Position Paper: Evaluating Analogies and Applying Public Health Models for Cybersecurity

Josiah Dykstra
josiah.dykstra@trailofbits.com
Trail of Bits
New York, NY, USA

O. Sami Saydjari
Sami.Saydjari@dartmouth.edu
Dartmouth College
Hanover, NH, USA

Jamie Met
jlmet@nsa.gov
National Security Agency
Ft. George G. Meade, MD, USA

Douglas Hough
douglas.hough@jhu.edu
Johns Hopkins Bloomberg School of Public Health
Baltimore, MD, USA

ABSTRACT

This paper presents a new approach to integrating analogies and analytical methods from public health and other domains into cybersecurity by introducing a structured framework for evaluating and judiciously applying them. Based on principles of analogy theory, the framework categorizes aspects of analogies into a stoplight system—green, yellow, and red—allowing practitioners to assess their applicability and potential pitfalls. We then employ the Haddon Matrix, a specific analytical method from the public health domain, demonstrating its relevance and utility in analyzing cybersecurity threats such as credential theft via phishing. Finally, we extend the framework's application to other public health and safety models, illustrating how these analogies and analytical methods can be more broadly evaluated and potentially adopted in cybersecurity. Through these contributions, the paper offers a structured method for cross-disciplinary cybersecurity innovation, providing specific insights and a generalizable approach for future research and practice.

CCS CONCEPTS

• **Applied computing** → *Life and medical sciences*; Psychology; • **Security and privacy** → **Social aspects of security and privacy**; • **Social and professional topics** → **Computing education**.

KEYWORDS

cybersecurity, public health, analogies, Haddon Matrix

ACM Reference Format:
Josiah Dykstra, O. Sami Saydjari, Jamie Met, and Douglas Hough. 2024. Position Paper: Evaluating Analogies and Applying Public Health Models for Cybersecurity. In *Proceedings of the 2024 Workshop on Cybersecurity in Healthcare (HealthSec '24), October 14–18, 2024, Salt Lake City, UT, USA.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3689942.3694751

HealthSec '24, October 14–18, 2024, Salt Lake City, UT, USA

ACM ISBN 979-8-4007-1238-8/24/10
https://doi.org/10.1145/3689942.3694751

1 INTRODUCTION

Since its birth in the mid-20th century, other fields have aided and informed developments and advances in cybersecurity. Although some concepts and methods from those fields applied naturally, others were adapted. Analogical reasoning is fundamental to human thought, reasoning, and knowledge acquisition, allowing us to extend what we know to areas with which we are unfamiliar [1, 7]. Such extensions apply to both individuals' knowledge and to humanity's knowledge as a whole. At the same time, analogies are like models: they are all wrong in some way, though some are useful [2]. To disregard an analogy for being imperfect is to miss an opportunity to quickly gain vast knowledge about a new discipline and leapfrog to do the engineering and experimentation in areas where the analogies do not apply. Similarly, methods from analogous domains can be generalized and applied to cybersecurity, yielding new and insightful ways of analyzing problems and developing solutions. Sources of cybersecurity analogies have included biology, physics, military, sports, and information theory.

Public health, in particular, has relevant—and often underexplored—implications for cybersecurity. Used superficially, however, terms such as "virus" have become shorthand for imperfectly applied analogies. This position paper explores how public health analogies and methods can contribute substantially to cybersecurity if applied carefully and with an evaluative framework. More than 100 years ago, C.E.A. Winslow created what is still the classic definition of public health: "Public health is the science and the art of preventing disease, prolonging life, and promoting physical health and efficiency through organized community efforts… and the development of the social machinery which will ensure to every individual in the community a standard of living adequate for the maintenance of health" [19]. The shared goal of safety and the similarities between threats to public health and digital security suggest that each field may have lessons for the other about approaches to developing and assessing mitigations. However, critical analysis is needed to assess such lessons for suitability to avoid unintended consequences.

Conceptual models are used in public health to depict "the mechanisms by which a selected set of risk and protective factors may be associated with a health behavior or outcome of interest, as well as the conditions under which such associations are typically observed" [3]. As with public health, cybersecurity must continually study digital risk and protective factors. Various models have been

created specifically for use in cybersecurity, but we encourage the consideration and adoption of relevant models from public health.

In this paper, we first describe a framework in Section 2 for evaluating the utility of analogies based on their similarities and limitations. Section 3 describes how public health and public safety models have been applied to cybersecurity. We then shed light on a public health method used in injury prevention, known as the Haddon Matrix, in Section 4 and show how it can be adapted by analogy to plan for prevention and interventions in cybersecurity and drive more nuanced and detailed analogy knowledge assessment. We conclude in Section 5 by presenting other models known to public health and suggesting a future research agenda.

2 AN EVALUATIVE FRAMEWORK FOR ANALOGIES IN CYBERSECURITY

Cyberspace is a complex, nonlinear, multidimensional arena that has been proven difficult to fully understand. Analogies are an obvious tool for helping engineers and society as a whole understand the security of cyberspace.

2.1 A Stoplight Framework for Analogy Analysis

A fundamental problem in analogical reasoning is to discern which aspects of an analogy apply directly, allowing the knowledge to be transferred with minimal effort, which aspects might apply with some conceptual transformations, and in which aspects it simply does not apply. We introduce a simple stoplight framework (Figure 1) to guide the understanding of how to apply analogies for what they can teach us and to avoid mistakes in overextending analogies to the point of incorrectly assuming invalid knowledge [16]. The framework allows us to assess which aspects and sub-aspects of analogies are applicable, to what extent, and how conceptual mapping aids in better using the value brought by the analogy. This method encourages nuanced and careful analysis of analogies and a method to do such analysis.

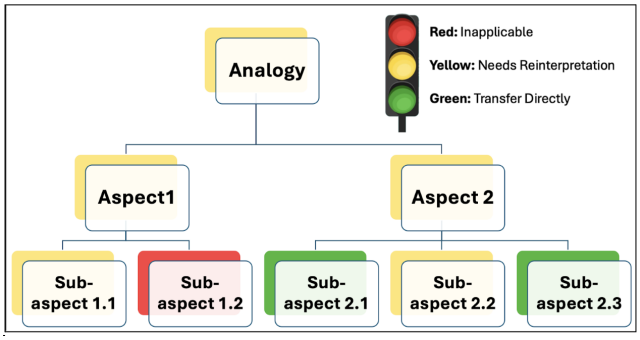

Figure 1: Stoplight framework for evaluating the utility and limits of analogy aspects.

To determine the color categorization of a new analogy, we present a step-by-step evaluation process:

(1) **Identify the Structural Similarity**: Analyze the key concepts of the source and target domains to see if there is a strong, moderate, or weak mapping in their relational structure.
(2) **Assess Relevance**: Determine if the mapped similarities are relevant to the context of the argument or concept being explained.
(3) **Evaluate Generalizability**: Consider if the properties and relationships from the source domain generalize to the target domain.

First, good analogies have a strong structural similarity between the source and target domain. This similarity involves identifying the key concepts in the base analogy and mapping one-to-one correspondence between the source and target concepts. The correspondence should be such that each element in the source domain that determines a particular property has a clear, possibly transformed counterpart in the target domain. The strength of an analogy often depends on how well these elements align and whether the relational structure between them is preserved across domains. Methodologies from other domains, such as the Haddon Matrix (presented in Section 4), are fruitful sources for determining which concepts to explore within the analogy.

Second, good analogies satisfy the criteria of relevance. Relevance refers to the extent to which the similarities highlighted by the analogy are pertinent to the argument or concept being explained. It is not enough for two objects to be similar; their similarities must be relevant to the properties or relations being transferred.

Third, the analogy should be generalizable. Generalization refers to the potential of the analogy to apply beyond the immediate comparison. A good analogy should demonstrate that the relationships and properties observed in the source domain can plausibly be extended to the target domain, making the analogy more robust and widely applicable.

We propose categorizing analogies and their components into three color-coded categories that denote the applicability and utility of the analogy. To categorize aspects of analogies into green, yellow, and red, we propose criteria based on the evaluation principles discussed below. Note that an individual analogy can have multiple colors: some aspects can be green, while others are yellow or red. Table 1 differentiates how the color of each analogy aspect corresponds to these criteria. Green analogy aspects are highly effective and reliable. Yellow analogy aspects are moderately effective but have some limitations. Red analogy aspects are ineffective or misleading.

How to distinguish green from yellow from red in an analogy depends on the purpose of the analogy. For example, relative size is a green aspect in an analogy between planets and marbles because that is the analogy's purpose. One can then ask how far the analogy can be taken. We can observe that size relates to mass, and mass is proportional to momentum, so relative momentum is in the yellow aspect of the analogy. Finally, we can see that marbles do little to model atmosphere, life sustainability, and magnetic fields, so we say these aspects are red (poorly applicable).

An analogy draws attention to the similarities between the subjects, not the differences. However, no rule limits us to a single analogy for understanding a new domain. Many, possibly overlapping analogies, are likely to prove useful. What is red for one

	Green Analogy Aspects	Yellow Analogy Aspects	Red Analogy Aspects
Structural Similarity	Clear, one-to-one correspondence between concepts in source and target domains, preserving relational structure.	Useful correspondence between concepts in source and target domains, preserving some relational structure.	Little correspondence between concepts in source and target domains, or the relational structure is distorted.
Relevance	Similarities are highly relevant to the argument or concept explained.	Similarities are relevant but may not cover all aspects of the argument or concept explained.	Similarities are irrelevant or confusing to the argument or concept explained.
Generalizability	Many relationships and properties in the source domain extend well to the target domain.	Some relationships and properties in the source domain may apply to the target domain.	Few or no relationships and properties extend from the source domain to the target domain.

Table 1: Criteria for stoplight colors of analogy aspects based on structural similarity, relevance, and generalizability.

analogy may be green for another. That difference does not make one analogy better than another; it just makes it differently useful.

The following subsections discuss how to analyze an analogy and mine it for its knowledge potential. We will use a running example of a game of cat and mouse as an analogy for cybersecurity.

2.1.1 Structural Similarity: Analogy Key Concepts. Identifying the key concepts to establish structural similarity begins with the analogy's purpose. We can then categorize each aspect's analogy color. We observe that how detailed we decompose the analogy into constituent aspects and how deep (layers) we go is a matter of the analogy's purpose and the energy and creativity an analyst wishes to invest.

To facilitate analogy decomposition, we provide a detailed and precise description of the base analogy to which we plan to compare cybersecurity.

Description. The cat-and-mouse game is a dynamic contest of pursuit and evasion, where the cat uses its strength, speed, and cunning to catch the mouse, while the mouse relies on agility, reflexes, and tactics to escape. Both participants adapt their strategies, with the cat attempting to outmaneuver and trap the mouse and the mouse continuously seeking opportunities to evade capture by exploiting its environment and the cat's weaknesses. This ongoing struggle showcases the complex interplay of offense and defense, where each side leverages its strengths to achieve victory.

Next, we explore some key aspects to illustrate decomposition.

Pursuit and evasion between a pursuer (the cat) and the pursued (the mouse) is one aspect in which the more powerful pursuer's goal is to catch the mouse to eat it, while the pursued's goal is to evade capture and survive, using speed, agility, and strategy.

Complexity results from the dynamic behaviors of both the cat and the mouse, their respective experience and skill levels, and environmental variables such as terrain and weather make it a priori unpredictable as to who will win any given "game."

Strategy and tactics are employed by both cat and mouse in the pursuit game. Each plays to their strengths, such as the cat's size and speed and the mouse's agility and hiding skills.

2.1.2 Analogy Mapping Concepts. To determine the degree to which an analogy component is structurally similar to the target domain requires mapping each from the pursuit-game domain to the cybersecurity domain.

Pursuit and evasion. The analogy can be applied in both directions. The cat could represent the cyber attacker, with its speed of attack and advanced planning taking the defender by surprise. The defender would be the mouse, reacting to the cyber attack, using their skills and strategy to evade it. Similarly, one could view the defender as the cat trying to thwart the cyber attacker, identify them, and possibly have them incarcerated for their crimes. Many sub-aspects to this aspect are green. One could dive deeper and ask what sorts of strategies cats and mice employ and examine sub-sub-aspects of this analogy aspect. The analogy breaks down (is red) in the sense that neither party is literally trying to kill the other, so the nature of the stakes is different. The aspect of speed is yellow. Cats are about four times faster than mice running in a straight line. Thus, mice employ quick turns, hiding, and deception to escape. The analogous cyber attack speed might be the time it takes to accomplish its mission or the speed of a defender's reaction in terms of time to detect, time to react, and effectiveness of reaction to mitigate damage. The indirect mapping makes this subaspect yellow because it needs reinterpretation from the cat-mouse domain to cyberspace operations.

Complexity. The outcome of any conflict between a cyber attacker and a cyber defender is generally too complex to predict because it depends on highly variable factors of skills, tools, experience, on-the-fly adaptation, and sometimes luck. The concept of highly complex system unpredictability is green between the two domains. The specifics of terrain and environment do not map and generalize well from one domain to the other, such as the fact that the mouse's small size allows it to hide in places the cat cannot reach. Such aspects are red.

Strategy and Tactics. The concept of strategy and tactics honed with experience is common to both domains and is, therefore, green. The interaction of these strategies and tactics, how and when they are employed in a situation-dependent way, the timing of deployment, and the decision process to deploy them are common to the two domains. The specifics of the interactions likely determine the

outcome probabilities. One could assess the nature of this interaction's effect on outcome and transfer the principles from one domain to the other.

2.1.3 Generalization: Applicability and Adaptability. While the conceptual mapping provides a framework for understanding parallels, it is important to recognize that the realms operate under fundamentally different principles. Evolutionary pressures, genetic variability, and complex behavior interactions influence biological systems. Digital systems are human-designed, rule-based, and can be systematically analyzed and modified. Returning to the cat-and-mouse-game analogy, we observe the following.

Pursuit and evasion. Pursuit and evasion depend on the pursuer, the evader, and the terrain. Cats and mice are driven by instinct with a primary goal of survival. Their terrain is fixed to be whatever it happens to be where they encounter one another. Although cats and mice can be good models for humans in some ways (all are animals), their instincts, capabilities, and intelligence differ substantially from those of humans. For example, the reaction time of a cat (around 20 milliseconds) is nearly five times faster than that of a mouse (around 100 milliseconds), which is as much as twice as fast as a human (as slow as 200 milliseconds). We have the added complication of humans having computer processes operating on their behalf, with reaction times well below the millisecond range. We also have other interesting factors, such as time-to-detect and time-to-react (which includes planning time and execution time), to consider, making the analogy all the more rich to explore.

Complexity. Although the complexity of interaction between cat, mouse, and terrain is conceptually similar to the complexity of attacker, defender, and cyberspace, the number of degrees of freedom involved in the digital domain makes its complexity far greater. Attackers and defenders can ally themselves to extend their capabilities quickly. Both can modify the terrain in which the conflict occurs (e.g., the defender reconfiguring firewall rules of operation), sometimes simultaneously. On the one hand, these sub-aspects limit the degree to which knowledge from cat-and-mouse games carries forward to the cybersecurity domain, but on the other, tip us off to deeply consider these sub-aspects to transform more knowledge between domains or at least develop interesting hypotheses to explore.

Strategy and Tactics. The concept of planning and strategy likely only applies to humans because of their reasoning ability, and thus, strategy is yellow in that it is an extension of tactics. Also, the notion of strategy and tactics extending beyond the experience of a single individual (through documentation) does not apply well in the cat-mouse domain but definitely applies in the human cyber-conflict domain.

2.1.4 Practical Implications. Studying analogies is intellectually interesting, but so is discerning the practical implications of the design and operation of cybersecurity systems. Just as the study of birds has influenced the design of airplane features, we can take inspiration from our analogies. Thus, we show here how analogies can suggest ideas for cybersecurity.

Agility and Adaptability. Although cats are five times faster, they only succeed around half the time. We liken cats to cyber attackers with the element of surprise, investing heavily in focused preparation. The mouse's agility and unpredictability allow it to overcome the cat's huge advantages. This suggests we must design and operate cybersecurity in ways that allow unpredictable agility (e.g., dynamic countermeasures to attack) and behavior-based adaptation of defensive mechanisms, like firewalls, to the nature of the detected attacks.

Continuous Monitoring and Reaction. Mice have a keen sense of smell and hearing, allowing them to detect the cat threat at a sufficient distance to avoid conflict entirely. This suggests the importance of effective intrusion detection systems tied into early-warning systems that adjust defense posture at the slightest hint of trouble (e.g., anomaly detection alerts) and, just as quickly, return to normal operations when warnings are determined to be false positives. This aspect also suggests that cyber defenders proactively hunt for threats within their systems.

Leveraging and Adapting Environment. Mice succeed partly because they can exploit their environment by blending into and hiding in small spaces that cats cannot follow. Although it would be hard for an enterprise to blend into the cyberspace terrain (assuming it has to be connected to the Internet), cybersecurity can leverage the high malleability of cyberspace by altering the terrain to create obstacles to attackers succeeding. For example, network segmentation can require attackers to succeed against multiple protection points for their attack to work. Customized intrusion detection parameters can make it difficult for an adversary to predict what actions trigger alarms. Frequent patches make it difficult for attackers to exploit the substantial terrain of known vulnerabilities in commercial systems.

Understanding these mappings and their limitations helps us appreciate the similarities and differences between domains, guiding appropriate strategies for dealing with each aspect.

In summary, all analogies can have green, yellow, and red aspects. Yellow aspects can have green sub-aspects as the analysis proceeds to the lower levels of the concepts. It is too facile to say that an analogy is bad because we can find one or even several red aspects. Such a hasty judgment may cause the community to lose out on potentially valuable knowledge and insight and inspire useful hypotheses to be pursued rigorously.

2.2 Example: Computer Viruses Are Like Biological Viruses

To help understand how to apply our proposed framework, we analyze viruses as one common analogy used in cybersecurity with respect to the framework. Table 2 shows the analysis of nine aspects of the analogy between biological viruses and computer viruses. Each aspect is considered independently and given a color coding.

Analogy Aspect	Biological Viruses	Computer Viruses	Aspect Strength
Replication	Invades host cells and uses the cell's machinery to copy itself.	Inserts code into programs or files and replicates across systems and networks.	[Green] Self-replication using host's resources. Biological virus replication relies on complex biochemical processes within living cells, which include nuanced interactions with cellular machinery. In contrast, computer viruses rely on code execution within digital environments, governed by programmed rules.
Mutation	Undergo genetic mutations, leading to variations that can evade the immune system	Can alter their code slightly with each infection (polymorphic viruses), making them harder to detect	[Yellow] Biological mutation is natural and random, while computer virus mutation is intentional and programmed. Biological mutations are driven by genetic replication errors and environmental factors. Computer virus mutations are intentional and programmed by humans, limiting the randomness and typically following predictable patterns to evade detection.
Host Range	Have specific host ranges, infecting certain species or cell types.	Target specific operating systems, applications, or hardware platforms.	[Yellow] The specificity of biological viruses is determined by the presence of specific receptors on host cells, influenced by evolutionary pressures. Computer-virus host range is determined by compatibility with operating systems or software, which is more easily modified by human programmers.
Transmission	Direct contact, airborne droplets, vectors, or surface contamination.	Emails, downloads, network connections, and removable media.	[Green] Spreading from host to host through various routes. Biological virus transmission is affected by factors such as human behavior, immune responses, and environmental conditions. Computer virus transmission relies on data exchange methods that can be controlled by software settings and network protocols.
Pathogenicity	Cause disease, with varying degrees of severity depending on the virus and host.	Cause damage to computer systems, from minor annoyances to major data loss or system corruption.	[Yellow] Cause harm to their hosts, but the nature and impact of the harm differ. The effects of biological viruses on organisms involve complex interactions with the host's immune system and can result in a wide range of health outcomes. The damage caused by computer viruses is limited to data and software corruption, with variable severity, depending on the mission of the virus.
Latency	Can enter a latent state, remaining dormant within the host until triggered.	Can remain hidden and inactive within a system until an event triggers activation	[Green] Dormant phase activated by specific triggers. Biological virus latency involves complex regulatory mechanisms within the host cell, influenced by the host's immune response and cellular environment. Computer virus latency is simpler, often involving pre-programmed triggers like specific dates or user actions.
Immune Evasion	Evolve mechanisms to evade the host immune system, such as changing surface proteins.	Use techniques to avoid detection by antivirus programs, such as encryption and code obfuscation.	[Green] Use strategies to evade host defenses. Biological immune evasion involves sophisticated strategies like antigenic variation, immune suppression, and hiding within cells.. Computer viruses use evasion techniques that are less sophisticated and can be countered by updating antivirus software and security protocols.
Environmental Stability	Vary in their ability to survive outside a host; some can remain infectious on surfaces for extended periods.	Can remain dormant on systems or media until activated, while others require specific conditions to be met to become active	[Red] The environmental stability of biological viruses is influenced by factors like temperature, humidity, and surface types, which can affect their viability outside a host. Computer viruses do not face such environmental constraints and their "survival" is purely a matter of data storage and file integrity
Lifecycle	Lifecycle includes attachment, entry, replication, assembly, and release from the host cell.	Lifecycle includes insertion into a host file, replication within the system, and spreading to other files or systems.	[Red] The lifecycle of biological viruses is tightly integrated with host cell biology and involves stages like uncoating, replication, and assembly, influenced by the host's metabolic processes. The computer-virus lifecycle is governed by programmed instructions and depends on less dynamic and compex system interactions.

Table 2: Comparison of nine aspects of the analogy between biological viruses and computer viruses.

3 PUBLIC HEALTH AND PUBLIC SAFETY MODELS IN CYBERSECURITY

The idea of using biological, public health, and public safety analogies to understand cybersecurity challenges has been a recurring theme in cybersecurity for nearly four decades. The concept is based on the notion that just as public health and safety professionals work to prevent and mitigate the spread of threats, cybersecurity practitioners can learn from their approaches to improve the security posture of networks and systems.

3.1 Public Safety Example: Fire Safety Codes

Catastrophic events such as the Great Chicago Fire of 1871 inspired the development of fire safety codes. Such events in cyberspace should inspire similar safety codes in the way systems are developed to minimize the probability of a successful attack on one system that spreads to others [11].

Fire safety codes are regulatory standards that mandate the use of fire-resistant building materials, enforce urban planning and zoning laws to limit fire spread, improve fire department capabilities, promote fire prevention and safety education, and establish national fire safety initiatives, all aimed at reducing the risk and impact of fires in urban environments. Key analogy aspects include:

- **Building Construction Regulations**—building codes requiring the use of fire-resistant materials like brick, stone and steel, as well as electrical system standards.
- **Urban Planning and Zoning**—building placement rules such as minimum street widths and open spaces to reduce the chance of fire jumping between areas of a city.
- **Early Detection and Response**—alarms and sprinkler systems to quickly detect and suppress fires before they spread.
- **Fire Department Improvements**—more fire stations, better training, and better equipment.
- **Fire Prevention and Safety Training**—increase awareness and planning through fire alarms, fire drills, and public education campaigns.
- **Advocacy**—creation of organizations to advocate for improvements in these areas.

A comparison of analogy aspects between fire safety codes and cybersecurity is detailed in Table 3.

Understanding these mappings can help in developing more comprehensive cybersecurity strategies by borrowing effective principles from fire safety codes.

3.2 Public Health and Safety Success Stories

Concerns regarding human health are as old as humanity itself. For thousands of years, advances in knowledge and practice were slow and limited. However, those advances have accelerated with the application of the scientific method and other breakthroughs. Healthcare is a broad term that includes medicine, the prevention, treatment, or relief of symptoms from diseases or abnormal conditions in individuals. Healthcare also includes public health, which focuses on preventing disease injury among populations of people. To our knowledge and surprise, there has never been a consolidated compilation of successes in public health. Nevertheless, we offer five exemplar successes illustrating how the field has carried out this definition in practice. In the subsequent section, we will explore how these lessons apply to cybersecurity.

John Snow and the Broad Street water pump. Nineteenth-century London was replete with outbreaks of disease. In 1854, an outbreak of cholera occurred in Soho. Dr. Snow, an obstetrician, noted that "Within 250 yards of the spot where Cambridge Street joins Broad Street, there were upwards of 500 fatal attacks of cholera in 10 days." He offered the then-unusual hypothesis that the well from which most residents drew their water was the cause. He convinced town officials to remove the well's pump handle. The outbreak subsided immediately [17].

Development and distribution of the polio vaccine Polio has afflicted humans for thousands of years. By the mid-twentieth century, half a million people worldwide were killed or paralyzed by the virus every year. In 1955, Dr. Jonas Salk and his team announced their success in developing and testing an effective polio vaccine. A worldwide effort was undertaken to administer the new vaccine. By 1957, annual cases in the U.S. had dropped by 90%, and by 1961 only 161 cases were reported. Worldwide vaccine distribution was much slower, but annual cases dropped from 350,000 in 1988 to six in 2021 [20].

Eradication of smallpox As with polio, smallpox has caused hundreds of millions of illnesses and deaths for thousands of years. The first true vaccine was not developed until 1796. Unlike polio, two million people a year were still dying of smallpox a hundred years later. In 1959, the World Health Organization launched the Smallpox Eradication Programme. In 1980, the program, led by Dr. D. A. Henderson, succeeded in completely eradicating smallpox—the only disease to have been so [20].

Campaign to reduce cigarette smoking Many health professionals long suspected that cigarette smoking was related to disease incidence, especially cancer and heart disease. Scientific evidence was sufficient by the 1950s to justify efforts to reduce smoking. These efforts were only moderately effective until the U.S. Surgeon General's report, Smoking and Health, in 1964, catalyzed public opinion and government action. Cigarette ads were banned on television and radio; smoking was banned on all U.S. domestic airlines; and smoking has been banned in many bars, restaurants, and worksites. Smoking rates have declined dramatically since 1965, from 42% to 14% of adults [12].

Motor vehicle safety Over the past century, remarkable progress has been made in reducing the fatality rate caused by motor vehicles. Since 1960, the number of deaths attributable to motor vehicles has grown somewhat, from 38,137 in 1960 to 42,338 in 2020. However, the rate per population has fallen 39%, and the rate per vehicle miles traveled has fallen by 73% over that period. Public health experts [10] have three explanations: better drivers, better cars, and better roads.

These instances reveal multiple ways that public health has achieved its goals. In the John Snow case, a single intervention—backed by compelling data and intense debate—was all that was needed. The success of the polio vaccine, however, resulted from years of research and vaccine development, the palpable fear of the disease (including the salience of its targeting of young children), and the one-and-done intervention of a single injection. The smallpox eradication campaign differed markedly from polio: An effective vaccine had been available for two centuries; the issue

Analogy Aspect	Fire Safety Codes	Cybersecurity	Aspect Strength
Building Construction Regulations	Use fire barriers, firewalls, and containment zones to prevent the spread of fire.	Use secure coding practices, regular software updates, and lifecycle security.	[Yellow] Both focus on reducing the risk of incidents through proactive measures, though the specific practices differ.
Urban Planning and Zoning	Regulate building placement, like minimum street widths and open spaces, to reduce fire spread between city areas.	Implement network segmentation, firewalls, and isolation to prevent malware spread and unauthorized access.	[Green] Both involve controlling connections between components of the larger system to reduce risk.
Early Detection and Response	Require smoke detectors, fire alarms, and sprinkler systems to detect and respond to fires early.	Develop incident response plans, including containment steps, eradication, recovery, and good communication.	[Green] Strong correlation; both involve early detection systems to identify and mitigate threats before they cause significant damage.
Fire Department Improvements	More fire stations, better training, and better equipment.	Local and community incident response team, with tools, and training to respond correctly to cybersecurity incidents.	[Yellow] The focus on rapid response and preparedness maps well, as both scenarios require immediate action to mitigate damage. Cybersecurity more intimately involves operators of systems under threat.
Fire Prevention and Safety Training	Increase awareness and planning through fire alarms, fire drills, and public education campaigns.	Educating users about phishing attacks and more secure behaviors (e.g., password choice) reduces attack surface.	[Green] Educating people on how to reduce incidents, and its significant effect on incidents, is common between both domains.
Advocacy	Creation of organizations to advocate for the improvements in all of these areas.	Cybersecurity standards and regulatory compliance (e.g., FISMA, GDPR) and standards organizations such as NIST, IETF, ISO, IEEE.	[Yellow] The role of standards and compliance within the two domains is abstractly similar, but the details of their roles and authorities differ substantially.

Table 3: Comparison of six aspects of the analogy between fire safety codes and cybersecurity.

was distribution, which required financial and logistical support from hundreds of countries and health-related agencies and widespread public acceptance and cooperation. That smallpox remains the only fully eradicated disease is testimony to the clinical and managerial challenges such an initiative requires. The success of the anti-smoking campaign demonstrates the importance of establishing challenging yet achievable goals and using multiple approaches. To that end, despite the multiple efforts to reduce smoking—banned ads, myriad public service announcements, high cigarette taxes, smoking bans in public places, and smoking cessation programs—31 million adults in the U.S. still smoke, spending $76 billion a year [12]. Finally, the dramatic advances in motor vehicle safety have resulted largely from improvements in the environment—that is, vehicles and roads—that did not require changes in individual behavior.

What all of these public health successes had in common was the power of persistence. While each included a breakthrough, they needed a push to completion. John Snow faced considerable skepticism from both community leaders and the scientific community. His ideas contradicted the deeply held prevailing theory of disease. Confident that his data were correct, Snow accepted the challenge of a short-term trial, even though it potentially set back full implementation. With polio, acceptance of the vaccine was not an issue, as parents everywhere clamored for their children to receive it. The persistence stemmed from the research and clinical trials necessary to obtain government approval for the vaccine and the ongoing efforts to eradicate polio entirely. With smallpox, total eradication of the disease required an extraordinary effort to vaccinate the entire population and seek out and treat the remaining cases, a process that went well beyond what economic theory would have deemed an efficient use of resources. The anti-smoking campaign faced—and continues to face—the twin challenge of convincing active smokers to stop and overcoming the intense opposition of the tobacco industry. Motor vehicle safety similarly requires relentless persistence, given the slow journey away from human-centric vehicle risks.

3.3 Implications for Cybersecurity

These public health success stories yield insights that are relevant to people involved in cybersecurity. In this section, we describe how cybersecurity research and practice may be improved using lessons from these examples.

The first observation is that "magic bullets" (e.g., removed pump handles, vaccines) may work to a limited degree, but they rarely provide the complete solution. Removing the pump handle solved the cholera epidemic in the Soho neighborhood but did not address the overall problem of cholera and other water-borne diseases

throughout London. Unfortunately, magic bullets grab the public's and policymakers' attention and lead to the assumption that solutions to complex problems can be simple and free. Cybersecurity has also tried changing to take away choices of dangerous actions, such as automatically rewriting URLs in emails to make them non-clickable, which is a narrow solution but not a magic bullet for solving social engineering.

Next, even interventions that are effective might lose their social potency over time. If an intervention (such as vaccination against polio) is successful and the presenting problem disappears, the public and policymakers may assume that the problem has been solved and the intervention need not continue. In a related issue, the public and policymakers may grow weary of vigilance if the immediate threat has decreased and there is no discernible benefit of continued action. Public health has often needed relentless communication with the public and policymakers about the importance of a topic before its solutions begin to have an impact. Cybersecurity, similarly, has found that continuous communication plays a role, such as continued phishing awareness, despite advances in technological detection of email-based threats.

Getting people to stop doing something is usually more challenging than getting people to not do it in the first place. As research has shown, it is often tough for smokers to stop smoking (because of physical addiction and social norms); it is easier to convince nonsmokers not to start smoking, especially if peer pressure and attractive depictions of smokers are minimized. As a result, total success may take years, if not generations. This can be seen in cybersecurity advocacy for developing good habits for password hygiene.

In the case of campaigns to eradicate smallpox and polio, 100% adherence or eradication is rarely achievable. Consequently, it is critical to create challenging but achievable measures of success. At the same time, these goals must inspire and elicit continued support from key stakeholders. In cybersecurity, there have been gradual declines in buffer overflows, but they are not eradicated.

This raises an important distinction for public health and cybersecurity about the distinction between prevalence and new incidence. While a mitigation is being deployed and adopted, the prevalence of smoking or a digital virus may remain high while the incidence of new smokers or new cyber infections is low. According to the Centers for Disease Control and Prevention (CDC), the prevalence of tobacco use among people 25-44 years old in the United States is 25.3%, and those individuals are likely to continue. On the other hand, the incidence of tobacco use among this age group is 1.8%. These two concepts are important for understanding the dynamics of a disease or cyber attack within a population, as they provide different insights into the burden.

Finally, one commonality among these public health examples is the ability to measure harm, often in the form of infection or death. Even so, healthcare and public health have struggled with measuring progress. Cybersecurity, in particular, continues to lack universally accepted outcome measures and mandatory reporting to underpin measures of harm (and reductions thereof).

The five examples in this section show fortuitous lessons and commonalities between cybersecurity and public health, but they lack a unifying or repeatable model.

3.4 Other Public Health Analogies in Cybersecurity

As we have explored throughout the paper, there are many potential public health and public safety analogies in cybersecurity. One of the earliest examples of this approach is attributed to Fred Cohen, who, in his 1984 dissertation, explored the idea that computer viruses could be viewed as a form of biological virus and proposed the use of public health models to understand and combat their spread [5]. Cohen's work laid the foundation for later researchers who built upon his ideas. These have been studied in some depth. After the Morris worm of 1988, Spafford analyzed the event and raised caution about the lack of an "immune system" to protect computers [15].

A few researchers and practitioners in cybersecurity have been looking for public health models and methods that might inform the creation of more effective ways of countering cyber threats. In 2010, Rice et al. mapped and applied the tripartite public health structure of disease types (communicable, non-communicable), disease phases and severity, and public health "actors" (individuals, communities, health care providers, government) to construct generic strategies in cyberspace. Rowe et al. used four categories of public health threats (communicable diseases, non-communicable diseases, risk behaviors, and environmental exposures) to create a taxonomy of cybersecurity threats [13]. Weber focused on the implications of cybersecurity interventions on the tendency within public health to engage in what Weber termed "coercive" measures (ranging from mandated seat belt use to quarantines during epidemics) [18]. In essence, Rice took a method from an analogous domain, mapped it into cybersecurity using structural similarity, and then applied it to cybersecurity. These advances make progress in aiding cybersecurity, but more possibilities remain.

By examining the evolution of public health analogies and methods in cybersecurity, we can see how researchers have built upon each other's work to develop a more comprehensive understanding of our digital society's challenges. From Cohen's early exploration of computer viruses as biological agents to Rice's adaptation of traditional public health approaches for cybersecurity and Weber's analysis of coercion through public health models, this body of research has provided valuable insights into how we can use public health principles to improve cybersecurity.

As expected from a field more than 100 years old, public health researchers and practitioners use a variety of conceptual models and frameworks to understand and address health problems. These models are used to identify the causes of a health problem, develop interventions to address the problem, and evaluate the effectiveness of those interventions. Even more public health models are likely to be relevant to cybersecurity and could be evaluated using our framework for analogies.

Some public health models are specific to a threat or feature thereof. For instance, numerous models in public health are used to study epidemiology. Between 1927 and 1933, public health physicians A.G. McKendrick and W.O. Kermack produced basic compartmental models describing communicable disease transmission [4]. For instance, the Susceptible-Infectious-Recovered (SIR) model structure is a simple form of this type. This class of models may apply to the study of cyber threats such as worms.

The Haddon Matrix, presented in the next Section, is an example of a class of social-ecological models that take a more holistic approach to understanding health [8]. The social-ecological model recognizes that health is influenced by a wide range of factors, including individual, community, and societal factors. One common public health model structure is the epidemiological triangle, which identifies three key elements that contribute to the occurrence of a health problem: the agent, the host, and the environment. The agent is the pathogen or other factor that causes the disease. The host is the person who is infected with the pathogen. The environment is the physical and social setting in which the disease occurs. The Haddon Matrix is one model that employs the epidemiological triangle.

Public health models can guide the development of interventions to address problems. For example, if a public health model identifies that a lack of access to healthcare causes a health problem, then an intervention could be developed to provide more people with access to healthcare. The PRECEDE-PROCEED Model is a framework for planning and evaluating health promotion interventions [6]. It consists of two phases: PRECEDE (Predisposing, Enabling, Reinforcing Causes, Educational Determinants, Community and Policy Determinants) and PROCEED (Planning, Resources, Economic Costs, Organizational Readiness, Evaluation, Dissemination).

The breadth of public health models and analogies has supported diverse lines of effort toward health goals. However, as one author summarized, "there is always a trade-off between simple, or strategic, models, which omit most details and are designed only to highlight general qualitative behavior, and detailed, or tactical, models, usually designed for specific situations including short-term quantitative predictions" [4]. This caution also applies to cybersecurity.

4 THE HADDON MATRIX

Given the utility of some public health models to cybersecurity in the past, we were motivated to explore other potential leads for health-related analogies. We have identified a lesser-known conceptual model from public health that shows promise for cybersecurity: the Haddon Matrix. As far as we can tell, this approach has not yet been widely adopted in cybersecurity despite its utility in public health and safety science. William Haddon was the director of the National Highway Safety Bureau in the U.S. Department of Transportation in the 1960s. In an article in the American Journal of Public Health [9], he articulated what has become a 3x3 matrix to analyze the causes and potential remedies for injury-causing events. One axis represented the phase of the injury-causing event (pre-event, event, post-event), and the other axis represented the event's components (or instruments). Haddon suggested that two matrices be created, one to identify the causal factors and the other to identify countermeasures. Haddon's approach in the public health domain has the tremendous advantage of inducing analysts to think broadly over all aspects of a problem and solution space, opening up the aperture of possibilities, and creating new opportunities for insight. Over the past 24 years, the Haddon Matrix has been used to study SARS preparedness and response, COVID-19 containment in nursing homes, medical response strategies to subway bombings, and other critical health and safety considerations.

To illustrate a traditional use of the Haddon Matrix, Tables 4A and 4B demonstrate how they can be used to analyze the causes of vehicle accidents and countermeasures. First, note that the "components" recall the factors discussed earlier: humans (driver and passengers), vehicles, and the environment (the roadway and surroundings). Table 4A shows the causal factors of vehicle accidents. Pre-event causes include inexperienced and distracted drivers, vehicles not designed to avoid accidents, and roads not designed to reduce the chance of an accident. As the event occurs, accidents are made worse because drivers lack situational awareness, vehicles are not built to mitigate the consequences of the accident, and roads are similarly not designed to lessen the impact of an accident. After the accident, the situation may be exacerbated in the short run by an emergency management system that cannot rapidly respond. In the long run, drivers do not learn from their mistakes, and vehicle manufacturers and road engineers do not conduct root-cause analyses of accidents.

Table 4B shows the now-familiar countermeasures implemented over the past century to reduce the probability and impact of vehicle accidents. The human side includes graduated driver's licenses (pre-event), mandated seat belts (event), and penalties for drunk driving (post-event). Vehicles now have third-brake lights (pre-event), airbags (event), and a redesign of gas tanks to minimize explosions. The road environment has been improved to reduce the probability of an accident (with speed bumps, rumble strips, and Botts' dots on the road surface), reduce the immediate harm of an accident (with guardrails and crash cushions), and lessen the severity of harm from the accident (with better EMS response). The breadth of considerations offered by the matrix is impressive.

From the discussion in this and other papers, the approaches used in public health can be instructive for cybersecurity. In particular, we think the Haddon Matrix offers a promising new framework for analyzing issues and solutions in cybersecurity. Tables 5A and 5B present an example of applying this paradigm to credential theft where the "agent of injury" is a ransomware attack. Pre-event causes include human aspects of the attacker and the victim, causal factors of the threat, and environmental factors such as issues relating to holding data or infrastructure of the victim 'offline.' When the incident occurs, the impact is influenced by how distracted the victim is and how easy it is to detect that the data or system has been compromised before the loss of access. After the incident, the harm may be exacerbated by psychological distress to the victim and the value of data/systems, loss of access, or loss of confidentiality/proprietary ownership. Countermeasures are also presented for pre-event, event, and post-event timeframes across the human element, attributes of the attack methodology, and environmental factors.

While ultimately powerful and generally applicable, the approaches that drove the public health successes presented earlier did not happen by using the Haddon Matrix. While one could complete the Matrix in hindsight as documentation of what has already been tried or successful, it is even more potent in the brainstorming, discovering, and proposing of opportunities for open problems. Ransomware, for example, remains unsolved despite many preventative efforts. One reason is that many attack and system access avenues are not identified before victimization. One could imagine a yet-unrealized proposal putting a theoretical cost on access

	Human	"Agent of Injury"	Environment
Pre-event (Reduce probability of event)	1. Inexperienced drivers 2. Distracted drivers 3. Incapacitated drivers	1. Vehicles not designed to avoid accidents 2. Vehicles do not communicate sufficient information to driver to anticipate accident	1. Roads not designed to avoid accidents 2. Poor street lighting
Event (Reduce immediate harm of event)	1. Lack of situational awareness 2. Lack of knowledge of how to react to accident	1. Vehicles not designed to mitigate consequences of accidents	1. Roads not designed to mitigate consequences of accidents
Post-event (Ameliorate further injury or future event)	1. Lack of understanding of causes of accident, and how improve skills	1. Lack of post-accident analysis of root causes	1. EMS system not designed to respond rapidly to accident scenes 2. Lack of post-accident analysis of root causes

Table 4A: A Haddon Matrix for Vehicle Accidents: Causal Factors

	Human	"Agent of Injury"	Environment
Pre-event (Reduce probability of event)	1. Minimum legal drinking age 2. Random breath testing 3. Graduated driver's licenses	1. Mandated third brake light 2. Unleaded gasoline	1. Roundabouts 2. Speed bumps 3. Red light cameras 4. Rumble strips and Botts' dots
Event (Reduce immediate harm of event)	1. Seat belt mandates 2. Mandated helmet laws	1. Child safety seats 2. Energy-absorbing steering columns 3. Air bags 4. Head rests	1. Guardrails 2. Crash cushions
Post-event (Ameliorate further injury or future event)	1. Penalties for drunk driving 2. Mandated DE classes	1. Gas tank redesigns (no more Pintos)	1. Rapid EMS response

Table 4B: A Haddon Matrix for Vehicle Accidents: Countermeasures

	Human	"Agent of Injury"	Environment
Pre-event (Reduce probability of event)	1. Volume of email received by victim 2. Inadequate awareness and training 3. Dangerous habits and online behavior	1. Potential for attacker to make money 2. Strong dependence of victim to need access/control. Victims care. Business loss.	1. Insecure device and software security configurations 2. Lack/insufficient Legal and regulatory framework. 3. Lack of data backups
Event (Reduce immediate harm of event)	1. Tendency to trust/believe 2. Fear of loss 3. Decision-making under stress or pressure. Action bias.	1. Revel attack at time of attacker's choosing. 2. Attacker controls what you know, including their own motivation and capability.	1. Real-time cybersecurity monitoring and response 2. Ineffectiveness of email filtering and security tools 3. (Un)Availability of assistance or guidance for users
Post-event (Ameliorate further injury or future event)	1. Emotional and psychological impact on the victim (patient and/or hospital) 2. Willingness to learn from the experience. Changed behavior?	1. Misuse/release of stolen information 2. Persistence of the attacker in the system 3. Minimal/no consequences for the attacker if identified and prosecuted.	1. Value of the data 2. Lateral access to systems and information 3. Financial industry willing to accept losses, use insurance. 4. HIPAA compliance penalties.

Table 5A: A Haddon Matrix for Hospital Outage from Ransomware: Causal Factors

	Human	"Agent of Injury"	Environment
Pre-event (Reduce probability of event)	1. Awareness and training 2. Incentives to avoid infection, including data storage.	1. Pre-screening, behavioral analytics 2. Ransomware detection tech	1. Multi-factor authentication 2. Incentives to improve cyber hygiene 3. Better data storage and backups. Network partitioning and isolation
Event (Reduce immediate harm of event)	1. Victim recognizes the incident 2. Takes proper immediate actions 3. Isolation of account/ machine from other access/connectivity	1. Real time mitigations/isolation 2. 2. Alerting to admins, ISP and partner providers 3. 3. Engagement between admin and user	1. Incident response capability and effective response plan. 2. Increase validation measures for transactions 3. Virtualize/isolate system; zero trust methods 4. Begin data backup recovery.
Post-event (Ameliorate further injury or future event)	1. Victim reports the incident 2. Updates passwords and credentials 3. Reviews systems for similar infections.	1. Add a signature of the malware. 2. Attribution and tracking of the attack 3. Initiate new backup	1. Cyber insurance 2. Legal actions and consequences for the attacker. Work with proper authorities. 3. Patching. 4. After action report

Table 5B: A Haddon Matrix for Hospital Outage from Ransomware: Countermeasures

that makes it more expensive for attackers (with an obvious, but hopefully less painful, cost to legitimate users).

It is insightful to note where there are gaps when completing the Haddon Matrix. These may be individual boxes, rows, or columns with few entries and represent under-explored opportunities for examination. In our countermeasures for ransomware (Table 5B), there are more countermeasures pre-event than before and after. For ransomware specifically, this illustrates a gap in that victims lack real-time tools for detecting and mitigating the breaches. The gap is also indicative of a general bias towards risk mitigation (i.e., prevention) when risk management (e.g., incident response) is equally essential.

The Haddon Matrix offers a structured framework for systematically analyzing the factors contributing to cyber threats, including before, during, and after the event. This structured approach can help cybersecurity professionals identify vulnerabilities and potential intervention points. It is also interdisciplinary. Causal factors and countermeasures can include technical, legal, and policy components. This holistic view can provide a more structured understanding of the threat landscape. The Haddon Matrix encourages us to think about cybersecurity from various perspectives and develop a holistic approach to cybersecurity rather than single mitigations.

At the same time, the Haddon Matrix is flexible for broad and diverse uses across cybersecurity. This makes it ideally suited as a teaching aid in brainstorming sessions, tabletop exercises, and assessment of existing initiatives. The Haddon Matrix could be used to develop security awareness training programs tailored to the organization's specific needs. For example, the training could focus on the pre-event factors (e.g., phishing awareness) or the event factors (e.g., incident response). It could also be used to conduct risk assessments that document and evaluate an organization's cybersecurity risks and implement appropriate controls. Finally, we recently used the Matrix to communicate the importance of cybersecurity to non-technical corporate decision-makers.

There are, of course, limitations in using the Haddon Matrix method from the public health domain for the cybersecurity domain. Because it was initially designed for physical injuries, there is a heavy emphasis on human and environmental factors. As a result, it may not delve deeply enough into the technical details of specific cyber threats. The framework also does not include a quantitative component, and its qualitative and descriptive approach requires evaluating the impact of various factors or prioritizing interventions.

Because the Haddon Matrix is an analysis approach from the public health domain, it may need some mapping and reinterpretation in the analogous domain of cybersecurity. Like analogous knowledge, analogous tools must be applied carefully, considering their strengths and weaknesses as key concepts are mapped. At the same time, the Haddon Matrix also creates a beautiful structure to expand the concepts and considerations in risk analysis and mitigation in any domain in which it is applied. Thus, this analogous tool increases the power of the analogy analysis framework we introduce by expanding the number of concepts and aspects to consider in the analogous knowledge from other domains (not just public safety).

Applying the evaluative framework presented in Section 2, aspects of the Haddon Matrix are both green and yellow. Note that the Haddon Matrix is a tool and not an analogy since we propose using it directly as designed. However, we have based this approach on analogous concepts, such as environmental factors influencing physical injury and cybersecurity incidents. Aspects of the Haddon Matrix that should be evaluated include different phases of incidents, independent components of incidents, and causal factors that reveal countermeasures. One aspect is green: physical safety and cybersecurity are influenced by human victims, system designers, and attackers. The "agent of injury" is a yellow aspect. In our experience creating the ransomware matrix, it was most challenging to untangle the agent of injury between delivery and harm, making it yellow and needing reinterpretation. That is, a phishing email may be the root cause of ransomware, even though ransomware was what caused the harm. Overall, the Haddon Matrix is consistent with green analogies, meeting criteria such as strong structural similarity, high relevance to the concept of harm, generalizability of relationships between model components, and properties from the source domain to the target domain. In this case, the Haddon Matrix appears to satisfy all these conditions, solidifying its categorization as a green analogy.

5 CONCLUSION

Cybersecurity benefits from fresh ideas. In a healthy and innovative ecosystem, cybersecurity professionals should always seek leads from other domains to combat persistent and emerging threats. Using biology and public health concepts to describe cybersecurity threats has become commonplace. However, less consideration has been given to approaches developed and applied by public health and public safety. We explore how public health experts think about their problems, the approaches they have tried, what worked, and when those approaches could be applied in cybersecurity. In this article, we have tried to widen the aperture of approaches to make a new perspective from the mature field of public health salient. Prior successes in public health encourage us to find equally powerful successes in cybersecurity. Indeed, there appears to be overconfidence in the existing approaches to cybersecurity. It is time to revisit public health approaches for cybersecurity.

The community of cybersecurity professionals advocating for a public health approach to cybersecurity needs support. The nonprofit CyberGreen Institute has begun to publish analyses of lessons from public health to cybersecurity [14]. Subdomains of cybersecurity, from hardware engineering to incident response, are likely to find specific parallels and inspiration from specific approaches to public health. Additional research and advocacy will strengthen the case for ideas inspired by public health, just as cyber hygiene has become mainstream. Tools like the Haddon Matrix, with modest reinterpretation, are available for adoption today.

As with all analogies, caution is required in the imperfect comparison between cybersecurity and public health. While instructive for suggesting potential new mitigations and leads, relying too rigidly on analogies can be derailed by inaccuracy, overgeneralization, and oversimplification. These pitfalls can be avoided by applying our stoplight framework. Similarly, analogous methods from other

domains, such as the Haddon Matrix can also improve both analytical approaches to the cybersecurity problem and can enhance the depth and breadth of knowledge considered in analyzing analogies to other domains. We do not see methods like the Haddon Matrix as the definitive evaluative framework that can be applied algorithmically, but rather, it is an initial strawman to enable researchers and practitioners to have a more sophisticated discussion on how to mine public health analogies for the concepts and principles that can advance our cybersecurity approaches. Other analogous methods from other domains should be similarly evaluated, including those we mentioned earlier, as well as methods such as hazard analysis from the safety domain, and root-cause analysis from the reliability domain.

While technological evolution and threats evolve quickly, insights from public health experiences and successes can better prepare us for future cyber threats. We look forward to the thoughtful evaluation of analogies and analogous methods using our framework and the specific adoption of the Haddon Matrix to fill gaps with fresh ideas.

REFERENCES

[1] Paul Bartha. 2019. Reasoning and Analogical Reasoning. *The Stanford Encyclopedia of Philosophy.* https://plato.stanford.edu/entries/reasoning-analogy/

[2] George EP Box. 1976. Science and statistics. *J. Amer. Statist. Assoc.* 71, 356 (1976), 791–799.

[3] Sonya S Brady, Linda Brubaker, Cynthia S Fok, Sheila Gahagan, Cora E Lewis, Jessica Lewis, Jerry L Lowder, Jesse Nodora, Ann Stapleton, Mary H Palmer, et al. 2020. Development of conceptual models to guide public health research, practice, and policy: synthesizing traditional and contemporary paradigms. *Health promotion practice* 21, 4 (2020), 510–524.

[4] Fred Brauer. 2017. Mathematical epidemiology: Past, present, and future. *Infectious Disease Modelling* 2, 2 (2017), 113–127.

[5] Fred Cohen. 1987. Computer viruses: theory and experiments. *Computers & Security* 6, 1 (1987), 22–35.

[6] Richard Crosby and Seth M Noar. 2011. What is a planning model? An introduction to PRECEDE-PROCEED. *Journal of public health dentistry* 71 (2011), S7–S15.

[7] Dedre Gentner and Keith J Holyoak. 1997. Reasoning and learning by analogy: Introduction. *American psychologist* 52, 1 (1997), 32.

[8] Karen Glanz, Barbara K Rimer, and K Viswanath. 2008. *Theory, research, and practice in health behavior and health education.* Jossey-Bass.

[9] William Haddon Jr. 1968. The changing approach to the epidemiology, prevention, and amelioration of trauma: the transition to approaches etiologically rather than descriptively based. *American Journal of Public Health and the Nation's Health* 58, 8 (1968), 1431–1438.

[10] David Hemenway. 2009. *While we were sleeping: success stories in injury and violence prevention.* Univ of California Press.

[11] Carl Landwehr. 2015. We need a building code for building code. *Commun. ACM* 58, 2 (2015), 24–26.

[12] Sam MacArthur. [n. d.]. Smoking as a Public Health Issue. https://www.mphonline.org/smoking-public-health/.

[13] Brent Rowe, Michael Halpern, and Tony Lentz. 2012. Is a public health framework the cure for cyber security. *CrossTalk* 25, 6 (2012), 30–38.

[14] Adam Shostack. 2022. *Public Health & Cyber Public Health.* Technical Report 22-01. CyberGreen Institute.

[15] Eugene H Spafford. 1989. The Internet worm program: An analysis. *ACM SIGCOMM Computer Communication Review* 19, 1 (1989), 17–57.

[16] Eugene H Spafford, Leigh Metcalf, and Josiah Dykstra. 2023. *Cybersecurity Myths and Misconceptions: Avoiding the Hazards and Pitfalls that Derail Us.* Addison-Wesley Professional.

[17] Kathleen Tuthill. 2003. John Snow and the Broad Street pump: on the trail of an epidemic. *Cricket* 31, 3 (2003), 23–31.

[18] Steven Weber. 2017. Coercion in cybersecurity: What public health models reveal. *Journal of Cybersecurity* 3, 3 (2017), 173–183.

[19] Hill Hibbert Winslow. 1916. *The New Public Health.* The Macmillan Company.

[20] World Health Organization. [n. d.]. A Brief History of Vaccination. https://www.who.int/news-room/spotlight/history-of-vaccination/a-brief-history-of-vaccination.