, processed, and evaluated data. For more about cyber threat intelligence and the conceptual delimitation of cyber intelligence and cyber information, see "What Is Cyber Threat Intelligence and Why Do I Need It?" iSIGHT Partners Inc. (2014), http://www.isightpartners.com/wp-content/uploads/2014/07/iSIGHT_Partners_What_Is_20-20_Clarity_Brief1.pdf.
13 Siboni, "An Integrated Security Approach."
14 Ahmed Patel, Mona Taghavi, Kaveh Bakhtiyari, and Joaquim Celestino Júnior, "An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Review," *Journal of Network and Computer Applications* 36, no. 1 (January 2013): 25–41.
15 Susan M. Bridges and Rayford B. Vaughn, "Fuzzy Data Mining and Genetic Algorithms Applied to Intrusion Detection," *12th Annual Canadian Information Technology Security Symposium* (2000): 109–122.
16 Patel, Taghavi, Bakhtiyari, and Celestino Júnior, "An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Review."
17 Rehman and Saba, "Evaluation of Artificial Intelligent Techniques."
18 Sager, "Killing Advanced Threats in Their Tracks: An Intelligent Approach to Attack Prevention."
19 The Federal Financial Institutions Examination Council developed the Cybersecurity Assessment Tool to help organizations identify their risks and determine their cybersecurity preparedness. The maturity level helps organizations to determine whether their behaviors, practices, and processes can support their cybersecurity preparedness. It also identifies potential actions that would increase this preparedness. For more, see https://www.ffiec.gov/cyberassessmenttool.htm.
20 Amirudin Abdul Wahab, "Facing Cyberattacks in 2016 and Beyond," *The Star*, January 28, 2016, http://www.thestar.com.my/tech/tech-opinion/2016/01/28/facing-cyber-attacks-in-2016-and-beyond/.
21 Rehman and Saba, "Evaluation of Artificial Intelligent Techniques."
22 Linda Ondrej, Todd Vollmer, and Milos Manic, "Neural Network Based Intrusion Detection System for Critical Infrastructures," *2009 International Joint Conference on Neural Networks* (Atlanta, GA, 2009): 1827–1834.

23 Yoshua Bengio, "Learning Deep Architectures for AI," *Foundations and Trends® in Machine Learning* 2, no. 1 (2009): 1–127.
24 Tyugu, "Artificial Intelligence in Cyber Defense."
25 "Fixed" algorithms use hard wired logic, on decision level, for reasoning about data. See Ibid.
26 Olin Hyde, "Machine Learning for Cybersecurity at Network Speed & Scale," an Invitation to Collaborate on the Use of Artificial Intelligence against Adaptive Adversaries, ai-one (2011), www.ai-one.com/.
27 "Noise" refers to inaccurate or irrelevant information in the collected data.
28 INFOSEC Institute, "Cybersecurity and Artificial Intelligence: A Dangerous Mix," February 24, 2015, http://resources.infosecinstitute.com/cybersecurity-artificial-intelligence-dangerous-mix.
29 A cognitive cyber entity can be understood as a single program, either software or hardware, that has human-like cognitive capabilities. In the realm of AI, the cognitive abilities of an intelligent agent would include perception of the cyber environment, acquisition, analysis of data gathered across cyberspace, and reasoning about that data.
30 Stan Franklin and Art Graesser, "Is It an Agent, or Just a Program? A Taxonomy for Autonomous Agents," *Third International Workshop on Agent Theories, Architectures, and Languages* (London: Springer-Verlag, 1997): 21–35.
31 Alessandro Guarino, "Autonomous Intelligent Agents in Cyber Offence," in *5th International Conference on Cyber Conflict*, eds. K. Podins, J. Stinissen, and M. Maybaum (Tallinn, Estonia: NATO CCD COE, 2013): 377–388.
32 Tyugu, "Artificial Intelligence in Cyber Defense."
33 Xia Ye and Junshan Li, "A Security Architecture Based on Immune Agents for MANET," *International Conference on Wireless Communication and Sensor Computing* (2010): 1–5.
34 Christian Bitter, David A. Elizondo, and Tim Watson, "Application of Artificial Neural Networks and Related Techniques to Intrusion Detection," *World Congress on Computational Intelligence* (2010): 949–954.
35 Ibid.
36 Tyugu, "Artificial Intelligence in Cyber Defense."
37 Packet headers contain attributes like the length of the transferred data, the network protocol type, or the source and destination addresses of a data packet. Therefore, the packet header carries information that can be sufficiently used to differentiate normal network behavior from intrusion attempts.
38 Ondrej, Vollmer, and Manic, "Neural Network Based Intrusion Detection System."
39 Bitter and others, "Application of Artificial Neural Networks and Related Techniques to Intrusion Detection."
40 The experimental simulations of malware detection emphasized worm and spam detection. For more, see Dima Stopel, Robert Moskovitch, Zvi Boger, Yuval Shahar, and Yuval Elovici, "Using Artificial Neural Networks to Detect Unknown

Computer Worms," *Neural Computing and Applications* 18, no. 7 (2009): 663–674.

41 Geoffrey E. Hinton, Simon Osindero, and Yee-Whye Teh, "A Fast Learning Algorithm for Deep Belief Nets," *Neural Computation* 18, no. 7 (2006): 1527–1554.

42 Victor Thomson, "Cyber Attacks Could Be Predicted With Artificial Intelligence," *iTechPost*, April 21, 2016. www.itechpost.com/articles/17347/20160421/cyber-attacks-predicted-artificial-intelligence-help.htm.

43 Tyugu, "Artificial Intelligence in Cyber Defense."

44 Serena H. Chen, Anthony J. Jakeman, and John P. Norton, "Artificial Intelligence Techniques: An Introduction to Their Use for Modelling Environmental Systems," *Mathematics and Computers in Simulation* 78, no. 2–3 (2008): 379–400.

45 Ibid.

46 Debra Anderson, Thane Frivold, and Alfonso Valdes, "Next-Generation Intrusion Detection Expert System (NIDES): A Summary," SRI International, Computer Science Laboratory: May 1995.

47 Katherine Noyes, "A.I. + Humans = Serious Cybersecurity," *Computerworld*, April 18, 2016, www.computerworld.com/article/3057590/security/ai-humans-serious-cybersecurity.html.

48 Tom Simonit, "Microsoft and Google Want to Let Artificial Intelligence Loose on Our Most Private Data," *MIT Technology Review*, April 19, 2016, https://www.technologyreview.com/s/601294/microsoft-and-google-want-to-let-artificial-intelligence-loose-on-our-most-private-data/.

49 Bernd Stahl, David Elizondo, Moira Carroll-Mayer, Yingqin Zheng, and Kutoma Wakunuma, "Ethical and Legal Issues of the Use of Computational Intelligence Techniques in Computer Security and Computer Forensics," *The 2010 International Joint Conference on Neural Networks (IJCNN)*: 1–8.

50 Nick Bostrom, "Ethical Issues in Advanced Artificial Intelligence," in *Cognitive, Emotive and Ethical Aspects of Decision Making in Humans and in Artificial Intelligence*, eds. Iva Smit and George E. Lasker (Windsor, ON: International Institute for Advanced Studies in Systems Research / Cybernetics, 2003) 2: 12–17.