Scientific Research Publishing

Journal of Information Security, 2025, 16(2), 227-251
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Prioritizing Defense in Depth Measures Using Artificial Intelligence (AI) and the Expected Utility Hypothesis

Rodney Alexander

Cochise College, Sierra Vista, USA
Email: rdnyalex@aol.com

How to cite this paper: Alexander, R. (2025) Prioritizing Defense in Depth Measures Using Artificial Intelligence (AI) and the Expected Utility Hypothesis. *Journal of Information Security*, **16**, 227-251.
https://doi.org/10.4236/jis.2025.162012

Received: February 20, 2025
Accepted: March 28, 2025
Published: March 31, 2025

Abstract

The purpose of this research was to determine whether Artificial Intelligence (AI) and the Expected Utility Hypothesis can be effectively applied to the prioritization of defense in-depth security tools and procedures to reduce cyber threats. The way this was determined, or methods used in this study consisted of using AI (Microsoft CoPilot) to rank the current top 10 cybersecurity threats and the cybersecurity defense in depth utilities that are designed to reduce those threats. The methods further involved using the Likert Scale Model to create an ordinal ranking of the cybersecurity threats. The defense in depth utilities and procedures were then compared to see whether AI (CoPilot), the Likert scale and the Expected Utility Hypothesis could be effectively applied to prioritize and combine the measures to reduce cyber threats. The results of this research reject the H_0 null hypothesis that AI and the Expected Utility Hypothesis does not affect the relationship between prioritization and combining of defense in depth utilities and procedures (independent variables) and related cyber threats (dependent variables).

Keywords

Artificial Intelligence (AI), Expected Utility Hypothesis (EUH), Information Assurance, Defense in Depth, Information Technology, Network Security, Cybersecurity

1. Introduction

The research background in cyber security defense-in-depth (DiD) prioritization included a literary review of recent cyber security breaches and how organizational network security managers prioritize their network defenses to prevent

those breaches. An analysis of former cyber security prioritization research disclosed that organizational network security managers need to use additional systematic decision-making approaches when prioritizing their network defenses. To summarize the problem involving former research, network security managers need additional decision theories when deploying their defenses.

This research introduced using the Expected Utility Hypothesis, artificial intelligence (AI) and the Likert scale to give network security managers an additional systematic way to prioritize their network defenses. The dependent variables of cyber threats were determined to see whether they could be influenced by the independent variables (prioritized defense in depth tools and procedures) to reduce organizational cyber breaches. The independent variables of defense in depth tools and procedures were determined to be effective means used by security managers to counter cyber threats.

Microsoft Security Copilot plays a significant role in the prioritization of cybersecurity threats by leveraging AI to enhance the efficiency and effectiveness of security operations. Security Copilot integrates with Microsoft Defender Threat Intelligence to provide contextual threat intelligence, helping security teams understand and prioritize threats based on their exposure level [1]. It offers step-by-step guidance for incident response, including triage, investigation, containment, and remediation [1]. Microsoft ensures that Security Copilot's output is reliable and accurate through several validation checks [2]. This includes checks for harmful actions, stereotypes, personal information exposure, and more. These checks are performed during the manifest validation and processing of user prompts [2].

Cyber-attacks can be reduced by deploying security tools and procedures. Cybersecurity should be applied commensurately with the risk and the value of the asset requiring protection [3]. Critical infrastructure requires the highest security priority.

In the field of cyber security, threats have evolved such that they are usually complex interactions between an assailant (the "threat actor") and the target system [4]. Hackers will try to use elaborate artificial intelligence (AI) means to intrude systems. Although implementation of technological solutions is the usual respond to security threats and vulnerabilities, wireless security is primarily a management issue [4].

How the network security manager designs and implements a network will influence how well the network is protected. Defense in depth (DiD) prevents network intrusions by deploying tools and procedures such as firewalls, access control and detection. Most of the systems use robust a architecture to enhance business and reduce costs by increasing the integration of external, business, and control system networks [4].

The large organizations can use Expected Utility Hypothesis and AI to improve the security on their networks. The DiD strategy recommends a balance between protection capability and cost, performance, and operational considerations [5]. Defense-in-depth is an important security architecture principle that has significant application to industrial control systems (ICS), cloud services, storehouses of

sensitive data, and many other areas [6].

Artificial intelligence gives organizations the opportunity to data mine social networks for hackers; social networks have become an important part of organizational operations. Millions of people use various forms of social networks as they allow individuals to connect with friends and family and share private information [7]. Social networks and AI have become effective ways to hunt threats and discover vulnerabilities.

The concept of defense in depth is adopted from military defense where different obstacles are deployed to eventually expend the resources of attacker [7]. A hacker's time, skills and funding can be exhausted by deploying defensive barriers centered on loss of privacy prevention, for example. The Expected Utility Hypothesis can help organizations determine the most effective ways to exhaust an attacker's resources.

During this process, one or more intermediate target devices (e.g., DNS servers, routers, etc.) may be used to gain progressively deeper access to the target network to approach the target system [3]. The overall security objectives remain the same: preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems [4]. The Expected Utility Hypothesis is a fundamental concept in economics and decision theory. It suggests that when faced with uncertainty, rational agents make decisions by maximizing their expected utility [8].

The reduction of security threats to organizational networks is maximizing the utility of tools and procedures designed to reduce those threats. By deploying the same defenses on the internal network as on the external edge, the network can secure itself and other networks [8].

Using AI and EUH, for example firewalls can be combined to secure different segments of the network.

At a high level, the threat actor can use several techniques to breach the target network, by passing the defensive devices and either installing malicious code on a target system or directly accessing the target system [3]. There are many tools available on the Internet which will allow hackers to breach systems, access networks and steal data. When considering the most logical route an attacker will take in compromising a control network, it is easy to visualize an attack path that pries deeper and deeper into the architecture [4].

An attacker will try to access the core of a system to steal or manipulate privacy data. A Social Network Service (SNS) is a kind of web service for establishing a virtual connection between people with similar interests, backgrounds, and activities [6]. People with the same hobbies and work environments need to keep network security in mind when using social media networks.

Effective management of the threats associated with technology requires a sound and thorough assessment of risk given the environment and development of a plan to mitigate identified threats [4]. Artificial intelligence can be used to identify threats to a network and to develop plans to mitigate those threats. Identifying critical assets based on a risk assessment is a good starting point, but security must

not end there [2].

Once critical assets are identified, a security blanket must be developed around the organizational critical assets. Once the target system is compromised, the threat actor can then act upon target data and/or target systems or intermediate systems in some way that achieves a malicious goal [3]. A hacker gains access to sensitive data by compromising vulnerable systems.

The main thrust of the research is to indicate that individuals are rational and make decisions by weighing the potential benefits and risks in a way that maximizes their overall satisfaction or utility [9]. The physical network security tool, *i.e.* a network intrusion detection system (NIDS) is mapped against the hidden process of intrusion reduction in this research. The expected utility hypothesis can be deployed in the information assurance planning process.

The logic of the theory can easily be extended to decisions about selecting goals or managerial strategy [10]. Can we predict the time of the next eruption of Old Faithful Geyser from the length of the most recent eruption [11]? The number of organizational security breaches can be predicted based on the type of layered defenses used to secure those organizational networks. This is a task perfectly designed for AI.

Instead of focusing on feature-centric network defense requirements, the defense in depth (DiD) model should be redesigned to be a functional or capability focused model [8]. Defense in depth priorities and focus should align with current threats, for example DDOS and DOS attacks. Exemplary actions on the target data can include but are not limited to theft of data exfiltration), destruction of data, modification of data, or Some combination thereof [3].

While on the Internet, user passwords can be stolen as well as bank information and medical records. The Expected Utility Hypothesis posits that when faced with various options and uncertain outcomes, a rational agent will choose the option that maximizes their expected utility. This concept was first introduced by Daniel Bernoulli in the 18th century in response to the famous St. Petersburg Paradox [12]. Network security outcomes can be predicted using EUH based on the deployment of certain defense in depth security tools.

Decision theory provides a normative framework for representing and reasoning about decision problems under uncertainty [13]. The ambiguity of deciding which defense in depth measures to use to reduce network intrusions can be solved using this modeling principle.

The purpose of this statistical analysis is to give organizational network security a clearer picture on how to manage the difficult multi criteria decision making problem associated with network security.

Symmetry in the DiD model allows for the network defense system to recognize the insider threat, preventing data exfiltration and allowing attacks to be stopped at the originating network instead of being defended by the attacked network [8]. At its core, the Expected Utility Hypothesis involves assigning a utility value to each possible outcome of a decision [14]. The reduction of security threats to an organizational network can be shown by using EUH.

The idea behind the defense in depth approach is to defend a system against any attack using several independent methods [8]. Defense in depth measures should be arrayed against threats to attack them from several different directions. Wireless Networks present a host of issues for network managers [4]. Network security managers face varying threats when it comes to wireless networks.

In today's rapidly changing world, networks change daily, software is updated weekly, and threats may change by the hour [3]. Computer networks are fluid environments which require the constant attention of network security managers. Statistical methods are important for exploring the relationships between variables and can be applied to many studies [15].

Expected Utility Hypothesis can be significant in exploring the relationship between network security threat variables and defense in depth security tool variables. Dynamic defenses must also be enabled, which change attack surfaces to proactively defend a network [8]. Defense in depth intrusion detection systems can adjust to the changing nature of attacks.

Unauthorized access points, broadcasted SSIDs, unknown stations, and spoofed MAC addresses are just a few of the problems addressed in WLAN [4]. Most of these threats are specific to wireless networks, especially during times when people are working from home and learning from home. This research study explores whether the Expected Utility Hypothesis and AI can be effectively applied to the array of information assurance defense in-depth measures to mitigate network security threats.

1.1. Network Security Threats

A "peel-the-onion" analysis shows that an attacker trying to affect a critical infrastructure system would most likely be after the core control domain [4]. This study uses the Likert Scale to rank network security threats (**Table 1**) and their corresponding defense in depth security measures which will assist network security managers in prioritizing their network resources.

Rank correlations also work well with ordinal rating data, and continuous data are reduced to their ranks [15].

Table 1. Top ten network security threat prioritization.

Priority	Threat
1	Malware
2	Phishing
3	Man-in-the-Middle (MitM)
4	Denial of Service (DoS)
5	SQL Injections
6	Zero Day Exploits
7	Insider Threats
8	Advanced Persistent Threats (APT)
9	Credential Theft
10	IoT Vulnerabilities

These attacks attempt to deliberately modify information shared within the smart grid to corrupt critical data exchange in the smart grid [15]. Malware can destroy data and functions designed to operate and control the smart grid. An increasing number of wireless devices are abused for illicit cybercriminal activities, including malicious attacks, computer hacking, data forging, financial information theft, online bullying/stalking [16].

Users should be extremely careful while social distancing and using wireless networks. The target of the attacks is either customer information (e.g., pricing information and customer account balance) or network operation information (e.g., voltage readings, device running status) [15]. Network intruders may attempt to disrupt this smart grid data traveling over the Internet. Malicious attacks targeting network availability can be considered as denial-of-service (DoS) attacks [15].

If networks become unavailable, then working from home or distance learning will come to a screeching halt. This causes the direct loss of about 83 billion euros with an estimated 556 million users worldwide impacted by cybercrime each year, according to the 2012 Norton cyber-crime report [16]. Cybercrime is responsible for large financial losses to the global economy; this is something to keep in mind while working from home.

Ad-hoc networks can pose a security threat [4]. A Bluetooth connection, for example, has fewer security controls than a managed wireless network. Differing from attacks targeting network availability, attacks targeting data integrity can be regarded as less brute force yet more sophisticated attacks [15]. Integrity attacks can try to discredit the integrity and data privacy of sensitive data.

The new paradigm of global availability in networks offered by IPv6, must also be accounted for [8]. Because of social distancing requirements and remote computing, global cloud security must be included in an organization's security structure. Threat actors can gain access to credentials for normal or privileged access to the target network [3]. Thieves may pay inside workers for compromising information.

An unauthorized node in a wireless network is capable of inflicting intentional interferences with the objective of disrupting data communications between legitimate users [16]. Denial of service attackers can cause havoc for Internet users. Since network availability is the top priority in the security objectives for the smart grid, we use experiments to quantitatively evaluate the impact of denial-of-service (DoS) attacks on a power substation network [15].

A denial of service (DOS) attack could potentially plunge entire regions into darkness.

An attacker must then not only compromise security controls at the perimeter but must be able to compromise each layer behind the perimeter to reach the critical asset [2]. While we are learning from home an attack is less likely to be successful if an attacker must breach multiple obstacles. A major difference between the smart grid and the Internet is that the smart grid is more concerned with the

message delay than the data throughput due to the timing constraint of messages transmitted over the power networks [15]. Denial of service attacks can prevent critical smart grid messages from reaching their final destinations.

Due to the broadcast nature of radio propagation, the wireless air interface is open and accessible to both authorized and illegitimate users [16]. It is important to keep in mind while social distancing that both friends and enemies have access to wireless networks because wireless networks transmit over the airways.

1.2. Defense in Depth Security Strategy

The first defense approach is prevention [17]. The first defense in depth measure that a network security manager should take is to protect the network and the data that crosses the network. The network should especially be protected in a way that allows users to safely work and learn from home.

The next defense approach is detection [17]. Detective measures are taken to reveal the presence of attacks and intrusions that have compromised or circumvented preventive mechanisms [17]. It is important to deploy defense in depth tools such as NIDS that can identify potential attacks such as Trojans.

Though firewalls, IDSs, and IPSs are ineffective network security systems when deployed by themselves, layering them provides additional protection [8]. Deploying defense measures as a unit increases their effectiveness. In the event there is a security-related incident in the controls system domain, activities to recognize, respond, mitigate, and resume need to be established [4].

Security planning and operations should take place before, during and after a security breach. For example, installing up to date antivirus is critical before breach operation. Incident response consists of policies, procedures, and technical measures that enable the identification of potential cyber intrusions and the structure to react to and remediate the event [2]. Tactically, security is incomplete without proper assessment of assets, risks associated with them and policies to control these risks; the outermost layer of the model covers all these aspects [7].

Organizations must consider the risk to organizational assets before establishing remote connections due to social distancing requirements. Each of these defensive devices have been created to act upon specific types of threats and when used in combination can theoretically help prevent, limit, or detect the attack of a threat actor, resulting in better safety for target data and target systems [2]. If a hacker can bypass one defensive tool they can be stopped by another defensive tool and user data can remain safe.

Defensive strategies that secure each of the core zones can create a defensive strategy with depth [4]. In information security terms, administrators or organizations deploy layers of defensive measures to minimize risk of unauthorized access or information attacks [7]. The defensive layer of an UpToDate antivirus, for example, can help reduce the risk of identity theft.

Deflection is a means of diverting attackers from the valuable assets to a faux environment where their techniques and methods can be studied [17]. Honey pots

can be used to deflect users away from sensitive areas where sensitive data may be stored. Security issues are not solved magically but administrators must evaluate different methodologies to consider as best practice for their organization [7].

Network security managers should develop the best defense-in-depth strategy that fits their organization. For example, if Trojans are a concern they should focus on firewalls and Network Intrusion Detection Systems (NIDS). Information assurance (IA) mechanisms may be subdivided into three categories: preventive, corrective and detective [18]. Organizations can remain safe from attacks by using the defense in depth measures of protection, identifying potential attacks, and removing them.

Target organizations typically take action to prepare and assess their security posture to locate holes in their security systems [3]. Network security managers are constantly looking for areas in their networks that can be breached by hackers while employees are remotely working because of social distancing requirements. Overlapped layers can cover shortcomings of one layer by another [7]. Encryption can also be overlapped within the network to cover firewall shortcomings.

The strategy recommends a balance between the protection capability and cost, performance, and operational considerations [6]. Organizational defense in depth requires strategic planning. Development of a defense-in-depth strategy starts with mapping the control systems architecture [4].

Network security managers must have intimate knowledge of the network to understand how to effectively deploy a defense in depth strategy. The DiD model uses layers of different network protection devices to create a secure network [8]. UpToDate antivirus is one example of a measure that can be deployed in the defense in depth model.

Layer 1 focuses on perimeter security and the controls surrounding the protection of the ingress/egress point of the substation electronic security perimeter [2]. The first level of protection is entry into the network. This can involve a remote connection or VPN.

Layer 2 focuses on the security controls for communication and devices that perform data aggregation [2]. The second level are the areas where critical data is stored, databases containing sensitive organizational data for example. Layer 3 focuses on host-based cybersecurity controls used to provide security at the device level [2]. The final protection level involves protecting individual devices, for example, laptops, desktops and servers.

No single security solution will keep a determined thief from the goal of compromising the hardware or software given enough time and resources [14]. Loss of privacy can be reduced by deploying defensive tools in the path of the attacker. A single strategy to defense information and its associated components may not be sufficient [7].

Multiple layered defense measures are required to protect organizational systems while employees work from home. Historically, a military defender would build a series of defensive positions and fall back as the attacker advanced, even-

tually defeating the attacker [8]. Confidentiality should be built on the onion approach with the most sensitive data being in the middle and hardest for an attacker to reach.

Instead of attempting to prevent inbound attacks and blocking specific forms of outbound traffic, a functional DiD model should look to deploy defenses that are symmetric [8]. Defense in depth can be designed to prevent both internal and external data theft. The DoD Defense-In-Depth model is extended to logical, layered, and virtual "boundaries" beyond more traditional physical and geographic boundaries [18].

Cloud or logical boundaries have enhanced the capabilities of traditional defense in depth strategies. Having multiple DMZs protects the information resources from attacks using Virtual-LAN (VLAN) hopping and trust exploitation [4]. Data can be processed in secure zones which are harder for hackers to reach. Dynamic defenses can be enabled both through dynamic computing platforms and dynamic network addressing [8].

Demilitarized zones (DMZ) can be dynamically established using DHCP to segment and block traffic. A tool such as encryption can be combined with firewalls, NIDS and authentication to create repeated barriers to defeat attackers [3]. These systems, when layered together, create a system of defense known as Defense-in Depth, where each layered defensive device prevents a deeper level of attack.

Each layer in defense in depth architecture has heterogeneous implementation of security controls which results in administration overhead [7]. Each defensive player must be configured separately by a security manager or an administrator. Multilayer security puts the critical assets at the most reliable and secure layer [2].

Sensitive organizational data, for example, should be placed in the most critical level of the defense in depth strategy. A DMZ is an exceptionally good way to enhance the security posture and add another layer to the defense-in-depth strategy [4]. Systems used by employees working from home can be placed in a secure zone (DMZ) which protects their communications.

With multiple layers, each layer can have unique yet complementary security controls [2]. Phishing attacks can be reduced with specific but supportive defensive layers. Defense in depth is based on layered architecture; every layer has its own implementation [7]. Although defense measures may cover vulnerabilities that others miss. Each requires individual configuration.

Differentiating between similar attacks like phishing and spear-phishing is crucial for effective threat prioritization. Here are some strategies to prioritize and differentiate these overlapping threat categories. Analyze the context of the attack. Spear-phishing attacks often contain personalized information, such as the recipient's name, job title, or specific details about the organization [19].

Phishing attacks, on the other hand, are more generic [19]. Verify the source of the email or message. Spear-phishing attacks may appear to come from a trusted source within the organization, while phishing attacks often use generic or spoofed email addresses [20].

1.3. Defense in Depth Security Tools and Procedures

Effective security policies and procedures are the first step to a secure control systems network [4]. It is important for organizations to outline in detail how they will protect their data from network intrusions. The best method for protecting the confidentiality of information transmitted over wireless networks is to encrypt all wireless traffic [4].

Using authentication and encryption is the most effective way to secure wireless networks. A well-defined and well implemented defense in depth strategy prevents a wide variety of attacks and generates real-time intrusion alarms to the administrators [7]. Network Intrusion Detection Systems NIDS can tell network security managers when their network is being attacked and steps necessary to prevent the attack.

There are several common methods for monitoring a network for unusual or unauthorized activity, with one of the most effective being Intrusion Detection Systems (IDS) [4]. Illegal access to systems can be monitored and blocked by several devices before intruders can steal data. Network Security Situation Awareness (NSSA) is a new notion deriving from Air Traffic Control (ATC) [21].

Knowing where the attacks are occurring is an important step in stopping an attack. Ensure that Software is up-to-date, systems are appropriately configured on its network, and access is appropriately controlled [3]. Software must be properly patched to prevent zero-day attacks.

Informing personnel of their responsibilities when it comes to cybersecurity is an important step in implementing and enforcing policies and procedures [2]. Employee training and an effective security awareness campaign are critical to a successful cybersecurity program for example security necessary to maintain Confidentiality. The next generation cyberspace intrusion detection systems will fuse data from heterogeneous distributed network sensors to create cyberspace situational awareness, and analogized cyberspace situational awareness with ATC [21].

Sensors can be deployed to spot phishing attacks that are designed to breach critical systems. Over time, there have been two key practices for this assessment: tabletop exercises and penetration tests [3]. Security managers should use these tools to assess their networks to ensure they are effective at preventing breaches such as phishing attacks which are designed to steal passwords.

Specific fingerprinting and operating system detection can be used to profile attacker activities, skill level and motivations [22]. What an attacker is trying to achieve can be viewed in real time. To maintain confidential transmission, existing systems typically employ cryptographic techniques for preventing eavesdroppers from intercepting data transmissions between legitimate users [16].

The defense in depth measure encryption can help stop man-in-the-middle attackers from disrupting and intercepting Internet communications. If the message is not encrypted, or encrypted with a weak algorithm, the attacker can read it, thereby compromising confidentiality [4]. Authentication and encryption are critical to wireless network security especially while working from home and

learning from home.

Situational awareness was defined by Endsley as "the perception of the elements in the environment with a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" [21]. Multi-factor Authentication can be used to deter an attacker for a limited amount of time. At the point that the authentication expires the user should reauthenticate. This intelligence is vital for initiating appropriate responses and for law enforcement investigations [22]. Cybersecurity forensics can benefit by capturing this data.

Penetration tests are live fire exercises in which White Hat Hackers perform as threat actors and are tasked with attempting to infiltrate the target network, access the target systems [3]. White hat hackers are hackers hired by the organization to identify system security weaknesses which might possibly disrupt critical activities. Network situation elements consist of Internet/Intranet (environment), entities in the network including software and hardware, network security events including alerts, logs and files, correlation team and network intrusion behavior [21].

The status of the entire must be known to prevent intrusions such as DoS attacks. Anomaly based intrusion detection systems, but care must be taken avoid overwhelming the human operator [22]. Network intrusion detection systems must take the limitations of the security manager into consideration.

White hat hackers can retrieve a sample of target data to prove that network defense is ineffective, thus locating a route that should be remediated [3]. Using this tool network security managers can fix network security issues before they cause real security problems. The long-term goal is to create a library of visual signatures that can be used by experts or novice analysts to detect malicious activity [22].

Due to the external nature of the penetration tests, they tend to be expensive to execute and are typically undertaken infrequently (usually once or twice a year) [3]. Unfortunately pen testing is too costly and disruptive and therefore not frequently conducted. NSSA fuses data from tools of IDS, VDS (Virus Detection System), Firewall, Netflow etc., to find what happening in the network [21].

Data is collected from several points to see for example when a Man in the middle attack is attacking the network. There are a wide variety of potential visualizations that can be used to display network traffic data in a way that is meaningful for security analysis [22]. Network security managers can see intrusions that are placed on the network from several different views.

In addition, they usually stop at the first successful breach, resulting in a single Successful breach log and one or more failed breach attempts [3]. Pen testing is unlikely to discover a vulnerability which can be exploit by an advanced persistent attack (APT) for example man in the middle attacks. These types of attacks put working from home at risk.

In the MAC layer, the MAC address of a user should be authenticated to prevent unauthorized access [14]. To prevent hackers from entering the network, security

managers should use MAC authentication. Training is a core component of an overarching security awareness program [4].

Because of social distancing requirements, network security training for administrators and users may have to be carried out remotely. Vulnerability scanning is not a passive operation, and as such can produce real-world failures that can impact operations inside of the organization [3]. Scanning should be done during non or low operational maintenance periods so that it does not disrupt normal organizational network functions.

Interception and alteration of wireless transmissions represents a form of "man-in-the-middle" attack [4]. Encryption can stop a man-in-the-middle attacker from viewing the content of the data that he has managed to steal especially during times when people are working from home and learning from home. To secure networks, the DiD model must be viewed as a system of systems and updated with current network defense strategies [8].

Latest Encryption algorithms allow systems to securely communicate together with lower risk of privacy or data loss. The open communications environment makes wireless transmissions more vulnerable than wired communications to malicious attacks [16]. Using a wired network is safer than using a wireless one.

In the network layer, the WPA and theWPA2 are two commonly used network-layer online bullying/stalking [16]. Authentication is a critical part of defense in depth. Firewalls, for blocking access from or to unwanted locations to or from the defended networks; Intrusion Detection Systems (IDS), for detecting Suspicious traffic on the defended networks [3]. The control center receives security events from each element to preprocess and save them in a database before transferring to situation analysis [21].

Once security data is analyzed, it can be uploaded to create UpToDate antivirus files. Security measures such as Demilitarized Zones (DMZ), firewall, Intrusion detection System (IDS), malware Protection and virtual private networks (VPNs) provide defense in depth strategy that deflect information security attacks aim to gain unauthorized access to an organization asset from the internet or public network [7]. Along with other measures such as antiviruses these defensive measures are critical for stopping attacks from the Internet.

New advances in cloud computing allow users to rapidly scale provisioned computing resources to consume DoS and DDoS attacks [8]. Network intrusion can be severely limited by placing resources in the cloud. Network segmentation has traditionally been accomplished by using multiple routers.

Firewalls should be used to create DMZs to protect the control network [4]. To stop malware such as trojans, firewalls should be used to create protected zones within the network. One problem with tabletop exercises is that they test the theoretical function of the systems under test, not the actual function [3]. Penetration test (pentest) can be used in leu of tabletop exercises to locate system vulnerabilities which hackers may try to exploit.

Systems such as firewalls, IDSs and IPSs are still used, but layered with new

devices that provide different new capabilities to the network defense system [8]. Privacy loss can be prevented with both traditional and new devices. Each of these devices acts as an obstacle to the attacker [7]. Advanced persistent threats (APTs) can be stopped by using successive defensive barriers.

Defense to stop the threat actors at the earliest point in the attack, and to provide the earliest warning of the presence of threat actors attempting to access a defended network [3].

While learning from home network security managers try to stop an attacker as far away from user data as possible. Preferably before they gain access to the network.

Current network defenses are designed around the features of specific network defense tools, such as identifying malware, blocking packets, or analyzing network events [8]. Two factor Authentication is designed to stop unauthorized network Intrusion. Malware is very prevalent in operating systems that typically run on laptops, desktops, and server hardware platforms [2]. Security managers should ensure that all device firmware updates are installed from a trusted source.

1.4. Artificial Intelligence (AI)

Artificial intelligence (AI), the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings [23]. Computers can perform some tasks quicker, more efficiently and consistently than humans. Artificial intelligence (AI) is technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy [24]. Human learning and problem solving can be enhanced by using AI.

Artificial Intelligence (AI) is playing an increasingly significant role in cybersecurity [25]. Some of the AI benefits in Cybersecurity include threat detection, automated responses and behavior analysis. In terms of threat detection, AI can analyze vast amounts of data to identify patterns and detect threats in real-time. This enables rapid response and mitigation [25].

Artificial Intelligence (AI) can enhance automated responses by automating routine tasks such as log analysis and vulnerability scanning, freeing up human analysts for more complex tasks [25]. Threat actor behavior can be quickly analyzed by AI systems to uncover malicious behavior. Systems can monitor behaviors, detect phishing attempts, and authenticate users by analyzing data like typing styles and voice patterns [25]. Finally, AI can continuously learn from new data, improving its ability to identify and counter emerging threats [25].

There are some challenges and risks associated with using AI to perform cybersecurity tasks. Cybercriminals can use AI to create highly personalized spearphishing messages or deepfake voices to deceive employees [26]. Attackers can use AI to tamper with data, creating false information that can be used for financial gain or to damage reputations [26]. The use of AI in cybersecurity raises ethical questions about privacy, data protection, and the potential misuse of AI tech-

nologies [26].

A few artificial intelligence trends are developing in the field of cyber security. Enhanced AI capabilities will continue to evolve, becoming more sophisticated in detecting and responding to cyber threats [27]. Collaboration will be increased collaboration between government agencies, private sector companies, and international partners to advance global AI security best practices [27]. Organizations will focus on workforce development, expanding AI expertise within their workforce to ensure they can effectively leverage AI technologies [27]. AI is a powerful tool in the fight against cybercrime, but it must be harnessed responsibly and securely [27].

2. Theoretical/Conceptual Framework

Expected Utility Hypothesis

Expected Utility Hypothesis (EUH) forms the basis for many economic models and can be applied to a wide range of decisions, from financial investments to everyday choices [28]. Organizations can use the hypothesis to make cybersecurity decisions. Utility is a measure of the satisfaction or benefit that an individual derives from a particular outcome. It's subjective and can vary from person to person [8]. The utility of certain cybersecurity defense in depth measures, *i.e.* software updates, can be compared to other measures, *i.e.* user training.

A comparative analysis between both AI and EUH in cyber security prioritization approaches reveals that, while both AI and EUH have their strengths and limitations, AI's speed, adaptability, and scalability make it a more effective approach for prioritizing cybersecurity threats in today's dynamic and complex threat landscape [29]. However, combining AI with EUH can provide a more comprehensive approach, leveraging the strengths of both methods to enhance cybersecurity defenses [29].

Probability is the likelihood of each possible outcome occurring [8]. By using EUH, organizations can calculate the probability that they will become the victim of certain cyber attacks, *i.e.* malware or SQL injections. Bernoulli's work laid the foundation for modern expected utility theory, which was further developed by John von Neumann and Oskar Morgenstern in their seminal book "Theory of Games and Economic Behavior" published in 1944 [30].

In game theory, expected utility is used to analyze strategic interactions where outcomes depend on the choices of multiple agents [30]. In cybersecurity strategic analysis can be made between cyber threats and defense in depth tools. It helps predict the behavior of individuals in competitive settings, such as auctions, bargaining, and voting [30].

Utility functions are a critical component of this hypothesis, providing a way to quantify an individual's preferences [30]. The utility of defense in depth tools can be matched with the cyber risks that an organization may face. These functions can take various forms depending on the nature of the decision-maker's risk preferences [30].

Risk management practices heavily rely on expected utility theory to assess and mitigate potential losses [31]. Using EUH organizations can reduce their risk of cyber-attacks. Insurance companies use it to determine premiums and coverage levels, while businesses use it to make decisions about project investments and risk mitigation strategies [31].

Despite its widespread use, the Expected Utility Hypothesis has faced several criticisms [31]. One of the main critiques is its assumption of rationality, which does not always hold true in real-world scenarios [31]. Behavioral economists have documented numerous instances where individuals deviate from rational behavior due to biases, heuristics, and other psychological factors [31].

The Expected Utility Hypothesis remains a fundamental concept in understanding decision-making under uncertainty [30]. It is a tool that organizations can use to prioritize their cyber defenses when the number and types of cyber-attacks that they face are not clear. While it has its limitations, it provides a robust framework for analyzing choices and predicting behavior in various contexts [30].

There are some limitations that can be encountered while applying AI and EUH in cybersecurity defense prioritization. AI algorithms are only as good as the data they are trained on. Poor quality or biased data can lead to inaccurate detection and false positives [32]. AI systems can be vulnerable to adversarial attacks where malicious actors manipulate input data to deceive the AI, leading to incorrect threat assessments [33].

EUH relies on simplifying assumptions about rationality and preferences, which may not hold in the complex and dynamic landscape of cybersecurity [33]. Accurately estimating probabilities and outcomes of cyber threats can be challenging due to the unpredictability of attackers [34].

As research in behavioral economics continues to evolve, it is likely that new models and theories will further refine our understanding of utility and decision-making [30].

Expected Utility is calculated by multiplying the utility of each outcome by its probability and then summing these products for all possible outcomes [8]. The expected utility is then calculated by taking the weighted average of these utility values, with the weights being the probabilities of each outcome occurring [30]. A theoretical model of this process is displayed in the table below (See **Table 2**).

Table 2. Expected utility hypothesis theoretical model.

		Theoretical Model								
		Alternatives								
		College (A)		**College (B)**		**College (C)**		**College (D)**		**Total**
Utilities	Living Cost (1)	$300	2 = 1 × 2	$200	1 = 1 × 1	$400	3 = 1 × 3	$500	4 = 1 × 4	**10**
	Dorms (2)	Good	4 = 2 × 2	Excellent	2 = 2 × 1	Average	6 = 2 × 3	Lacking	8 = 2 × 4	**20**
	Tuition (3)	$500	12 = 3 × 4	$450	9 = 3 × 3	$400	6 = 3 × 2	$350	3 = 3 × 1	**30**
	Class Size (4)	Medium	8 = 4 × 2	Small	4 = 4 × 1	Large	12 = 4 × 3	X-Large	16 = 4 × 4	**40**
	Total		**26**		**16**		**27**		**40**	

Expected Utility Hypothesis answers questions about the dependence of a response variable on one or more predictors [11]. The question of reducing the dependent variable (security threats) is dependent on the independent variable (network security tools). These statistical concepts are illustrated by using a data set from published literature to assess a computed tomography– guided interventional technique [12].

The methods used in this study consisted of scanning 20 peer reviewed Cybersecurity Articles from prominent Cybersecurity Journals for a list of defense in depth measures (tools and procedures) and the threats that those measures were designed to reduce. The methods also involve using the Likert Scale Model to create an ordinal ranking of the measures and threats (See Table 3).

Table 3. Security measures and threats ordinal ranking.

		Prioritization of 10 Cybersecurity Threats										
		1	2	3	4	5	6	7	8	9	10	
		Malware	Phishing	(MitM)	DoS Attacks	SQLi	Zero-Day Exploits	Insider Threats	APTs	Credential Theft	IoT Vulnerable	Total Utility
Utilities	Software Updates	1	10	18	24	50	6	110	8	45	20	**292**
	User Training	7	2	30	40	110	42	56	64	36	100	**487**
	(MFA)	4	4	9	110	110	110	110	32	9	110	**608**
	Network Segmentation	3	110	21	110	110	24	110	16	110	30	**644**
	(IPS)	8	110	24	4	110	48	110	110	110	110	**744**
	Password Policies	110	12	110	110	110	110	110	110	18	10	**810**
	Least Privilege Principle	110	110	110	110	20	110	14	14	110	110	**818**
	Data Backup Plans	9	16	110	36	110	110	110	110	110	110	**831**
	Email Filtering	5	6	110	110	110	110	110	110	54	110	**835**
	Web Filtering	5	8	110	110	110	110	110	110	54	110	**837**
Totals		**262**	**388**	**652**	**764**	**950**	**780**	**950**	**684**	**656**	**820**	**6906**

Note: A score of 110 means that the utility does not apply to the threat.

3. Methodology

3.1. Research Design

This experimental survey research design was used to survey a simple random sample frame of 20 peer reviewed information security research articles. The se-

lection criteria ensured that the articles included a diverse representation of different aspects of network security. Specifically, the articles had to mention various network security tools and procedures, highlighting their effectiveness in mitigating cyber threats. This approach allowed for a comprehensive analysis of current practices and trends in information security.

The peer reviewed information security research articles were scanned for a list of ten network security tools and procedures. The ordinal ranking was done using a Likert scale instrument with a (1 - 10) prioritization of the tools and procedures listed most frequently in the peer reviewed articles. Below is a Flow chart of the Research Design.

Step 1. Find 20 peer review articles that deal with the subject of cybersecurity

Step 2. List those dependent variables (threats) and independent variables (tools and procedures designed to reduce those threats.

Step 3. Using the Likert Scale, prioritize the variables according to how many times they were listed together in the articles.

Step 4. Using expected utility analysis determines if there is a pattern of how often threats are listed with tools and procedures.

3.2. Data Analysis

The data analysis was conducted using a Likert Scale, with a (1 - 10) prioritization of 10 network security tools and procedures and expected utility analysis to conduct a pair-wise comparison of each of the ten tools and procedures to their ability to reduce threats to network security. Decision-makers will understand the gaps between each alternative and the aspiration level [16]. Using expected utility hypothesis based on aspirations, the network security manager can see how one defense in depth security measure can cover a gap that another measure fails to cover. The research methods used in the study provided the advantage of using statistics to make inferences about larger groups, using very small samples, referred to as generalizability [35]. The findings are presented in the results section. The process used to analyze the data involved listing how often the independent variables were reported as reducing the dependent variables. This could imply a correlation between independent and dependent variables. The variables were then prioritized (ranked) and listed on an Expected Utility Hypothesis Scale to identify any possible correlations between the independent and dependent variables.

4. Results

The purpose of this chapter is to present the analysis which reject the H_0 null hypothesis that expected utility analysis does not affect the relationship between the prioritization and combining of 20 Cybersecurity Article's defense in depth tools and procedures (independent variables) and cyber threats (dependent variables). Preferential independence can be described as the preferential outcome of one criterion over another that is not influenced by the remaining criteria [16]. En-

cryption can be seen in a network security expected utility analysis as the preferred security tool for preventing privacy loss.

Data collected before the analysis in this experiment shows a lack of combining security measures and tools to combat specific security threats. The data capture (recording) and coding methodology employed in this study was used to determine the best defense in-depth choices from a list of decision alternatives (network security threats). Finally, a summary of the results is included in this chapter.

5. Investigative Questions

The study design included one investigative question which provided foundation for the main research questions. This section lists the investigative question and includes the statistical analysis to explore the question.

Investigative Question 1

Of the ten network security tools and procedures, prioritize them according to their prioritization from 20 Network Security Articles. Expected utility analysis was then used to array network threats to defense in depth measures. Network security issues, for example, malware, SQL injections and phishing attacks can be graphically displayed using expected utility diagrams.

They can depict the key elements, including decisions, uncertainties, and objectives as nodes of various shapes and colors. The effects of using security tools such as antivirus and procedures such as pen testing can be shown in a utility fashion.

6. Discussion

The current agenda of prioritizing and combining defense in depth measures can continue to evolve based on this investigation. Defense in depth is an effective method of mitigation and prevention of automatic attacks that an organization faces from public internet [7]. Multi-factor Authentication can help to prevent Internet attacks password sniffing for example.

Two types of countermeasures can significantly reduce the risk of such attacks: strong encryption and strong authentication of both devices and users [4]. It is imperative that network security managers deploy strong encryption and authentication on their wireless network as a part of their defense in depth approach. Defense in depth takes a holistic approach to network security, protecting the network from several different perspectives with both tools and procedures.

It is of importance to increase the secrecy capacity by exploiting sophisticated signal processing techniques, such as the artificial-noise-aided security [16]. While working from home, communications must remain private to protect personal and organizational information. The new concept has decision makers setting an aspiration level, though it may not be reachable using current resources, or simply

redesigning the decision space [16]. Defense in depth allows the security manager to be creative in security tool deployment so that he can successfully achieve his security goals.

Secure communications should satisfy the requirements of authenticity, confidentiality, integrity, and availability (CIA) [16]. The goal of defense in depth security is to protect CIA. Communications are also vulnerable to denial-of-service (DoS) attacks [4]. Firewalls and NIDS should also be included in the wireless network defense in depth deployment to prevent DOS attacks.

7. Conclusions

The research concluded that expected utility analysis can play a role in the organization's decision process to array and combine defense in depth measures against network threats. If an eavesdropper lies in the transmit coverage area of the source node, the wireless communications session can be overheard by the eavesdropper [16]. Like how spies operate, eavesdroppers (sniffers) can easily intercept wireless communications. A combination of both security procedures and security tools plays an important role in defense in depth.

An aspiration level could be attained by expanding employees' competence set (e.g., training) or adding or changing new resources (e.g., through strategy alliance, innovation, or creativity) to expand the original decision space [16]. Both administrator and employee training are critical in achieving network security goals and objectives. To maintain confidential transmission, typically cryptographic techniques relying on secret keys are adopted to prevent eavesdropping attacks from intercepting the data transmission [16]. To help meet social distancing requirements, encryption should be used to prevent intruders from tapping into private communications.

Differing from the Internet, the smart grid has only two major directional information flows: bottom-up and top-down [15]. Because of the vertical nature of smart grid communications, redundant communication paths are required to enhance communications. Hackers collect data on different systems; the information collected is analyzed for possible security problems [22]. Stopping this reconnaissance is the first step in preventing an attack.

Organizations can take several steps to reduce the risk of such unintentional DoS attacks [4]. Encryption and authentication are two of many measures that should be taken to prevent both intentional and unintentional DoS attacks. Building interrelationships (dependence and feedback) among criteria and improvement of criteria in general is used to achieve the aspiration level [16]. Deploying defense in depth analytically can help to build the synergy between security tools necessary to achieve organizational security goals.

There are examples of detailed case studies that illustrate successful application of AI and expected utility hypothesis in cybersecurity prioritization in real-world organizational settings. A Fortune 500 international food chain with over 100,000 employees faced significant cybersecurity challenges [36]. Cyclops Security's AI-

powered Risk Prioritization platform helped the organization uncover critical risks by correlating and analyzing security data [36].

The platform identified several critical systems missing required protections and highlighted that two company executives with privileged access rights were accessing critical systems without using multi-factor authentication (MFA) [37]. A study compared the optimal resource allocation to cybersecurity and cyber insurance using Expected Utility Theory (EUT) and Prospect Theory (PT) [37]. The research demonstrated that EUT, which relies on rational decision-making principles, can help organizations optimize their resource allocation by assessing the probabilities and impacts of different threats [37].

Fructification of each layer of model presents vast variety of implementation alternatives and adoptability according to the design and architecture of organization [7]. Each organization will deploy a different variation of defense in depth. A malicious node in wireless networks can readily generate intentional interference for disrupting the data communications between legitimate users, which is referred to as a jamming attack (also known as DoS attack) [16]. Innocent conversations, both business and pleasure can be interrupted by interference.

The smart grid must have the ability to detect the attempt of an intruder to gain unauthorized access to computer systems [15]. Network intrusion detection systems can identify malware that has gained access to the smart grid. Insecure, poorly configured wireless access points can compromise confidentiality by allowing unauthorized access to the network [4]. Network administrators should be professionally trained on wireless network security when implementing wireless networks.

The available published knowledge of expected utility analysis can be used to prioritize defense in depth measures against network threats. This is confirmed by the research conclusion.

Defense in depth decision making can be deployed using EUH to enhance organizational IT security. To make the security policy effective, it must be practical and enforceable, and it must be possible to comply with the policy [4]. Organizations must develop effective network security plans. These plans should be strictly enforced.

Defense in depth and expected utility analysis can be an important asset to the organization. Further advances can be gained in the use of defense in depth by continuing expected utility analysis. The decision space may be modified to achieve aspiration level of the objective space in changeable space situations [16]. The security of portable devices is changing the network security decision space, and defense in depth tools must adapt to meet those changes.

To better understand the role that expected utility analysis can play in IT security this research proposed a expected utility analysis structural and measurement model of the relevant factors. The future of IT security should include additional exploratory models to advance understanding of why the current models are not substantially improving IT security. To understand the shortcoming of current IT security models, further exploratory studies should be conducted on additional models.

Acknowledgements

I would like to thank the reviewers for their detailed comments that greatly improved the paper.

Ethical Considerations

The potential benefits of research in organizations, especially public safety organizations, can be greatly beneficial, but there are risks that some employees or the organization could be unfairly stigmatized. This study was conducted with the informed consent of all the participants.

The participants were not subjected to risk. To avoid conflict of interest, the survey participants are in no way related to the researcher.

Consent for Publication

For specifically addressing an autonomous agency, the design included an informed consent process to ensure that participation was voluntary, with adequate information provided to participants to make their decision of whether or not to participate [38]. Specifically addressing diminished autonomy, while ensuring extra protection is afforded to prevent harm from exclusion.

List of Abbreviations

***Advanced Persistent Threat* (*APT*).** "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception)" [39].

Biometrics. "The measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity" [40].

Botnets. "A botnet is a group of compromised computers under the control of an attacker" [41].

Defense in-depth. "Defense in-depth is the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise. The strategy is based on the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier" [42].

***Denial of service* (*DOS*).** "A denial-of-service attack is an attempt by multiple attackers to make a service unavailable to its users" [43].

Firewall. "A firewall is a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules" [43].

***Hash Algorithm* (*Hash*).** "An *encryption algorithm set* of rules by which information or messages are encoded so that unauthorized persons cannot read them" [40].

Intrusion detection system. Host intrusion detection systems and network intrusion detection systems are methods of security management for computers and networks [44].

***Man-in-the-middle attack* (*MitM*).** "A kind of cyberattack where an unapproved outsider enters into an online correspondence between two users, remains escaped the two parties. The malware that is in the middle-attack often monitors and changes individual/classified information that was just realized by the two users" [45].

Password. "A password is an un-spaced sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user" [46].

***Public Key Infrastructure* (*PKI*).** "A cryptographic element that is the publicly shared half of an encryption code and that can be used only to encode messages" [47].

Phishing. "Phishing is the combined use of fraudulent e-mails and legitimate looking websites by cyber criminals to gain user credentials" [41].

Social Engineering. "Social engineering refers to psychological manipulation of people into accomplishing goals that may or may not be in the target's best interest. In cyber-attacks, it is often used for obtaining sensitive information or getting the target to take certain action (e.g. executing malware)" [39].

Spam. "Spam is the use of e-mail technology to flood mailboxes with unsolicited messages" [41].

SQL injection attacks. "These consist of attacks against web applications with the aim of extracting data or stealing credentials or taking control of the targeted web server" [41].

Watering Hole Attacks. "The concept of a watering hole attack is similar to a predator waiting at a watering hole in a desert, as the predator knows that the victims will have to come to the watering hole. Similarly, rather than actively sending malicious emails, the attackers can identify 3rd party websites that are frequently visited by the targeted persons and then try to infect one or more of these websites with malware" [39].

Worms/Trojans. "Worms and malicious programs have the ability to replicate and redistribute themselves by exploiting the vulnerabilities of their target systems" [41].

Zero-day Attacks. "Zero-day vulnerabilities, *i.e.*, threats that use an error or a vulnerability in the application or the operating system and arise immediately after the vulnerability is found, but before the relevant upgrade is issued" [48].

Conflicts of Interest

The author has no financial and non-financial competing interests.

References

[1] Microsoft Copilot. (2025) Expected Utility Hypothesis. Microsoft Copilot.

[2] Ewing, C. (2010) Engineering Defense-in-Depth Cybersecurity for the Modern Substation. *Proceedings of the* 12*th Annual Western Power Delivery Automation Conference*, Spokane, 13-15 April 2010, 1-5.

[3] Carey, M.J. and Paulsen, G.B. (2017) System and Method for Simulating Network Security Threats and Assessing Network Security. U.S. Patent Application No. 14/837,033.

[4] Fabro, M. (2006) Control Systems Cyber Security: Defense in Depth Strategies (No. INL/CON-07-12804). Idaho National Laboratory (INL).

[5] Cleghorn, L. (2013) Network Defense Methodology: A Comparison of Defense in Depth and Defense in Breadth. *Journal of Information Security*, **4**, 144-149. https://doi.org/10.4236/jis.2013.43017

[6] Mell, P.M., Shook, J. and Harang, R. (2017) Measuring and Improving the Effectiveness of Defense-in-Depth Postures. *Proceedings of the* 2*nd Annual Industrial Control System Security Workshop*.

[7] Rathore, S., Sharma, P.K., Loia, V., Jeong, Y. and Park, J.H. (2017) Social Network Security: Issues, Challenges, Threats, and Solutions. *Information Sciences*, **421**, 43-69. https://doi.org/10.1016/j.ins.2017.08.063

[8] Goztepe, K., Kilic, R. and Kayaalp, A. (2014) Cyber Defense in Depth: Designing Cyber Security Agency Organization for Turkey. *Journal of Naval Science and Engineering*, **10**, 1-24.

[9] Schneier, B. (2006) Security in the Cloud. www.schneier.com/blog/archives/2006/02/security_in_the.html

[10] Meier, K.J., Favero, N. and Zhu, L. (2015) Performance Gaps and Managerial Decisions: A Bayesian Decision Theory of Managerial Action. *Journal of Public Administration Research and Theory*, **25**, 1221-1246. https://doi.org/10.1093/jopart/muu054

[11] Weisberg, S. (2005). Applied Linear Regression (Vol. 528). John Wiley & Sons.

[12] Bernoulli, D. (1738) Specimen theoriae novae de mensura sortis. *Commentarii Academiae Scientiarum Imperialis Petropolitanae*, **5**, 175-192.

[13] Haddawy, P. (1999) An Overview of Some Recent Developments in Bayesian Problem-Solving Techniques. *AI Magazine*, **20**, 11-19.

[14] El-Khameesy, N. and Mohamed, H.A.R. (2013) A Proposed Model for Datacenter in -Depth Defense to Enhance Continual Security. *International Journal of Information Technology and Computer Science*, **5**, 55-67. https://doi.org/10.5815/ijitcs.2013.04.07

[15] Zou, K.H., Tuncali, K. and Silverman, S.G. (2003) Correlation and Simple Linear Regression. *Radiology*, **227**, 617-628. https://doi.org/10.1148/radiol.2273011499

[16] Zou, Y., Zhu, J., Wang, X. and Hanzo, L. (2016) A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proceedings of the IEEE*, **104**, 1727-1765. https://doi.org/10.1109/jproc.2016.2558521

[17] Nilsson, D.K. and Larson, U.E. (2009) A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure. *Journal of Networks*, **4**, 552-564. https://doi.org/10.4304/jnw.4.7.552-564

[18] Bass, T. and Robichaux, R. (n.d.). Defense-in-depth Revisited: Qualitative Risk Analysis Methodology for Complex Network-Centric Operations. 2001 *MILCOM Proceedings Communications for Network-Centric Operations: Creating the Information Force* (Cat. No.01CH37277), **1**, 64-70. https://doi.org/10.1109/milcom.2001.985765

[19] IBM. (2023) Spear Phishing vs. Phishing: What's the Difference? https://www.ibm.com/think/topics/spear-phishing-vs-standard-phishing

[20] CrowdStrike. (2022) What's the Difference between Spear Phishing vs. Phishing? https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/spear-phishing-vs-phishing/

[21] Liu, M.X., Zhang, Q.Y., Zhao, H. and Yu, D.M. (2008) Network Security Situation Assessment Based on Data Fusion. First International Workshop on Knowledge Discovery and Data Mining (WKDD 2008), Adelaide, 23-24 January 2008, 542-545. https://doi.org/10.1109/wkdd.2008.35

[22] Conti, G. and Abdullah, K. (2004) Passive Visual Fingerprinting of Network Attack Tools. *Proceedings of the* 2004 *ACM workshop on Visualization and Data Mining for Computer Security*, New York, 45-54. https://doi.org/10.1145/1029208.1029216

[23] Microsoft (2025) Responsible AI Validation Checks for Declarative Agents. https://learn.microsoft.com/en-us/microsoft-365-copilot/extensibility/rai-validation

[24] Stryker, C. (2024) What Is Artificial Intelligence (AI). IBM. https://www.ibm.com/topics/artificial-intelligence

[25] Fortinet: Fortinet. AI in Cybersecurity: Key Benefits, Defense Strategies, & Future Trends. https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity

[26] Forbes: Vellante, D. (2025) The State of AI Cybersecurity in 2025 and beyond. https://www.forbes.com/sites/danielvellante/2025/02/10/the-state-of-ai-cybersecurity-in-2025-and-beyond/

[27] CrowdStrike (2025) 2025 Global Threat Report. CrowdStrike, Inc. https://www.crowdstrike.com/en-us/global-threat-report/

[28] Chen, J. (2021) Expected Utility: Definition, Calculation and Examples. Investopedia Expected Utility: Definition, Calculation, and Examples.

[29] Microsoft (2025) Security Copilot Use Cases for Security and IT Roles. https://learn.microsoft.com/en-us/copilot/security/use-case-role-overview

[30] Von Neumann, J. and Morgenstern, O. (1944) Theory of Games and Economic Behavior. Princeton University Press.

[31] Sharpe, W.F. (1964) Capital Asset Prices: A Theory of Market Equilibrium under Conditions of Risk. *The Journal of Finance*, **19**, 425-442. https://doi.org/10.1111/j.1540-6261.1964.tb02865.x

[32] ThreatLocker (2024). Dangers of AI in Cybersecurity You Need to Know about. https://www.threatlocker.com/blog/dangers-ai-cybersecurity

[33] Palo Alto Networks (n.d.) What Are the Risks and Benefits of Artificial Intelligence (AI) in Cybersecurity? https://www.paloaltonetworks.com/cyberpedia/ai-risks-and-benefits-in-cybersecurity

[34] National Institute of Standards and Technology (2025) Using Enterprise Risk Management (ERM) and the NIST Cybersecurity Framework (CSF) for Cybersecurity Risk Management (NIST IR 8286B). https://csrc.nist.gov/pubs/ir/8286/b/upd1/final

[35] Cooper, C.R. and Schindler, P.S. (2008) Business Research Methods. 10th Edition, McGraw-Hill.

[36] Cyclops Security (2025) Case Study: Uncovering Risk. https://blog.cyclops.security/case-study-uncovering-risk

[37] ArXiv (2025) Optimal Resource Allocation to Cybersecurity and Cyber Insurance: A Comparative Analysis Using EUT and PT. https://arxiv.org/abs/2411.18838

[38] National Commission for the Protection of Human Subjects (1979) Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research. Department of Health and Welfare.

[39] Chen, P., Desmet, L. and Huygens, C. (2014) A Study on Advanced Persistent Threats. In: De Decker, B. and Zúquete, A., Eds., *Communications and Multimedia Security*. CMS 2014. Lecture Notes in Computer Science, Vol. 8735, Springer, 63-72. https://doi.org/10.1007/978-3-662-44885-4_5

[40] Dictionary, Merriam-Webster (2015) An Encyclopedia Britannica Company. http://www.merriam-webster.com/dictionary

[41] Singh, A. and Bora, M.S. (2013) Cyber Threats and Security for Wireless Devices. *Journal of Environmental Science, Computer Science, and Engineering & Technology*, **2**, 595-601.

[42] Rouse, M. (2007) Defense in Depth. https://www.techtarget.com/searchsecurity/definition/defense-in-depth

[43] Cobb, M. (2014) Firewall. http://searchsecurity.techtarget.com/definition/firewall

[44] Cole, B. (2014) What Is an Intrusion Detection System (IDS)? http://searchcompliance.techtarget.com/definition/intrusion-detection-systems-IDS

[45] Mallik, A., Ahsan, A., Shahadat, M. and Tsou, J. (2019) Man-in-the-Middle-Attack: Understanding in Simple Words. *International Journal of Data and Network Science*, **3**, 77-92. https://doi.org/10.5267/j.ijdns.2019.1.001

[46] Merriam-Webster (2020) Password. Merriam-Webster.com Dictionary. https://www.merriam-webster.com/dictionary/password

[47] Merriam-Webster. (2020) Public-Key. In Merriam-Webster.com Dictionary. https://www.merriam-webster.com/dictionary/public-key

[48] Pavlyushchik, M.A. (2014) System and Method for Detecting Malicious Code Executed by Virtual Machine. U.S. Patent No. 8,713,631.