4-2023

Active Cyber Defense in the Healthcare Sector

Evelyne Diaz Araque
Clark University, EDiazAraque@clarku.edu

4-2023

Active Cyber Defense in the Healthcare Sector

Evelyne Diaz Araque
Clark University, EDiazAraque@clarku.edu

CHALLENGE CONVENTION.
CHANGE OUR WORLD.

Active Cyber Defense in the Healthcare Sector

Evelyne Diaz Araque

Master's of Science in Information Technology, Clark University

Capstone Research Thesis

Professor Richard Aroian

April 30, 2023 – Spring 2023

Acknowledgements

I would like to thank my incredible support network for their continuous support on this project and in all my journey at Clark University: Gloria, Laura, Noam, Luis Fernando and Sandra, Amantina, Sandra, Johan, and Dario. I would like to thank my career-long mentors, Professor Kenneth Basye, Professor Robert Tobin, Professor Gene Grella, Professor Peter Wyner, Professor Richard Cehon, Professor Kevin Longo, Professor Enrique Laso Sanz, Betty Jean Jaskoviak, Professor Frederic Green, Professor Catalin Veghes, Professor Jacqueline Morrill, Professor Richard Aroian, Professor Scott McCarthy and last but not least, Professor Li Han; I could have not asked for a better role model to accompany me in my journey at Clark. I will forever cherish our conversations and the way you approached and taught me to confront every obstacle with incredible grace, firm assertiveness, and virtuous leadership.

Additionally, I want to thank my community, Michal and Mai Igell, Timna Perets, Benjamin Tchetchik, Sigal Rozen, Yotam Monk, Rotem, Gali and Neta Ginossar, Amy Singer and David Katz, Efrat Ben-Avraham, Sarah Benhfid, Orr Makonnen, John Edwin Porras, Yotam Constantini, Zen Amir, Minh Vu, Iona Temple, Amit Wagner, Tamar Arbel, Tally Kritzman-Amir, Eviatar Naor, Kul Kulton, Tali Limon, Ronit Kadishay, Michal Sivan, Santiago Santamaria, Elad Zamir, Jeff and Judy Narod, the Mejia Santos family, the Sanchez family, Shuki Zadok, Lisa Dobson, Kate Bielaczyc, Caitlin Marie Schubert, Demet Sentürk, Fatima Diallo, Marla Bazile, Sara Vera-Cruz, Sarah Vacca, Chloe Tomblin, Caroline Murphy, Sharon Krefetz, Savior Watts, Finn O'Driscoll, Sam Mescon, Akhmad Kurbanov, Jamie Yeo, Frank Armstrong, Stephen DiRado, Nati Botero, Adryana Hutchinson, Dalton Grady, Zohar Kafri-Shushan and Elana Rudavsky.

Lastly, I would like to dedicate this hard-earned accomplishment to my mother, the strongest woman I have come to know in my life. Your tenaciousness, courage and resilience through countless adversaries has always been the fire inside of me and for that, I will be forever indebted.

In loving memory of Tally Kritzman-Amir and Robert Tobin, gone too soon.

Table of Contents

Abstract

The healthcare industry is a vulnerable sector when it comes to cybercrime. To date, it continues to suffer the highest losses for twelve consecutive years (IBM, 2022). As care-providing systems depend more and more on technology, information assets become an appealing target for cyber criminals. Health data often contains sensitive and identifiable information such as full names, addresses, phone numbers, emails, Social Security Numbers, etc. All these falls under the term Personal Identifiable Information (PII) which are protected by many laws and acts with the purpose of protecting one's privacy from harms such as identity theft and other fraudulent offenses. In addition to the privacy concern, there is also financial and reputational concerns involved.

The health sector suffers frequents attacks and the number continues to grow every year. The purpose of this research thesis paper is to analyze the cyber defense technique Active Cyber Defense (ACD) in relation to the healthcare sector. It seeks to investigate the ways in which the health sector can benefit from incorporating ACD in its security strategy as well as analyzing the various security challenges that the health sector faces and how it attempts to address them. This research will be supported by research papers, government documents, reports, and articles.

1 Introduction

1.1 Introduction to Cyber Space

The introduction to this paper will explore the origins of both cybersecurity and cyberspace, i.e., the internet, because in order to understand the importance of cybersecurity one must understand first the origin of cyberspace as a whole.

The internet as we know it today dates back to the 1960s as a project called ARPANET created by Robert W. Taylor who drew inspiration from J. C. R. Licklider's philosophies (Markoff, 1999). ARPANET stands for Advanced Research Projects Agency Network of the US Department of Defense (DoD). The ARPANET was a project aimed to research the network communications and data resource-sharing for military purposes (Hauben, 1997). The biggest use of ARPANET was for electronic mailing to support communication between individuals in a confined local network (Hauben, 1997). This was possible through a then-innovative concept called "packet-switching" (Lee, Vox, 2014). Packet switching essentially means breaking down data into miniature "packets" in order to effectively transmit it over a network (Lee, Vox, 2014).

The ARPANET in 1969:

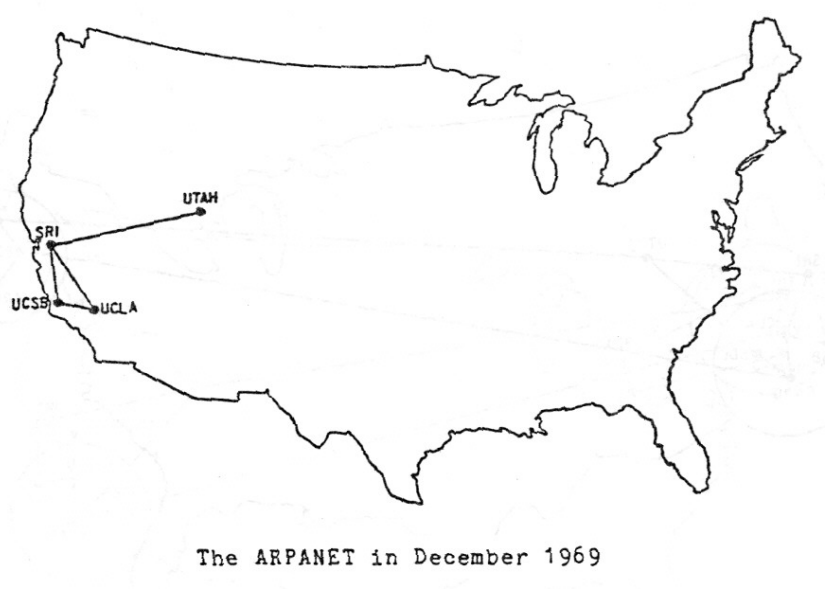

Image: Chiappa, MIT, 2014

Well until the ARPANET era, computers operated in a rather archaic and inefficient way. The people that operated the computers, which were easily of the size of a living room, used punch cards to type their code, then they would stack the punched cards and feed it into the "local computer center" (Hauben, 1997). Processing time was immensely long very often taking a whole day to process several lines of code. Programmers regularly had to wait over a day to see the outcomes of their code, and if there was a bug, they would have to wait another day to see if they managed to fix it (Hauben, 1997). If another bug was found, it would take another day of processing, and so on, so the overall process of debugging was tedious and impractical. Not surprisingly, people had to come up with better and more effective ways to work with computers. Slowly, the concept of time-sharing started to immerse thanks to the pioneers Fernando Corbato and Robert Fano (Hauben, 1997). Time-sharing would, hypothetically, allow users to use a computer at the same time all the while giving them the "impression" that they are the only ones using the computer (Hauben, 1997). This concept served as a cornerstone in computer networks, and it also shed light over the social implications it was bound to bring. In Corbato's and Fano's words: "The time-sharing computer system can unite a group of investigators in a cooperative search for the solution to a common problem, or it can serve as a community pool of knowledge and skill on which anyone can draw according to his needs." (Hauben, 1997).

Following the time-sharing ideas, J. C. R. Licklider, the director that founded ARPA's Information Processing Techniques Office (IPTO) started to envision time-sharing as an "interactive computing" process in which the user will have the ability to interact in real-time with the computer all the while it processes the user's requests, something that was not feasible with batch computing (Hauben, 1997). Licklider was a crucial visionary at the time because under his command as the IPTO's director he was able to allocate a lot of funding and resources to the research that will in years later birth the internet. Another important

trailblazer was Robert Taylor. Taylor later served as the director of IPTO after Licklider and in interviews he always regarded Licklider as the figure that never ceased talking about "intergalactic network" to plant the seed of that idea in everyone's mind. Taylor recalls that Licklider used that term to refer to the immense capability of "interconnected" communities that can be created by users that benefit from time-sharing in computing networks (Hauben, 1997). This largely meant that people with common interests could be connected and exchange information while being in different locations (Hauben, 1997). Licklider's vision at such an early time set the ground for many university researches that continued expanding the notion of computer networks (Hauben, 1997).

In April 1968, Licklider and Taylor wrote an article with the title, *The Computer as a Communication Device*, which easily can be considered as the prediction of the global network as we know it today: "We believe that communicators have to do something nontrivial with the information they send and receive. And we believe that we are *entering a technological age* in which we will be able to interact with the richness of living information—not merely in the passive way that we have become accustomed to using books and libraries, but as active participants in an ongoing process, bringing something to it through our interaction with it, and not simply receiving something from it by our connection to it." (Licklider & Taylor, 1968). An important aspect to draw from Licklider's and Taylor's piece is the shift in "social dynamics" that they foresaw, far beyond the hardware and software dynamics that were, too, ahead of their time (Hauben, 1997). One of the concerns that Licklider and Taylor raised in their article was the question of accessibility and whether the future infrastructure will be built to allow everyone equal access (Hauben, 1997). Licklider and Taylor both stressed the importance of allowing anyone who wants access to information through a computer system to have it, one can only hope that as a global society we continue to pursue Licklider's and Taylor's "principle of equality of access" (Hauben,

1997). In an interview for NYT, Taylor reiterated: “I want the internet to become a right, not a privilege” (Markoff, 1999).

Following the work that Taylor accomplished with ARPANET, he then left to work for the University of Utah which ended up birthing the personal computer in the early 1970s (Markoff, 1999). In the NYT article, Markoff inquires Taylor regarding the “next major burst of innovation” after the personal computer to which Taylor replied: “Broadband networks”. By then, it was clear to Taylor that the concept of computer network will only continue to evolve (Markoff, 1999). By 1975, ARPANET had become an international phenomenon with over 50 nodes from the USA to “Norway and London” connected through “satellite link” (Lee, Vox, 2014).

The ARPANET in 1975:

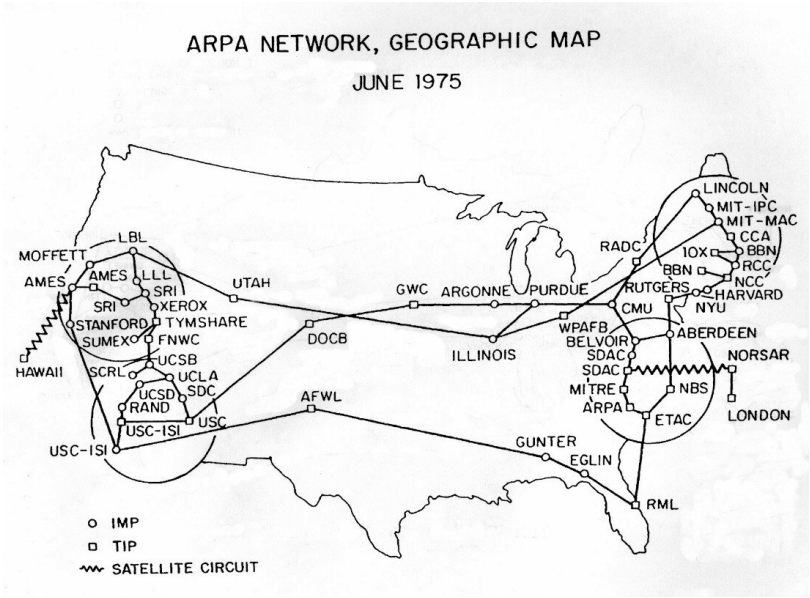

Image: Chiappa, MIT, 2014

What once served only the military and the academia slowly started transitioned into something larger. With that premise in mind, the US military which was the entity that managed ARPANET at the time, understood that the network will soon grow and turn “unmanageable”, therefore the military commissioned computer scientists Robert Kahn and

Vint Cerf in to create global standards that would allow different networks to communicate creating a "shared internet" (Lee, Vox, 2014). On January 1, 1983, ARPANET officially transitioned to the TCP/IP protocol created by Kahn and Cerf and with that, modern internet was initiated turning the internet into the biggest "network of networks" in the world (Lee, Vox, 2014). From the user's end this new protocol standard did not change much, however, from the network stand-of-point it became dramatically easier for new networks to emerge and enter the internet domain (Lee, Vox, 2014).

1.2 Introduction to Cybersecurity

With the progress made with resource-sharing computer systems new threats began to emerge and thus in June of 1967, ARPA director was commissioned to create a "Task Force to study and recommend hardware and software safeguards that would satisfactorily protect classified information in multi-access resource-sharing computer systems" (Ware, 1970). Naturally, Robert W. Taylor was appointed to oversee this newly formed Task Force. The Task Force consisted of twenty members that formed a "Steering Group", a policy panel and a technical panel and was "under the authority of the Defense Science Board" (Ware, 1970). As resource-sharing systems was mostly used for military and academic purposes, it is fair to say that the need to protect systems originated in wanting "to store and process classified information" (Ware, 1970). Resource-sharing essentially meant that many users could use a system while sharing the same "primary [computer] memory" and this inherently posed a problem to the owners of the classified information, therefore creating the need for laws and regulations in regards of computer systems (Ware, 1970).

Computer Security pioneer, Willis Ware, author of the paper, *Security Controls for Computer Systems*, colloquially known as The Ware Report, explains that there's need not only to protect the user from another user but also "by the system itself" (Ware, 1970). The Ware Report was the foundation for computer security and since it was written it has been

regarded as the cornerstone for Computer Security. It was published internally in 1970 and was made public in 1979 (Ware, 1970). In the paper, Ware outlines the ever-growing "Security Problem" in resource-sharing systems which is the inability to control every terminal particularly because of the nature of the systems which are "widely spread geographically" (Ware, 1970). Ware talks about the first apparent principle, "isolation – simply removing the entire system to a physical environment in which penetrability is acceptably minimized" (Ware, 1970). Of course, as said earlier, this principle becomes inadequate when the systems are distant and located in different locations (Ware, 1970).

In the Ware Report, Willis Ware cites five types of computer vulnerabilities:

a. Accidental Disclosure – refers to hardware, software or "subsystems" malfunctions which results "in an exposure of information" (Ware, 1970). This clause emphasizes cases in which there is no "deliberate intent" of causing harm (Ware, 1970).
b. Deliberate Penetration – refers to cases in which there is a deliberate intention of penetrating a system and 1) gaining access over information, 2) manipulating the system to behave per the threat actor's desires, or 3) disable the system so that it can no longer carry out its normal functions (Ware, 1970).
c. Active Infiltration – refers to cases in which a legitimate user gains access to parts of the system to which they have no authorization for. This clause largely refers to cases in which a legitimate user abuses their privileges in the system to perform fraudulent actions; this can be creating or exploiting "trap-doors" and "loopholes" to bypass security controls and access unauthorized data to maliciously make use of it in the present or future (Ware, 1970).
d. Passive Subversion – refers to cases in which malicious controls are placed in the system to exfiltrate data in a passive manner without interrupting security controls or

manipulating the system itself (Ware, 1970). One example given here is that of "the wire tap" which is similar to tapping a telephone line.

e. Physical attack – refers to attacks in which the physical integrity of the systems is compromised such as in a "mob action" (Ware, 1970).

It is astonishing to note that this prototype of vulnerabilities continues to be relevant today. Going off the vulnerabilities concern, the following are the "General Characteristics" that Willis Ware considers vital to have for a "secure system":

a. Flexibility – the system must be "flexible" so that appropriate changes can be made when security concerns fluctuate. This can be in the form of "shifting job assignments, issuance and withdrawal of clearances, changes in need-to-know parameters, transfer of personnel", etc.
b. Responsiveness – the system should be "responsive" to shifts in "operational conditions" for example, during emergencies. Ware also recommends designing built-in capabilities of disabling or pause "security controls, impose special restrictions, grant broad access privileges" to specific individuals, etc.
c. Auditability – the system should be "auditable" so that security personnel can monitor its "performance, security safeguards, and user activities".
d. Reliability – the system should be "reliable" in the sense that it should be designed to operate in a "fail-safe" manner; meaning it can withhold access and information should the user fails to pass "security self-checks".
e. Manageability – the system should be "manageable" from a security stand-of-point; meaning that the system should be in complete disposition to make dramatic changes if the system faces "catastrophic system failure, degradation of performance, change in workload, or conditions of crisis".

f. Adaptability – the system should be "adaptable" so that security controls can be adjusted according to the needs of the information (higher sensitivity over lower sensitivity, etc.) in an economic manner.
g. Dependability – the system should be "dependable" so that it does not "deny service to users" in moments of crisis; the system should strive to be "self-protecting" in a way that it allows legitimate users access in alarming situations.
h. Configuration Integrity – this essentially means that the system must test itself regularly to ensure that its security controls are in place and working; the system should attempt to self "violate its own safeguards deliberately" to ensure its security is up to date.

1.3 Cyber threats

Theories about self-replicating automata traces back to 1966 when John Von Neumann published his paper, *Theory of Self-Reproducing Automata*, in which he makes strong comparisons between the natural automata, the human body, and the artificial automata, a computer machine and how the artificial automata can mimic the behavior of a biological virus such as replicating itself and spreading in its vicinity (Von Nuemann, 1966). In that paper, Von Neumann suggests rather philosophical views on automatons, for example that it is impossible to determine whether an automaton is "good or bad, fast or slow, reliable or unreliable" without knowing the environment in which it operates (Von Nuemann, 1966). The correlation between that and computer threats might not be clear and direct, but it is right to say that for such premature stage of computing it was certainly scratching the surface of the concept of computer threats and how it could potentially evolve in the future.

1.4 Most prominent early cyber threats

The very first evidence of computer threats known to literature started roughly from late 1970s until early 1990s, most of them being "experimental" in nature (Chen, 2005).

Consequently, the viruses targeted mainly MS DOS which stands for Microsoft Disk Operating Systems as these made up the majority of the early machines (Chen, 2005). The first computer threat documented was the “Creeper”, a computer worm in today’s terms, written by Bob Thomas and Ray Tomlinson at Bolt, Beranek & Newman Inc. (BBN) in 1971 (Chen, 2005). The “Creeper” replicated and propagated itself in the ARPANET displaying the message “I’M THE CREEPER: CATCH ME IF YOU CAN” (Chen, 2005; Russell, Gangemi, 1991; Core War, 2023):

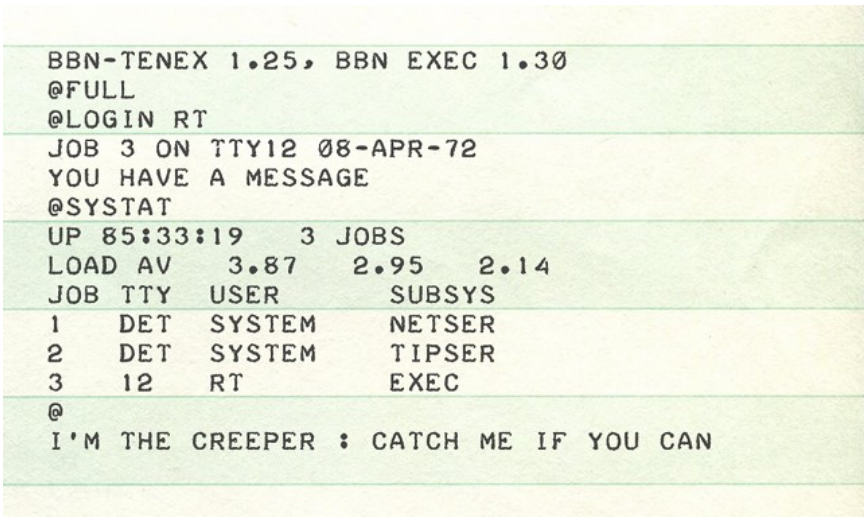

Image: Core War, UK

To eliminate the “Creeper”, Ray Tomlinson created the counterpart, the “Reaper” to move in the ARPANET and remove all the copies of the “Creeper” (Russell, Gangemi, 1991; Core War, 2023). The term computer “worm” was coined by John Shoch and Jon Hupp in 1979 and was inspired by the “Creeper” (Chen, 2005). A computer worm refers to a separate and disconnected program that its sole purpose is to “exploit the network” it resides in and to “seek out vulnerable computers to infect with a copy of themselves” and as opposed to viruses, worms do not require human execution and thus are completely independent (Chen, 2005).

In 1982, Elk Cloner, the first documented virus was released to the “wild” by computer programmer and high school student, Rich Skrenta. Skentra was fifteen-years old at

the time and he copied the program onto a floopy disk and shared it with the circle of friends he used to play with (Sydney Morning Herald, 2007). In 1983, Fred Cohen, a USC student coined the term "computer virus" and much like a biological virus, a computer needed a host in order to operate, it also depended on the neighboring environment (Chen, 2005). In 1987 a virus named "Christmas Exec" was one of the first viruses to propagate via e-mail in IBM mainframes and probably one of the first occurrences of "social engineering" since it convinced the user to launch the program and thus initiate the virus (Chen, 2007).

On Nov. 2nd, 1998, the infamous "Morris Worm" created by Cornell student, Robert Morris, paralyzed 6000 machines which constituted "10% of the internet at that time" and became the first worm to cause real harm in the era of internet (Chen, 2005). Morris was the first person in the US to ever be convicted for a cybercrime under the Computer Fraud and Abuse Act of 1986 (Denning, et al. 1994). The investigations ended in a conviction in 1991 concluding that there was no real intent of harm. Morris was sentenced to three years on probation; he was fined $10,050 and was mandated to fulfill 400 hours of community service work (Chen, 2005; Denning, 1994).

Fast forward to today, computer safety continues to be a challenge for the computer community worldwide. This is particularly true because it is virtually impossible to build software that is free from vulnerabilities, hence there will always be flaws to exploit by threat actors (Chen, 2005). And as software grows more complex so does the capacity to keep it secure (Chen, 2005). As Willis Ware said: "…the expanded problems of security provoked by resource-sharing might be viewed as the price one pays for the advantages the systems have to offer."

2 Active Cyber Defense (ACD)

2.1 Introduction to Active Cyber Defense

Modern western warfare strategy, which inevitably made its way to cyber warfare, is historically based on the renowned script *The Art of War* by Chinese general, military strategist and philosopher Sun-Tzu (Sawyer, 1993). The script, consisting of thirteen chapters, is considered to be "China's oldest and most profound military treatise" (Sawyer, 1993). It is estimated that the script was written in "the last years of the sixth century B.C." and while there are many other warfare scripts from the East from later years, this managed to turn into the holy grail of modern warfare strategy (Sawyer, 1993).

Sun-Tzu said:

> *"To be certain of an impregnable defense, secure positions which the enemy will not attack. Thus when someone excels in attacking, the enemy does not know where to mount his defense; when someone excels at defense, the enemy does not know where to attack."*

Sun-Tzu's general tactic consisted of deploying manipulative approaches on the enemy in order to create momentum for an effortless triumph (Sawyer, 1993). While studying Sun-Tzu's script I came across remarks that explicitly referred to the need of being active, even when defending: "The army should always be *active*, even when assuming a defensive posture, in order to create and seize the temporary tactical advantage that will ensure victory. Avoiding a strong force is not cowardice but indicates wisdom because it is self-defeating to fight when and where it is not advantageous." (Sawyer, 1993).

Active Cyber Defense (ACD) was and continues to be controversial in the cyber security community, this is largely due to the misconception that ACD revolves around "hacking back", indiscriminately and irresponsibly (Denning, 2013). This misconception could not be farther from the reality. ACD focuses on synchronization, real-time detection, intelligence gathering, analysis, and mitigation of threats before they take place (Rosenzweig,

2013). In the prolific essay, *Framework and Principles for Active Cyber Defense,* renowned security researcher Dorothy E. Denning explains the various reasons why this misconception is erroneous. In the essay, Dr. Denning carefully draws comparison lines between active air and missile defense (AMD) and active cyber defense (ACD) to highlight the importance of ACD and why is it critical that we, as a community, adopt it (Denning, 2013).

Starting from the definition of active air and missile defense: "direct defensive action taken to destroy, nullify, or reduce the effectiveness of air and missile threats against friendly forces and assets (Denning, 2013). Dr. Denning suggests the replacement of the term "air and missile" with "cyber" to result with Active Cyber Defense (ACD) and its definition, namely: "Active Cyber Defense is direct defensive action taken to destroy, nullify, or reduce the effectiveness of cyber threats against friendly forces and assets" (Denning, 2013).

Dr. Denning follows to describe ACD by four parameters:

a. Scope of effects, whether its deployment is internal or external. To continue with the air defense comparison, an internal response would take place when a threat has penetrated a "country's airspace" and the measures taken to thwart the attack are within its own territory as opposed to thwarting an attack in someone else's territory (Denning, 2013). In cyber defense the parallel would be to thwart an attack on your network by imposing internal restrictions like blocking IP addresses or implementing Intrusion Prevention Systems (IPSs) and Intrusion Detection Systems (IDSs), an external response can be taking down a command and control (C2) server or planting spyware in the attacker's system (Denning, 2013).
b. Degree of cooperation, whether its deployment is cooperative or non-cooperative. For instance, a cooperative deployment in air defense can look like agreeing to a call for help from an ally country to counter an attack in their own territory in contrast to counter an attack without the consent and cooperation of local authorities (Denning,

2013). In cyber defense the equivalent non-cooperative scenario is when the defender confronts the attacker or lures the attacker into disclosing key information. An example is when the defenders take active measures to "hack back" the attacker either by planting decoys or deception tools like honeypots or spyware (Denning, 2013).

c. Types of effects: i) sharing threat information like IP addresses of malicious actors, ii) collecting information about the threat, iii) blocking execution of programs or traffic from suspected malicious actors, and iv) preemption effects are those that repress and "eliminate" means used in the attack (Denning, 2013).

d. Degree of automation, whether the deployment was done manually or automatically. Most security controls in air defense and cyber defense are bound to be both manual and automatic because they require human intervention in various stages (Denning, 2013). And even with crafting the best automated processes it is likely that "affirmative action" to be needed by humans (Denning 2013). Take for example in air defense, shooting down a foreign object is a sufficiently serious action to trust only computer decision-making with it (Denning, 2013). In cyber defense it is similar, executing hostile actions cannot be left to the judgement of algorithms only (Denning, 2013).

To challenge the misconception that ACD is indiscriminate and unscrupulous, Dr. Denning offers the following ethical and legal principles to which ACD should always abide by:

a. Authority – ACD should be used only when it abides by "laws, contracts, and policies" enforced by its appropriate jurisdiction, whether it be a company or a state. Governmental entities are the only ones to have authority to carry out hostile

"external non-cooperative" action against attackers both in air defense and in cyber defense.

b. Third-party immunity – ACD should seek always to abstain from "intentionally" harming third parties. Similar to warfare principles, "noncombatants" and their property should not be at the crosshair of a defender.
c. Necessity – ACD should be used when it is essential to reduce the harm and stop the attacker, ACD should not be used as means for "retaliation or retribution".
d. Proportionality – ACD should only be used when the positive outcome outweighs the costs or harm that could result from the deployment of ACD.
e. Human involvement – the implementation and deployment of ACD should be carefully supervised by humans for all critical decision-making. Nevertheless, it is also highly important to know when to avoid interrupting processes that can be carried out more effectively and efficiently by computers like the processes performed by IPSs, IDSs, firewalls that are vital to maintain a secure perimeter.
f. Civil liberties – ACD should strive to ensure the "civil liberties" of all individuals affected in its deployment. Liberties like right for privacy, freedom of speech, and freedom of association should be preserved indiscriminately and equally among all stakeholders including "suspects".

By equating active air defense and active cyber defense, Dr. Denning manages to show the indispensability of active cyber defense when it is applied with absolutely necessity while preserving ethical and legal principles like authority, third-party immunity, proportionality, human involvement and civil liberties (Denning, 2013). Furthermore, Dr. Denning reminds the reader that ACD is in fact already applied in many security controls regularly used, such as whitelisting/blacklisting, authentication systems, anti-viruses, firewalls, IPSs and IDSs, and more (Denning, 2013). Thus, Dr. Denning's essay is not only

arguing ACD's effectiveness but also asking to recognize that the security community has been indeed benefiting from ACD's qualities since the invention of the mechanisms mentioned above.

2.2 Evolution over time

A more modern reference to warfare tactics involving active defense is in the dictionary, *Department of Defense Dictionary of Military and Associated Terms,* published in 1984 where the definition for active defense is the following:

"The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy." (DoD, 1984).

As mentioned earlier in this paper, a vast majority of the strategies and tactics for cyber defense were adaptations from military methodologies. In order to elaborate on Active Defense as a methodology we will first examine the concept within the DoD domain. For that purpose, it is necessary to recall that the internet's birth was largely facilitated by the US Department of Defense in the ARPA research group. As such, we will discuss the topic referencing the 2001 paper, *Active Computer Network Defense: An Assessment,* by Major of the USAF, Eric J. Holdaway (Holdaway, 2001). In the paper, Holdaway claims that most of the defenses, up until the time that the paper was written were passive defenses. And while that was suitable for the threats existing in that era, it is no longer going to be practical or sufficient as the security threats and incidents are growing at an exponential rate (Holdaway, 2001). Holdaway then proceeds to expand on what is active defense, in his words active defense "originate[s] by the defender against the attacker" and it aims to "at least thwart any attack in the progress, and ideally make further attacks more difficult." (Holdaway, 2001). He then presents three types of cyber active defenses:

1. Counterattack – as its name suggests, it aims to carry out a computer network attack (CAN) in real-time or immediately after the original attack was launched. This will

require an incredibly fast response from the defender's end as well as locating the source of the attack which can oftentimes become the real challenge. To successfully track down an attacker's source it is likely that the defender will need to navigate through private networks and while there are "international agreements" that can facilitate the process, there is no guarantees that that would always be the case (Holdaway, 2001).

2. Pre-emptive attack – it aims to counterattack the attacker's "information systems infrastructure" to impede from the attacker to successfully proceed with the attack. Since this method is "hostile" in nature, it is to be expected that only state actors can use this form of counterattack against other known hostile actors. The main goal of this methodology is to "disable and destroy [the attacker's infrastructure] before they can be effectively used", this can include destroying network scanners, packet sniffers, "password crackers" and command and control (C2) servers (Holdaway, 2001).
3. Active deception - it aims to "channel an attack away" in a way that the defendant uses the "momentum" in their favor to defeat the attacker. Holdaway used judo as an example for when you are leading your attacker astray into thinking they are succeeding when in reality they are being "neutralized" (Holdaway, 2001). One way to achieve this could be creating a "trap door" which will redirect the attacker into a false network, tricking them into thinking they are gaining control while being observed without knowing. This methodology can provide a great deal of intel about the attacker's techniques, tactics and procedures (TTPs) which the defender can exploit in their favor to prevent future attacks.

In the summary of the paper, Holdaway makes a strong case for incorporating passive defense and active defense as a synergy that can benefit the welfare of an information system

as they differ greatly in their approaches and practicality (Holdaway, 2001). One thing is certain, sticking to the manual can be difficult to apply when an attack is underway so having options is likely to be advantage rather than a disadvantage.

In a different paper titled, *Implementing Active Defense Systems on Private Networks*, Josh Johnson instructor at SANS Institute, explains the importance of integrating defensive means in different stages of the cyber kill chain with the goal of sabotaging the attack: "…as long as the successful completion of the final phase is prevented, the overall defense can be considered successful." (Johnson, 2021). Examples of defensive measures can be placing honeypots in different areas of the network and monitoring ports for suspicious activity. Johnson warns about the dangers we face nowadays, social engineering being at the heart of them (Johnson, 2021). For instance, Johnson explains how "technology savvy" officials fall victim to malicious attacks, and he assures that if they fall, it is to be expected that others will do, too. Part of the problem, according to Johnson, is that malicious actors continue to evolve in their tactics making it easier to take down systems, exfiltrate data, create backdoors and bypass security controls without being detected (Johnson, 2021). And while it is imperative that systems have Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) on most occasions it is simply not sufficient to detect and stop an attacker who is present on your network. In his paper, Johnson talked more specifically about private networks due to liability concerns, however the references used in this section are relevant in both private and public networks.

2.3 Active Cyber Defense Techniques

2.3.1 Predictive Analytics

Predictive analytics is a powerful tool that cybersecurity professionals have adopted in their attempt to not only predict future outcomes through analysis of "past and current data" but also help develop better and stronger defense strategies (Flynn, 2022). In its essence,

predictive analysis uses “data analytics” to create models correlating old and present data with the goal of predicting possible future scenarios (Flynn, 2022). Predictive analysis’ first step is to “determine vulnerability”. Every company or sector will face a different set of threats and understanding them is the first big step in protecting your network. After the vulnerabilities have been defined, the analytical models “compare” the organization’s security controls in place with current “cybercrime trends” across other competitors in the same domain (Flynn, 2022). A great aspect of predictive analysis is that it can help the defense team understand where and how they might get hit and most importantly, whether the systems can successfully tolerate it (Flynn, 2022). Another rising trend of predictive analysis is helping gauge which is the most appropriate “cyber insurance” and with data breaches becoming more and more prevalent it is to be expected that predictive analysis continues to evolve, too (Flynn, 2022).

Two big players in predictive analysis are of course Artificial Intelligence (AI) and Machine Learning (ML), both growing fields in the past couple of years (Flynn, 2022). What a human can do in several hours, AI can do in seconds so it’s natural that AI becomes part of the cybersecurity landscape. QuadMetrics, an industry analytical giant founded by Dr. Mingyan Liu, a researcher from University of Michigan, manages to achieve predictive accuracy 90% of the time and only 10% of it are false positives (UMich, 2016). Another example of AI efficiency is its ability to pick on user’s behavior. Every person has a different way of interacting with a computer and AI can pick on those patterns and compare it with unauthorized behavior to alert when intruders may be present in the system (Flynn, 2022). The action of “predicting attacks” per say is largely achieved through machine learning (ML) tools. For instance, ML can track “malicious activity in other networks” to determine the likelihood of that happening to your network or it can follow known problematic IP addresses to alert about it (Flynn, 2022). This takes us to the next technique, behavioral analysis.

2.3.2 Behavioral Analysis

In 2016, the SANS institute published a whitepaper, *Using Analytics to Predict Future Attacks and Breaches,* by Dave Shackleford. In the paper Shackleford thoroughly explains why it is vital not only to focus on prevention but also on early "detection and response" (Shackleford, 2016). Shackleford firmly believed that attackers were benefiting from companies' lack to locate the indicators of compromise (IOCs) quickly enough, and because of that, defenders were facilitating things for the attackers instead of thwarting them (Shackleford, 2016). Interestingly, in the paper Shackleford introduced the notion of sandboxes, a tool that is the primary tool for defense professionals. He called it "detonation platforms" meant to evaluate and see the behavior of malicious code in action in a controlled and safe environment (Shackleford, 2016).

Every user has a different way of engaging with systems. Attackers, on the other hand, tend to move farther and farther from the limits of normalcy and that is where behavioral analysis becomes an asset in cybersecurity (VMware, 2023). Behavioral analysis is supported by machine learning (ML) and various algorithms that try to process large amounts of "unfiltered endpoint data" to determine where normal behavior starts and where it ends (VMware, 2023). Some of the things that security experts study in behavioral analysis are "events, trends, and patterns" both in present and past. Tracking and analyzing abnormal behavior can be highly insightful for defense professionals (VMware, 2023). It can achieve better "visibility" on the systems and shed light over "root causes" that can help prevent the next attack. But what is abnormal behavior? well, abnormal behavior can be a wide array of things, for example multiple log-in attempts after work hours, sudden files modifications, unexpected low computer performance, irregular system behavior, high data movement across systems and more (Roebuck, 2021; VMware, 2023). The main challenge is that attackers continue to develop sophisticated tactics, techniques, and procedures (TTPs) and

that broadens the spectrum of abnormalcy in a way that makes it harder to track TTPs (VMware, 2023). It is worthwhile mentioning another branch of behavioral analysis, system behavioral analysis, which is essential particularly in the post-attack forensic efforts. Similar to human behavioral analysis, system behavioral analysis works by analyzing the logs created after any action takes place in a system to create models and patterns that reveal system flaws that the attacker might have exploited (Skopik, et al., 2022).

2.3.3 Adaptive Security

Adaptive Security Architecture was coined by Sun Microsystems in 2008. The goal of this methodology was to foresee, react to and "contain threats" all the while minimizing the threat surface, speed, and improving "recovery time" (Brook, 2018). The origin of this idea stem from biological systems which similarly to adaptive security can react to new threats and adapt to new environments by triggering the immune system (Brook, 2018). The difference between traditional measures like IDS/IPS, firewalls, whitelisting, anti-viruses, and adaptive security is that the adaptive security model monitors the threats continuously and changes accordingly to create a better defense perimeter (Brook, 2018). The traditional methods are passive by default as they will get triggered if an attack is underway, while adaptive security aims to be active all the time. Some of the advantages of implementing adaptive security are early detection, containing the event promptly as it occurs, its ability to discover ongoing security vulnerabilities, and halt the infection of the malware (Brook, 2018). According to Gartner, the four stages for adaptive security are (Gartner, 2017):

a. Predict – analyze risks, rank exposure, foresee threats and attacks, and incorporate baseline systems and security measures.
b. Prevent – strengthen and isolate systems, thwart attacks.
c. Respond – repair, modify policy accordingly, research incidents, perform reflective assessment.

d. Detect – detect incidents, validate risks and profile them, contain incidents.

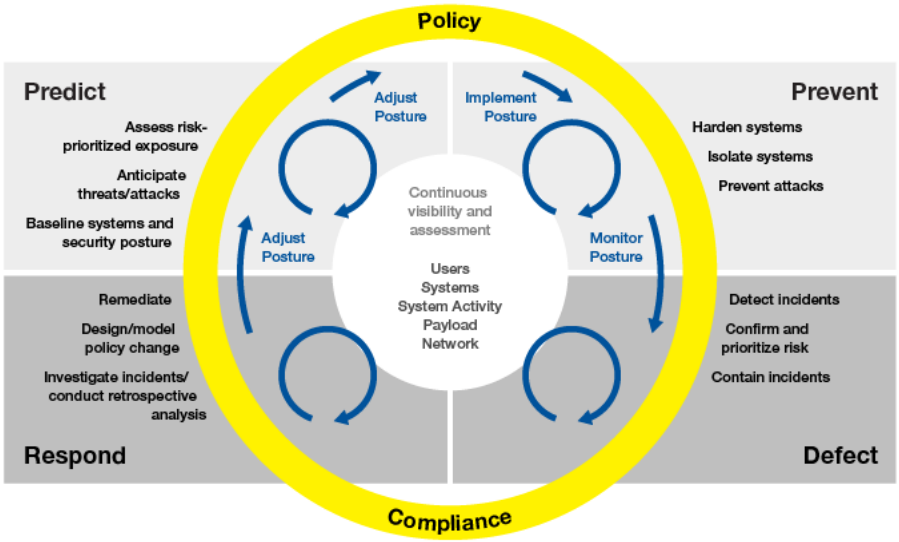

Image: Gartner, 2017

In 2022, Trellix (formerly, FireEye), came up with an Adaptive Defense Model (ADM) with the claim that it will be virtually impossible to keep up with the increasing number of incidents happening daily if we do not improve our defense strategies. In the whitepaper, *Trellix Adaptive Defense Model*, Trellix suggests that although Martin's Cyber Kill Chain and MITRE ATT&CK are effective, they place the attention on the attacker, whereas Trellix ADM attempts to do the opposite. Trellix ADM shifts the focus from the attacker to the defender and seeks to leave behind the "static and linear mindsets" that other models seem to have (Trellix, 2022). Trellix ADM prides itself in its dynamicity as it seeks to corner the attacker through three series of OODA loops. An OODA loop stands for Observe, Orient, Decide and Act and is also a derivative from military tactics, it was developed by Colonel John Boyd in the 1960s and it has become a pillar in cyberwarfare (Luft, 2020). Trellix model is fairly similar to Gartner's, but it divides itself into before, during and after an attack stages (Trellix, 2022).

Trellix ADM model:

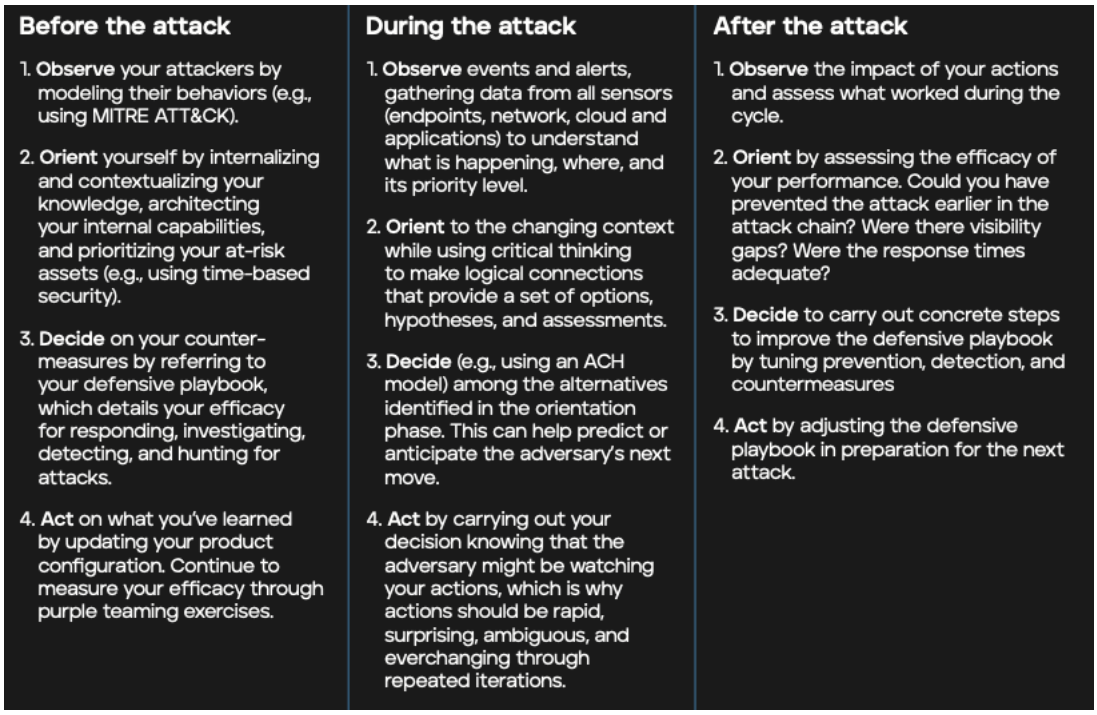

Image: Trellix, 2022

2.3.4 Deception technology

The magnitude and complexity of cyberattacks continues to grow and that requires a higher level of sophistication and complexity in defense mechanisms. The art of deception is a potent tool to master on the way to keep hackers away, or at least divert them, from your premises. You might be familiar with honeypots, the baseline for deception methodologies. A honeypot is a standalone asset, for instance a database, and its objective is to fool the attacker into walking a path that leads to triggering the defense team. Once the defense team gets notified the honeypot becomes inactive and thus is not very useful (Fortinet, 2023).

Deception technology is a strategy that aims to redirect the attacker onto a false and attracting environment that seems to possess a company's most protected asset with the goal of protecting the real assets (Fortinet, 2023). The decoy environment, contrary to standalone honeypots, is a robust platform that intends to look like a legitimate environment. With valid "servers, applications, and data", decoy environments try to lure the attacker into thinking they have successfully penetrated the company's security perimeter (Fortinet, 2023). The real

assets remain intact and security controls triggers the response team to take defensive action against the intruder. Any time the deception operation prolongs, and the intruder engages with decoy system and attempts to move laterally, escalate privileges or exfiltrate data, the victim company gets alerted and can take corrective action (Fortinet, 2023). The purpose of deception technology is to decrease the potential harm caused by intruders, protect the real company assets, and lastly yet no less important, research (Fortinet, 2023). A great deal of what we know today about cybercriminals and their TTPs was acquired through deceptive tools. Imagine being able to track, log and record every movement of an attacker in a controlled environment without them knowing they are being monitored. This kind of insight is invaluable not only to the victim, but to the cybersecurity community as a whole (Fortinet, 2023). The intelligence derived from these logs can shed light on things like the behavior of an attacker, which assets appeals them the most, the methods they employ for breaking into a system, how they engage with the decoy, which attack vectors they use during a breach, and more (Fortinet, 2023). The information gathered not only discloses the attacker's posture and intent but also helps security teams to enhance the defense strategy from a conscious place (Fortinet, 2023). In addition, this intel encourages the design of better security capabilities able to pick on more complex attack vectors that older mechanisms cannot (McKeon, 2022).

Nevertheless, deploying a deception technology is no easy task. It requires a lot of resources which have to be meticulously crafted, like the correct scale, complexity, and sophistication for an attacker to buy into the idea that they are inside a legitimate asset and not a decoy asset (Fortinet, 2023). The challenge with decoy environments is that if not rendered with sufficient fake data and equipped properly in terms of infrastructure it may not be able to handle the attacker's traffic and thus expose itself to the attacker who in turn can rapidly leave the premise and come back stronger and more hostile (Fortinet, 2023). With the presence of powerful tools like machine learning (ML) and Artificial Intelligence (AI),

deception tools become handy for a variety of reasons: a) it can help reduce burnout within the incident response (IR) teams who deal with large amount of incidents and false positives on a daily basis, b) it can speed up the detection time when an attacker is in the system, and c) shorten the "dwell time" of an attacker in the system (Fortinet, 2023).

2.3.5 Port and address hopping

In military communications it is common practice to shift frequency channels to divert enemies and keep them "in the dark" (Shi, et al., 2007). Influenced by this tactic, port and address hopping is another descendant from military strategies (Shi, et al., 2007). Port and address hopping is part of the Moving Target Defense (MTD) strategy and works by altering port and address information in a semi-arbitrarily manner "during data transmission" to obfuscate entry points into a system (Luo, et al. 2015; Shi, et al., 2007). To elaborate on this technique two research analytical studies will be discussed, *Port and Address Hopping for Active Cyber-Defense* by Shi, et al. 2007 and *Analysis of Port Hopping for Proactive Cyber Defense* by Luo, et al. 2015. To examine the effectiveness of port and address hopping, Shi, et al. and Luo, et al. tested it against simulations of DoS attack, eavesdropping attack, and reconnaissance attack (Luo, et al. 2015; Shi, et al., 2007).

In the first paper, Shi, et al., discusses the reliability of the "TCP/IP protocol suite" versus its security qualities. TCP/IP connectivity allows pertaining parties to connect with little to no interruption ensuring integrity. However, the fixated port mechanism exposes the connection to "port scanning and eavesdropping" because by default "once a TCP connection is established" the port numbers cannot be changed hence it fails to ensure confidentiality and availability in a case of a DoS attack or eavesdropping attack (Shi, et al., 2007). Shi, et al. carry out two experiments, a) the availability of information during a DoS attack and b) the confidentiality of information during an eavesdropping attack. The procedure was as follows:

a. Two variables, 'no hopping' and 'port & address hoping', are tested under the conditions of normal traffic and abnormal traffic (namely, a DoS attack) to test its response time. The two variables remain "approximately equal" with normal traffic. Yet, when abnormal traffic reaches "up to 10.5Mbps" the response time of 'no hopping' grows exponentially leading to a crash at 13Mbps. The response time of 'port & address hopping' remains stable up to ~27.5Mbps and peaks and crashes at 32Mbps. The findings are illustrated in the following image:

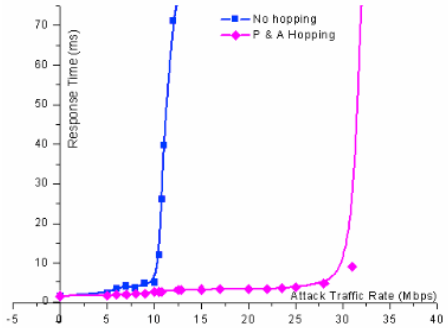

Fig. 2. Fitting curves of DoS experimental data

Image: Shi, et al., 2007

Table 2. DoS attack experimental data

ATR (Mbps)	Average Response Time (ms) No hopping	P&A hopping
0	1.4258	1.4675
5	2.2436	1.5884
10	4.8988	2.5003
10.5	12.1402	2.6182
12	71.2185	2.9593
13	-	3.1387
20	-	3.2694
25	-	3.6639
31	-	9.0805
32	-	-

b. The port and address hopping server possess 24 IP address used for hopping. A "professional sniffing tool" is used to mimic an eavesdrop attack. A brief message in plaintext is transmitted between the server and the client. Four variables are tested but we will focus on three, 1) no hopping, 2) only port hopping, and 3) port & address hopping. No traffic dispersion occurs in 1 and 2 and the sniffing tool (the attacker) manages to obtain the plaintext message in its entirety. In 3 the traffic is dispersed and thus harder for the sniffing tool to capture the message. The findings showing clear success rates with the port and address server as illustrated below:

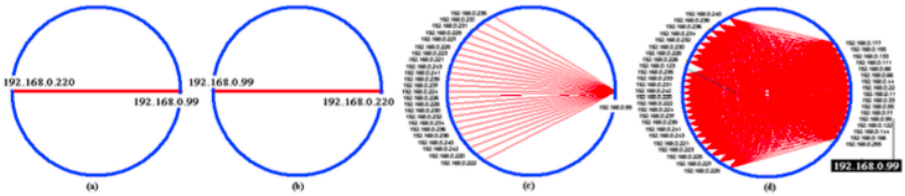

Fig. 3. Traffic dispersion results by sniffing attack, (a) no hopping (b) port hopping (c) port and address hopping (d) port and address hopping with virtual clients

Image: Shi, et al., 2007

In the second paper, Luo, et al., considered the "attack success rates" (ASR) of a reconnaissance attack against four factors, a) the port pool size, b) the number of probes performed, c) the number of vulnerable services active in the server host, and d) the hopping frequency.

a. Port pool size – the analysis performed showed correlation between attack success rates (ASR) and the quantity of available ports, namely, the port pool size. When the quantity of available ports grew the attack success rates reduced, and conversely, when the quantity of available ports shrank the attack success rates increased. In figure 1, v denotes the number of vulnerable services:

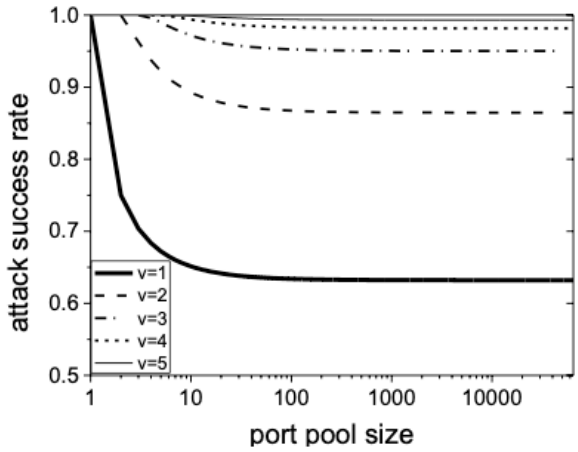

Figure 1. ASR vs the Port Pool Size

Image: Luo, et al., 2015

b. Number of probes – to explain the analysis performed consider the terms 'static ports', the unchangeable assignation of ports by the server when a service takes place (no hopping), and 'perfect port hopping', the ideal event of port hopping happening every time there is a probe attempt by an attacker. The findings in the analysis indicate that the attack success rates (ASR), and the number of probes perform, both grow "linearly" when static ports were used. And as the number of probes performed increases and v (number of vulnerable services) is fixated, the attack success rates grow at a slower pace. The test also showed that port hopping succeeds best when

there is less v's (number vulnerable services) and that attack success rates decrease when perfect hopping is employed instead of static ports.

c. Number of vulnerable services – as possible to assume, the findings so far have shown direct correlation between v's, the number of vulnerable services, and attack success rates. If static ports are used the defense mechanism will fail as all v's will eventually be discovered by the attacker. If perfect port hopping is used and the pool size maxes at 64512 the probability of a successful attack reduces.

   Thus, the effectiveness of port hopping will always depend on the number of vulnerable services. See figure 3:

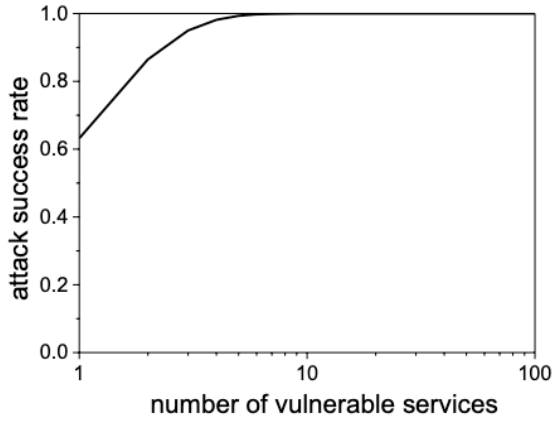

Figure 3. ASR vs the Number of Vulnerable Services

Image: Luo, et al., 2015

d. Hopping frequency – in this final analysis illustrated by figure 4, the interrelation between attack success rates and hopping frequency is clearly noted. The figure shows that when hopping frequency is high, attack success rate decreases accordingly. And as said previously, the number of vulnerable services should aim to remain small and fixed. Additionally, the analysis shows that since the "overhead of port hopping" increases "exponentially" as the hopping frequency grows, it is important to account that when employing a port hopping mechanism.

Figure 4:

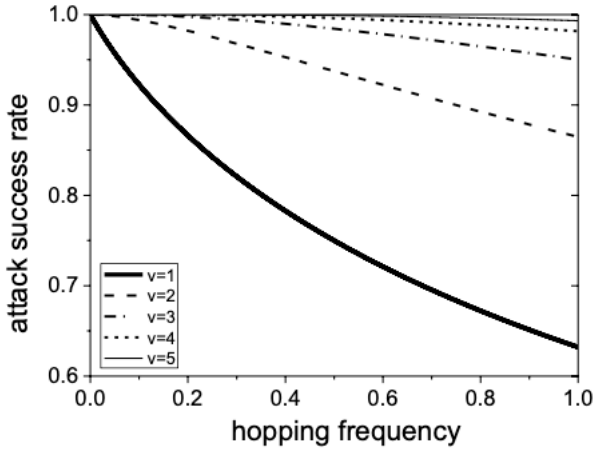

Figure 4. The ASR vs the Normalized Hopping Frequency

Image: Luo, et al., 2015

3 Cybersecurity in the Health Sector

As in many sectors, cybersecurity's vitality in the healthcare domain is unquestionable. The US Cybersecurity & Infrastructure Security Agency (CISA) classifies the healthcare sector as a "critical infrastructure industry" along with financial services, energy, water, communication, technology, education, and transportation (IBM, 2022). Cybersecurity in the health sector exists to preserve the confidentiality, integrity, and availability (CIA triad) of all information assets (HIMSS, 2023). The stakeholders in the health sector are patients, medical staff, c-level executives, vendors, and industry suppliers (HIMSS, 2023). The importance of safeguarding healthcare information is vast. Cyberattacks on healthcare systems and infrastructure not only can disrupt routine care activity but it can also impact "critical life-saving functions" that depend on the connectivity of networks and the access of medical workforce to those (CISA, 2023). These unfortunate incidents can easily wreak havoc on the healthcare providers and the patients. The risks range from leakage of sensitive patient data to considerable financial loss in the attempt to reclaim control over a compromised system or in compensation fees and irreversible reputation damage (CISA, 2023).

A common belief is that cybersecurity in the healthcare domain is an issue concerning solely the IT team and not enterprise as a whole (CISA, 2023). Hundreds of cyberattacks on healthcare providers forcing them to kneel and yield to the attacker's requests have proved this misconception wrong. When the IT team gets compromised, all company sectors are impacted. The Cybersecurity & Infrastructure Security Agency (CISA) ascertains, "Cyber Safety is Patient Safety!". Arctic Wolf reports that in 2022 the average cost loss caused by attacks on healthcare systems in the US was $10.1 million. An astronomical number that grew by 41.6% since 2020 (Arctic Wolf, 2023). The healthcare sector is the most impacted sector and continues to lead for the 12th year in a row with costs mounting $10.10 million, an all-time high record (IBM, 2022).

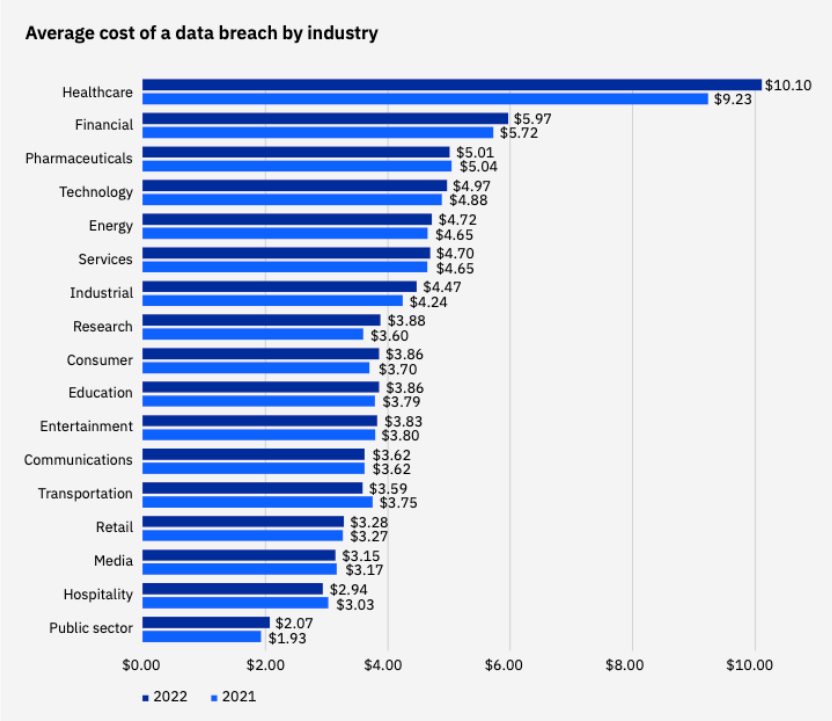

Figure 4: Measured in USD millions

Image: IBM 2022 report

Some of the applications that require constant protection and maintenance are electronic health record (EHR) systems, electronic prescribing systems, practice management support systems, clinical decision support systems, radiology and imaging information systems, research database systems, billing systems, cloud-based systems, in addition to physical infrastructure systems such as smart elevators, heating, ventilation and air-conditioning

(HVAC) systems, infusion pumps, remote patient monitoring systems, and the list goes on (HIMSS, 2023).

The healthcare system works with large amounts of protected health information (PHI) and personal identifiable information (PII) but often lacks the necessary resources to secure those while providing 24/7 "uninterrupted access" to healthcare systems. All of these turn the healthcare sector into an attracting target for threat actors (Arctic Wolf, 2023). Following is a list of the most 12 recent breaches in the US in chronological order (Arctic Wolf, 2023):

1. Shields Health Care group – the Massachusetts-based imaging provider serving nearly 50 other healthcare providers reported being hit in March 2022 by a data breach affecting more than 2 million users. PHI such as full names, physical and email addresses, Social Security Numbers (SSNs), insurance information, medical records were exfiltrated from Shields' systems leading to a class action lawsuit that is still pending settlement.
2. Advocate Aurora Health – the Midwest giant provider that employs 26 hospitals in Wisconsin and Illinois reported being impacted in July 2022 by an "improper use" of Meta Pixel, a website tracking device, leading to a breach exposing the data of 3 million users. This unfortunate incident was also followed by a class action suit.
3. Trinity Health – the Michigan-based service provider was compromised in a ransomware attack in 2020 on their cloud-based customer relationship management (CRM) software affecting 3.32 million users. Blackbaud, the CRM software, managed to thwart the encrypting attempt of the attackers, however failed to impede the exfiltration of the data.
4. American Medical Collection Agency (AMCA) – AMCA is a billing collections provider from New York, it provides services to Quest Diagnostics and LabCorp,

among others. In 2018 AMCA was breached by attackers who gained access to sensitive information of over 21 million patients. The attackers put up for sale the stolen info in the dark web critically endangering the patients. In 2019 AMCA filed for bankruptcy after their four main clients decided to cut ties with the company. A "multistate investigation" by 41 attorneys general determined in 2020 that AMCA is responsible for $21 million "in injunctive damages".

5. Banner Health – the Arizona service provider was victim to a malware attack in 2016. The attackers gained access to the company's network through their "payment processing system" of the food and beverage interfaces. It took almost a month until the breach was detected. The private data of 3.6 million users was taken and the total breach cost was $6 million.
6. Medical Informatics Engineering (MIE) – the Indiana "electronic health records software firm" was hit in 2015 with a mixed brute-force, SQL injection and malware attack on their "WebChart web app". Attackers successfully brute-forced their way into the system by guessing weak credentials, then they launched an SQL injection attack in the company's database, few weeks later they launched a malware attack to obtain sensitive data files. 3.9 million users were impacted and the total cost was $1 million.
7. Anthem, Inc. – Anthem, formerly WellPoint, is an Indiana-based health insurance provider that suffered the "largest healthcare industry cyber attack in history" in 2015. Through phishing email and malware attack, hackers gained access and stole electronic PHI records of 79 million users. In the settlement, Anthem was required to pay $115 million and forced to "nearly triple its cybersecurity budget".
8. Community Health Systems – in 2014, the Tennessee-based healthcare provider that "operated 206 hospitals in 29 states" was victim to a breach carried out by an

advanced persistent threat actor (APT) from China, according to the Securities and Exchange Commission (SEC). The personal information of 4.5 million people was exposed, and the costs reached $3.1 million.

9. University of California, Los Angeles Health – in 2014 the UCLA Health suspected that intruders had gained access to their network but shortly after stated it was a false alarm. In 2015 UCLA Health retracted their previous statement and announced that its systems were indeed compromised back in 2014 in a malware attack affecting the information of 4.5 million individuals. The class action lawsuit did not take long to arrive, the settlement was for $7.5 million.
10. Premera Blue Cross – the healthcare provider in Washington state was victim in 2014 to a phishing attack involving one of its employees pressing on a malicious link granting the attacker full access to their systems. It took Premera eight months before they were able to discover the breach. The cybersecurity firm hired to help with the case concluded that the attackers had ties to the "Chinese government". The breach affected 11 million people and the class action lawsuit settlement was for $74 million.
11. Excellus Health Plan, Inc. – The New York service provider announced in 2015 that they have been victim to a breach dating back to 2013 in which the information of 10 million patients was compromised in a malware attack. The attackers "gain access to administrative controls" which led to the nullification of encryption mechanisms in place. Excellus was forced to employ a cybersecurity firm to carry out a forensic investigation, the total costs mounted $17.3 million.
12. Advocate Medical Group (AMG) – the service provider from Illinois was victim in 2013 to a less common way of attack, physical theft. The attackers stole desktop and laptop computers from AMG's premises and staff vehicles. The data

of more than 4 million users was stolen and the costs associated with the attack were $5.55 million.

This list clearly highlights the need for proper security tools and resources in the healthcare domain. The sensitive information typically targeted is names, credit card information, physical and email addresses, medical records, birth dates, ID numbers, Social Security Numbers (SSNs), employee information, insurance membership information, telephone numbers, demographic information, dates of services, dates of claims, and more. Most of this info is protected under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA is a federal law meant to enforce the national standards for the protection of "patient health information from being disclosed without the patient's consent or knowledge" (CDC, 2022). The HIPAA is the biggest umbrella covering protected health information (PHI), but other regulatory laws like the 42 CFR Part 2, Section 5 of Federal Trade Commission (FTC) Act and the Personal Information Protection and Electronic Documents Act (PIPEDA) operates in similar ways (HIMSS, 2023).

From IBM's 2022 report, its deducible that the cost of breaches across industries eventually impacts the end-user, too, not only because their sensitive information gets compromised exposing them to risks like identity theft, but because 60% of the organizations examined in the report confirmed having "increased the cost of their services and products" to compensate for the costs associated with the attack. (IBM, 2022). The report also shows that companies that employ AI capabilities have a better chance in thwarting an attack. The cost of companies using AI was $3.15 million as opposed to $6.20 million for their counterparts who do not use IA in their defense mechanism. Companies that incorporate "AI and automation" services also experience a shorter time in detection and containment of an attack, 249 days for companies using AI and 323 for companies not using AI (IBM, 2022). In

spite of ransomware attacks mounting 12% of attacks in critical infrastructures, “human error and IT failure” continues to lead with 22% and 25%, correspondingly.

According to the Healthcare Information and Management Society (HIMSS), industry best practices divide into two, risk assessment and security controls. Risk assessment is the “cornerstone” of any action, that is because in order to ensure proportionate and accurate response a risk must be thoroughly examined first. Factors like “probability of occurrence, impact on the organization” and its stakeholders, and risk priority must be accounted for when crafting an incident response plan.

Security controls vary and healthcare providers should aim for a multifaceted approach otherwise defined as Defense In-Depth by the National Institute of Standards and Technology (NIST) (McKeon, 2022). The reason to this is that a robust multilayered plan can ensure that if one control fails the others can replace it and maintain a protected perimeter (HIMSS, 2023). Some of the most common security controls are policies, procedures, standards, anti-viruses, backup and restoration systems, data loss prevention systems, email and web gateway, encryption at-rest and in-transit mechanisms, encryption for archived data, firewalls, incident response (IR) plans, disaster recovery (DR) plans, business continuity (BC) plans, intrusion detection (IDS) and intrusion prevention (IPS) systems, security information and event management (SIEM) systems, mobile device management systems, secure disposal systems, security awareness and education programs, vulnerability management programs, patch management systems, anti-theft systems, secure authentication mechanisms, network segmentation, penetration testing, threat intelligence sharing plans, and vulnerability scanning systems (HIMSS, 2023). HIMSS rightfully points to legacy systems as another challenge for security teams. A large amount of healthcare providers still works and relies on legacy systems, archaic systems that were discontinued and thus do not have proper maintenance and vulnerability patching routines. This often means that health systems have

exploitable vulnerability gaps that sooner or later will be discovered by attackers (HIMSS, 2023). The decision to shift from legacy systems to more modern systems is not a decision to take lightly and although it promises better security the costs involved in such procedure are sometimes too high for a company to bear. But is it a risk worth taking? Is the overall cost of a potential breach smaller than the cost required for transitioning from legacy systems to modern ones? The answer to that dilemma is up to the judgement of the officer reigning the security team.

4 Active Cyber Defense in the Healthcare Sector

The section preceding this one outlines the many reasons behind the need to develop stronger, more sophisticated, security capabilities that will shrink the window of possibilities for attackers targeting health organizations. This section will discuss the ways in which the healthcare sector can benefit from incorporating Active Cyber Defense (ACD) techniques in the defense strategic plan.

Predictive analytics creates models based on current and past data with the goal of predicting possible security incidents by “identifying patterns”, it also determines whether these incidents will be successful or not (Giordani, 2022; Sisense, 2022). This capability can improve accuracy in incident response in the health sector and it can also boost system resilience in the event of an attack so that care delivery is not interrupted. One way to achieve resilience is understanding the vulnerabilities holes in a system, and predictive analytics does that with ease and agility leading to more accurate results. Predictive analytics is a powerful tool because it can answer the “when”, “where” and “where next” questions when it comes to potential attacks (Sisense, 2022). It helps predict attacks before they occur by analyzing “historical data, user behavior, and external factors”, it can process enormous amounts of data in short periods of time while routine activity are in play, and it can also automate a lot of processes freeing security teams to deal with other things while reducing overall burnout.

Lastly, as cyber incidents continue to peak, a growing industry of cyber insurance has emerged with the function of "helping businesses make up for any expenses" associated with breaches (Flynn, 2022). Predictive analytics plays an important role by helping companies determine the degree of coverage they might need. As shown earlier in this paper, the healthcare sector is the most targeted hence this property can be highly useful when choosing an appropriate cyber insurance coverage.

Behavioral analysis has been the focal point of cybersecurity researchers. Since the arrival of AI and ML, behavioral analysis has become highly insightful in the battle against cybercriminals. Every single step and procedure, either done by the computer itself or by a human hand, is recorded in log files. Behavioral analysis in cybersecurity consists of analyzing those log files to determine normal behavior versus abnormal behavior. The analysis of user behavior, as well as the system's behavior, can reveal a great deal of actionable information to security teams in the healthcare sector. The conclusions drawn can indicate gaps in the optimal user behavior with health systems versus the actual behavior of the user. Knowing these gaps can help IT teams gauge better how aware and educated is the medical workforce regarding cyber hygiene and whether more training and awareness programs are needed. And in the case of system behavioral analysis, forensics teams rely almost entirely on computer log files, not only for understanding how and where the security control failed and what was the exploited vulnerability, but also in helping forensic teams to recover lost data and retract the system to the state prior to the attack (Skopik, et al., 2022). Employing these capabilities can be very cost-effective with cloud-based services that allow scalability and storage at request (VMware, 2023). This is particularly relevant for the health sector where strict budgetary limitations exist.

Adaptive Security can be a game-changer in the healthcare cybersecurity landscape. Healthcare functions rely heavily on a myriad of information systems, whether its Internet of

Things (IoT) devices like infusion pumps, remote patient monitoring devices, or life-supporting systems and information management systems used to record patient data. Adaptability is key due to the fragility of information assets in the healthcare domain. Suggested earlier was the need to transition from legacy systems to modern ones, the overarching concept is to consider dynamic and rapid solutions over rigid and time-consuming ones. With this premise in mind, adaptive security has the capability of revolutionizing the cybersecurity healthcare landscape because it proposes framework that acts quickly and efficiently not only to anticipate, react, and contain an attack but also to minimize the attack surface and shorten the recovery time (Brook, 2018).

Deception technology is already widely used in the healthcare domain. In part because it is a very affective way of shifting the power dynamics between the attack and the defender. With deception technology, the defender manages to reverse roles from being the prey to seemingly being the predator. Having robust fake environments to deceive attackers can help health cybersecurity teams protect the real assets. Attackers are tricked to commit "mistakes that disclose their presence" in the system and in the meantime, the attacker is convinced they are navigating an authentic environment (Crandall, 2019). Deception technology tools also enables its users to monitor and observe the attacker in real-time, this can be dramatically favorable for cybersecurity professionals in the healthcare domain.

Port and address hopping has as its goal to complicate the conditions for a successful attack, and although successful attacks have diminished the healthcare sector persists to be the most targeted sector so it can surely benefit from this technique. It originates from military methodologies and focuses on prevention by continuously changing port and addresses during the transmission of data to dazzle the attacker from achieving its goal. Port and address hopping is part of the Moving Target Defense (MTD) strategy that also stems

from military. MTD's premise is that attacking a moving target is intuitively harder than targeting "a stationary one" (Gerard, 2023).

There are many ways that can help healthcare providers combat cybercrime. The various resources explored in this research paper lucidly shows that an attack is not a matter of "if" but "when". For better or worse, cyber events throughout history have pushed us to prioritize cybersecurity as a critical component that requires the adequate attention and funding, but the race for proper solutions against cyberattackers continues. Attacks on critical infrastructure industries like the health sector have not lessened, therefore security professionals cannot be idle in light of the ever-growing attack landscape (IBM, 2022; McKeon, 2022). We, as a cybersecurity community, must continue pushing the limits of creation to ensure we provide the best cybersafety we can.

5 Conclusion

This research paper begins with a rather broad perspective, discussing the birth of the internet as an ARPA project, and as it progresses the perspective narrows gradually to address the cybersecurity challenges that the health sector faces, and culminates examining the usefulness of Active Cyber Defense (ACD) in the healthcare sector.

The first chapter is an introduction. Section 1.1 introduces the Cyber Space, starting from its creation in the ARPA labs, through its evolution as a time-sharing system that later enable its users to interact with it in real-time while carrying out other processes, and until it morphed into the massive network connecting millions of individuals across continents and serving as a well of infinite knowledge for humans to use. Section 1.2 introduces Cybersecurity. It uses the material presented in the previous section as a foundation to expand on the arrival of cybersecurity. It studies the first computer vulnerabilities. Section 1.3 and 1.4 follows with an extensive historical discussion about cyber threats over time.

The second chapter explores Active Cyber Defense (ACD). Section 2.1 delves into a rigorous discussion presenting ACD through its origins in the military strategic warfare. It then challenges the misconception that ACD is reckless and generally, bad practice, by examining Dorothy E. Denning's essay, *Framework and Principles for Active Cyber Defense.* In the essay, Denning reflects ACD's virtues through equating it to Active Air and Missile Defense (AMD). Denning also proposes holding ACD under the same scrutiny as AMD with legal and ethical principles like authority, third-party immunity, necessity, proportionality human involvement, and civil liberties. Section 2.2 introduces ACD's evolution over time studying a military paper by Major Eric J. Holdaway in which Holdaway stresses the importance of using passive and active measures in synergy for better defensive results. Section 2.3 presents five ACD techniques in-depth: 2.3.1 predictive analysis, 2.3.2 behavioral analysis, 2.3.3 adaptive security, 2.3.4 deception technology and 2.3.5 port and address hopping.

The third chapter talks about cybersecurity in the health sector, it introduces it as a critical infrastructure industry. It expands on the importance of protecting health information systems and its respective stakeholders. It also demonstrates the increasing costs associated with breaches as illustrated by various resources. IBM reports that the healthcare sector has been the most targeted and impact sector for twelve consecutive years reflecting the ever-growing need for proper protection. The chapter provides a list of recent data breaches impacting healthcare providers in the US.

The fourth chapter explains, through the findings presented throughout the paper, how the healthcare industry can benefit from incorporating ACD techniques. ACD is a cybersecurity methodology that in contrast to the passive and traditional defense methods, seeks to be proactive. One layer of security will most certainly not suffice to protect a system; thus, multilayer approach is preferable for successfully thwarting an attack and anticipating

others. The combination of multiple security controls in conjunction with ACD techniques can be highly beneficial. And as Josh Johnson rightfully said, when these systems work "cohesively" instead than separately it can be the determining "factor between a breach and a successfully mitigated attack" (Johnson, 2021).

Cybersecurity has come a long way as illustrated by the myriad of events following the birth of the internet. As shown in the IBM 2022 report, humans still constitute the weakest link in a series of vulnerabilities, therefore education and awareness trainings must be an inseparable part of a defense strategic plan. The IBM report also suggests that "AI and automation offer the biggest savings", hence its worthwhile to consider the application of AI capabilities in healthcare solutions. The number of challenges standing before security teams in the health sector is great. The findings presented in this paper are meant to support the thesis that the healthcare sector can benefit immensely from incorporating active ACD in the security strategic plan to better protect health information.

Work Cited

"Core War: Creeper and Reaper." *Creeper & Reaper*, https://corewar.co.uk/creeper.htm.

"Fighting Cyber Crime with Data Analytics." *Electrical and Computer Engineering, University of Michigan*, 23 May 2016, https://ece.engin.umich.edu/stories/fighting-cyber-crime-with-data-analytics.

"First Virus Hatched as a Practical Joke." *The Sydney Morning Herald*, The Sydney Morning Herald, 3 Sept. 2007, https://www.smh.com.au/technology/first-virus-hatched-as-a-practical-joke-20070903-gdr0fn.html?page=fullpage#contentSwap2.

"What Is Behavioral Analysis: VMware Glossary." *VMware*, 9 Apr. 2023, https://www.vmware.com/topics/glossary/content/behavioral-analysis.html.

"What Is Deception Technology? Defined & Explained." *Fortinet*, https://www.fortinet.com/resources/cyberglossary/what-is-deception-technology.

3 Ways Predictive Analytics Can Boost Your Cybersecurity. Sisense, 2022, https://www.sisense.com/blog/3-ways-predictive-analytics-can-boost-cybersecurity/.

Biggest Healthcare Industry Cyberattacks. Arctic Wolf, 4 Jan. 2023, https://arcticwolf.com/resources/blog/top-healthcare-industry-cyberattacks/#:~:text=Trinity%20Health&text=The%20attack%20on%20one%20of,more%20than%2010%20million%20records.

Brook, Chris. "What Is Adaptive Security? A Definition of Adaptive Security, Benefits, Best Practices, and More." *Digital Guardian*, 5 Dec. 2018, https://www.digitalguardian.com/blog/what-adaptive-security-definition-adaptive-security-benefits-best-practices-and-more#:~:text=Sun%20Microsystems%20(acquired%20by%20Oracle,surface%2C%20velocity%20and%20recovery%20time.

Chen, W.S. William. "Statistical Methods in Computer Security", *Marcel Dekker,* 2005

Chiappa, J. Noel. *ARPANET Technical Information: Geographic Maps*, 7 Nov. 2014, http://mercury.lcs.mit.edu/~jnc/tech/arpageo.html.

Cost of a Data Breach 2022. IBM, 2022, https://www.ibm.com/reports/data-breach.

Crandall, Carolyn. *How Deception Technology Enhances Medical Device Security*. HealthITOutcomes, 6 Sept. 2019, https://www.healthitoutcomes.com/doc/how-deception-technology-enhances-medical-device-security-0001.

Cybersecurity in Healthcare. Healthcare Information and Management Systems Society, 16 Dec. 2021, https://www.himss.org/resources/cybersecurity-healthcare#:~:text=Cybersecurity%20in%20healthcare%20involves%20the,as%20the%20"CIA%20triad.".

Denning, Dorothy E. “Framework and Principles for Active Cyber Defense.” *Naval Postgraduate School*, Dec. 2013, https://faculty.nps.edu/dedennin/publications/Framework%20and%20Principles%20for%20Active%20Cyber%20Defense%20-%2011Dec2013.pdf.

Denning, Dorothy Elizabeth Robling, and Lin Herbert. *Rights and Responsibilities of Participants in Networked Communities*, National Academy, Washington, D.C., 1994.

Department of Defense Dictionary of Military and Associated Terms: Incorporating the NATO and IADB Dictionaries. Joint Chiefs of Staff, 1984.

Dewar, Robert S. “The ‘Triptych of Cyber Security’: A Classification of Active Cyber Defence.” *NATO CCD COE*, 2014, https://ccdcoe.org/uploads/2018/10/d1r1s9_dewar.pdf.

Flynn, Shannon. “How Predictive Analytics Can Combat Cybercrime.” *MUO*, 29 Jan. 2022, https://www.makeuseof.com/predictive-analytics-combat-cybercrime/.

Gerard, Michael. *Automated Moving Target Defense Is the Future of Cyber-Gartner*. Morphisec, 17 Mar. 2023, https://blog.morphisec.com/automated-moving-target-defense-gartner.

Giordani, John. *How Predictive Analytics Could Change Cybersecurity*. LinkedIn, 30 Apr. 2022, https://www.linkedin.com/pulse/how-predictive-analytics-could-change-cybersecurity-john-giordani/?trk=articles_directory.

Hauben, Michael, and Ronda Hauben. *Netizens: On the History and Impact of Usenet and Internet*. IEEE Computer Society Press, 1997.

Health Insurance Portability and Accountability Act of 1996 (HIPAA). Centers for Disease Control and Prevention, 27 June 2022, https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient%27s%20consent%20or%20knowledge.

Healthcare and Public Health Sector. Cybersecurity and Infrastructure Security Agency (CISA), https://www.cisa.gov/stopransomware/healthcare-and-public-health-sector.

J.C.R. Licklider and Robert W. Taylor, “The Computer as a Communication Device,” Science and Technology, April 1968

Lee, Timothy B. “40 Maps That Explain the Internet.” *Vox.com*, 2 June 2014, https://www.vox.com/a/internet-maps.

Luft, Alastair. “The OODA Loop and the Half-Beat.” *The Strategy Bridge*, The Strategy Bridge, 17 Mar. 2020, https://thestrategybridge.org/the-bridge/2020/3/17/the-ooda-loop-and-the-half-beat.

Luo, Yue-Bin, et al. *Analysis of Port Hopping for Proactive Cyber Defense*. NADIA - Advancement Trough Research, 2015, http://article.nadiapub.com/IJSIA/vol9_no2/12.pdf.

Markoff, John. “Technology & Media: Talking the Future with: Robert W. Taylor; an Internet Pioneer Ponders the next Revolution.” *The New York Times*, The New York Times, 20 Dec. 1999, https://www.nytimes.com/1999/12/20/technology/technology-media-talking-future-with-robert-w-taylor-internet-pioneer-ponders.html.

McKeon, Jill. *Adopting Defense in Depth Strategies to Combat Healthcare Cyberattacks*. HealthITSecurity, 11 Jan. 2022, https://healthitsecurity.com/features/adopting-defense-in-depth-strategies-to-combat-healthcare-cyberattacks.

Roebuck, Mary Francis. “Major Warning Signs of a Data Breach in Progress.” *Roebuck Technologies*, 14 Apr. 2021, https://www.roebucktech.com/it-blog/major-warning-signs-of-a-data-breach-in-progress/.

Rosenzweig, Paul. “International Law and Private Actor Active Cyber Defensive Measures.” *Social Science Research Network (SSRN)*, 27 May 2013, https://deliverypdf.ssrn.com/delivery.php?ID=764097064115114092100031111086073029057062017031026026005090102067007086028083022031101007022041026027017100024067081023005069041034005023078067009106102085099089030085076126079029083071007121011089068093092118066071004105095073087086105080116110124&EXT=pdf&INDEX=TRUE.

Russell, Deborah, and G. T. Gangemi. *Computer Security Basics*. O'Reilly & Associates, 1991.

Sawyer, Ralph D. *The Seven Military Classics of Ancient China: Including the Art of War*. Westview Press, Inc., 1993.

Shackleford, Dave. SANS Institute, 2016, *Using Analytics to Predict Future Attacks and Breaches.*

Shi, Leyi, et al. *Port and Address Hopping for Active Cyber-Defense*. 2007, https://link.springer.com/chapter/10.1007/978-3-540-71549-8_31.

Skopik, Florian, et al. *Detecting Unknown Cyber Security Attacks through System Behavior Analysis*. Springer International Publishing, 7 Apr. 2022, https://link.springer.com/chapter/10.1007/978-3-031-04036-8_5.

Trellix, 2022, *Trellix Adaptive Defense Model*.

van der Meulen, Rob. “Build Adaptive Security Architecture into Your Organization.” *Gartner*, 30 June 2017, https://www.gartner.com/smarterwithgartner/build-adaptive-security-architecture-into-your-organization.

Von Nuemann, John. “Self-Reproducing Automata”, *University of Illinois Press*, 1966

Ware, Willis. “Security Controls for Computer Systems”, *Defense Science Board, Task Force on Computer Security*, 11 Feb. 1970