

Systems Thinking for Cybersecurity: A Reality-Based Approach

Michael Collins ^{a, @}

a: Independent Researcher

@: michael@cybercognition.com.au

ABSTRACT: The effectiveness of our current cybersecurity strategies, characterised by escalating financial expenditure and excessive dependence on technological solutions, is being challenged. The lack of corresponding improvement in outcomes suggests a paradigm shift in how we approach cybersecurity is required. Furthermore, the cybersecurity curriculum has been centered on building technical skills, with very little emphasis on teaching cognitive skills, or "how" to think about cybersecurity.

Despite being advocated as a remedy for the complex challenges of cybersecurity, systems thinking has largely fallen short of fulfilling all of its promises. This paper aims to bridge the gap by proposing a path forward that incorporates theory and practice, underpinned by extensive empirical evidence. When implemented by cybersecurity practitioners, this approach can reduce the competitive advantage of attackers by better organizing information to make sense of the complex world in which they operate.

This effectiveness of this approach stems from its ability to offer practitioners a more accessible and effective approach to thinking in cybersecurity. This reality-centric paradigm advocates an adaptive approach to cybersecurity, moving away from static, belief-based approaches and towards methods based on empirical evidence and practical experience. It emphasizes the importance of continuous learning, adaptation, and the willingness to adjust our understanding in the face of evolving threats, reducing our reliance on increasing expenditures for tools and technologies, a cycle that is now spiraling out of control rather than producing better results.

KEYWORDS: Systems Thinking | Cybersecurity | Information Security | DSRP | Cognition | Metacognition

Statement of Significance

This study pioneers the application of the DSRP-483 framework in cybersecurity, offering an evidence-based approach to enhance cognitive processes of practitioners. By leveraging systems thinking principles, it equips cybersecurity professionals with advanced tools to navigate complex challenges in their field. This research contributes to the evolving landscape of cybersecurity by providing a structured methodology for improving decision-making and problem-solving capabilities in an increasingly interconnected digital environment.

“The attackers' advantage lies in what you think you have (belief) and what you manage (reality). Instead, you must manage from reality, as that is the prepared Defenders Mindset.” – John Lambert ⁽¹⁾

Introduction

Systems thinking has long been touted as an approach to better understanding the complexity involved in defending digital businesses from an increasing number of attacks.

Previous research has identified several areas that have contributed to the failure of systems thinking to deliver on its promises including lack of empirical evidence, inconsistent or vague definitions, niche use cases, lack of construct validity and gaps between theory and practice, with the most significant divide being that none of the studies had proposed a theoretical basis for the cognitive patterns that result in systems thinking (2).

Imagine a cake that's universally praised as a culinary masterpiece. Chefs and food critics rave about its exquisite taste and texture, declaring it the pinnacle of baking. Yet, when asked for the recipe, they fumble. Some list ingredients without measurements, others describe vague techniques. No one can replicate it consistently. The cake remains a tantalizing mystery, its true composition unknown.

For too long, academics have been mesmerized by the allure of the systems thinking cake, neglecting the crucial recipe that gives rise to this cognitive delicacy. Their fixation on the end product, the systems, has overshadowed the essential ingredients and processes that constitute thinking itself. This myopic focus has led to a proliferation of discipline-specific applications and inconsistent definitions, akin to chefs arguing over the cake's appearance while ignoring the fundamental baking principles. To truly advance the field, we must shift our attention to the cognitive patterns that underpin all forms of thinking, including systems thinking. By examining the mental ingredients and methods that create this intellectual confection, this paper proposes a replicable, empirically grounded approach that transcends disciplinary boundaries and bridges the gap between theory and practice in the domain of cybersecurity. Practitioners can now have their cake and eat it too.

Current State of Cybersecurity

Since the humble launch of the internet in the late 20th century, the digital landscape has seen explosive growth. This expansion encompasses various aspects such as e-commerce, social media platforms, online education, and digital entertainment. The sheer volume of content available today is mind-boggling and continues to increase at an unprecedented rate. A recent survey conducted by Netcraft (3) showed 1,141,129,846 websites across 272,032,056 domains and 13,114,233 web-facing computers. With the incorporation of these technologies into our daily lives, the internet has grown beyond traditional computers and cell phones. The Internet of Things (IoT) provides seamless connectivity and automation, allowing us to control and monitor numerous elements of our homes, offices, and even our health. Furthermore, the 'Internet of Things', which includes smart gadgets, linked appliances, and wearable technology, has become a key component of the digital landscape, with projections estimating that the number of IoT devices utilised in 2025 would reach 64 billion (4).

This profound technological transformation that is reshaping our society in the 21st century is often characterized as “The Fourth Industrial Revolution”. A term introduced in 2016 and popularized by the founder and executive chairperson of the World Economic Forum who described it as the merging of new technologies like 3D printing, genetic engineering, quantum computing, the Internet of Things (IoT), and artificial intelligence (AI) (5).

This revolution is blurring the boundaries between the physical, digital, and biological worlds. It's driven by the exponential growth of digital technologies and is fundamentally different from previous industrial revolutions due to its rapid pace and wide-ranging impact across various sectors.

Organizations globally are pursuing the digitization of most private and public spheres of life, and they are becoming increasingly reliant on digital technologies to drive revenues and economic growth. GSMA reports that in 2022 mobile technologies and services alone generated \$5.2 Trillion of economic value globally (6).

While this transformation has opened up new avenues for ease of use and innovation in a variety of industries, including healthcare, transportation, and home automation, it has also revealed several challenges. As society becomes more interconnected and reliant on digital technologies, the vast amount of data generated and collected in this hyperconnected world creates a perfect storm of opportunities for cybercriminals.

Cost of Cyber Crime

Cybercrime is one of the biggest threats to the world economy, the national interests of individual states and business (7). For companies, the costs and losses connected with cybercrime are immense and the number of crimes and economic losses from cyberattacks is only projected to increase.

Cybercrime also poses a threat to the national security of governments across the world. The increased frequency of cyberattacks destabilizes international order and undermines the normal operation of international relations. For example, in 2017, the NotPetya ransomware attack targeted thousands of computers in over 150 countries, including government agencies and critical infrastructure (8). This attack disrupted healthcare systems, transportation networks, and public services, highlighting the vulnerability of nations to cyber threats and the need for enhanced cybersecurity measures.

While the cost of cybercrime globally is difficult to determine precisely, the World Economic Forum estimates the annual cost of cybercrime will likely increase by 15% every year until it hits \$10.5 trillion in 2025 (8). The increasing reliance on digital technologies and the growing sophistication of cyber threats highlight the need for robust cybersecurity measures and continuous efforts to mitigate the economic impact of cybercrime. These costs illustrate the significant impacts that cyberattacks can have on both financial and reputational aspects of businesses.

Cost of Cyber Security

Businesses have been compelled to invest large amounts in cybersecurity measures to combat the growth in cybercrime. This includes investments in advanced security solutions, hiring

specialized personnel, and conducting regular security audits to identify potential gaps in their security posture. Global end-user expenditure on information security is anticipated to reach \$212 billion in 2025, reflecting a 15.1% rise from 2024, as per a recent projection by Gartner, Inc (9). Global market research firm IDC projects that the worldwide security product market will maintain double-digit growth over the next five years, with total revenue expected to reach \$200 billion by 2028 (10).

If financial metrics are the yardstick by which success is measured, then it is anticipated that cybercriminals will continue to be successful for the foreseeable future.

Changing How We Think (Adapting to Reality)

If throwing more money, technology, and tools at the problem isn't changing the outcomes, it might be time to change how we think about cybersecurity. Instead of thinking like defenders, we should think like attackers, testing our mental models against reality rather than what our beliefs about reality are, with the expectation that reality will eventually align with our perspectives.

However, as past research has suggested (2), merely asking individuals to think differently is insufficient; rather, cybersecurity practitioners must be equipped with thinking tools that can be applied universally across domains and at all levels of the organisation, from practitioners to leaders. This is best addressed by first understanding how humans think and the underlying patterns of cognition.

Why HOW you think matters.

Cognition refers to the mental process of understanding and gaining knowledge (11). It comes from a Latin word that means "getting to know" or "becoming familiar with something". Cognition is essentially how we think, learn, and make meaning about the world around us.

Mental Models

Mental models are cognitive frameworks that individuals use to interpret and understand the world around them. These models play a crucial role in shaping our perceptions, decision-making processes, and interactions with our environment. They serve as internal representations of external reality, helping us make sense of complex information and navigate various situations in both personal and professional contexts.

The significance of mental models extends across multiple domains:

1. **Decision-making:** Mental models influence how we analyze situations and make choices. They provide a structure for processing information, evaluating options, and predicting outcomes. By refining our mental models, we can enhance our ability to make more informed and effective decisions.
2. **Problem-solving:** When faced with challenges, individuals draw upon their mental models to identify potential solutions. These cognitive frameworks help us recognize patterns, make connections between seemingly unrelated concepts, and approach

problems from different angles.

3. Learning and adaptation: Mental models are not static; they evolve as we gain new experiences and knowledge. This adaptability allows us to continuously update our understanding of the world and adjust our behaviors accordingly. The process of refining mental models is essential for personal growth and lifelong learning.
4. Communication and collaboration: Shared mental models within teams or organizations facilitate better communication and coordination. When individuals have aligned mental models, they can more easily understand each other's perspectives and work together effectively towards common goals.
5. Innovation and creativity: By consciously examining and challenging our existing mental models, we can foster innovative thinking. This process of questioning assumptions and exploring alternative viewpoints often leads to creative breakthroughs and novel solutions.
6. Risk assessment and management: In complex systems, such as financial markets or ecological environments, mental models help us understand interconnections and potential consequences of actions. This understanding is crucial for identifying and mitigating risks effectively.
7. Emotional intelligence: Mental models also play a role in how we interpret social cues and manage our emotions. By developing more sophisticated models of human behavior and emotional responses, we can enhance our empathy and interpersonal skills.

It's important to note that while mental models are invaluable tools for understanding and navigating the world, they can also lead to biases and limitations if not regularly examined and updated. The process of metacognition – thinking about our thinking – is crucial for recognizing the strengths and weaknesses of our mental models and refining them over time.

“Insights into our own thoughts, or metacognition, is key to high achievement in all domains” – Stephen Fleming ⁽¹²⁾

By actively developing and refining these models, individuals can enhance their problem-solving abilities, decision-making processes, and overall effectiveness in various aspects of life. The conscious cultivation of diverse and flexible mental models is a powerful tool for personal and professional growth, enabling us to navigate the complexities of our ever-changing world with greater insight and adaptability.

Cutting through the ‘Fog of More’

The point of information is to aid in decision making which implies that the quality of the information you have access to correlates to the quality of the decisions that you make, which subsequently influences the quality of actions taken and the resulting outcomes.

Cybersecurity practitioners face a multifaceted challenge in navigating the dynamic landscape of their internal organizational structures coupled with the external threat landscape. Internally, the workforce itself undergoes frequent changes, with new employees joining, existing staff transitioning roles, and the increasing prevalence of remote work arrangements. The continuous flux of internal systems, movement of data, coupled with the dynamic nature of personnel, creates a complex ecosystem that demands constant adaptation to the information that is coming from the environment.

Externally, the threat landscape presents an equally daunting challenge, characterized by its relentless evolution and the sheer volume of threat intelligence that must be processed. Cyber attackers constantly refine their tactics, techniques, and procedures (TTPs), leveraging emerging technologies and exploiting newly discovered vulnerabilities. The rise of state-sponsored cyber operations, the sophistication of organized cybercrime syndicates, and the emergence of hacktivism contribute to a complex and unpredictable threat environment.

“We attribute these failures primarily to the complexity of modern systems management, as well as a noisy and confusing environment of technology, marketplace claims, and oversight / regulation. Defenders are just overwhelmed.”
– Tony Sager ⁽¹³⁾

This highlights a pervasive misconception that simply accumulating more resources, be it system logs, alerts, tools, vendors, finances, or personnel, will inevitably lead to improved security outcomes. However, this belief is fundamentally flawed. The reality is that an abundance of information, without proper organization and utilization, can hinder effective cybersecurity practices.

Instead of clarity, it creates a fog that obscures critical insights and impedes decision-making. The true challenge lies not in acquiring more data, but in developing the cognitive skills to organize and leverage information more effectively. By focusing on improving their ability to synthesize and analyze the data they already possess, cybersecurity practitioners can significantly enhance their situational awareness and decision-making capabilities.

This shift in approach from accumulation to organization, is the key to improved security outcomes and crucial for cutting through the “fog of more” and establishing a more robust and effective cybersecurity posture.

Adapting to Reality

Mental models are formed through a dynamic process of organizing information. Their value is measured on how well they match reality, which is assessed by testing them in the real world and obtaining feedback in the form of information. The way we organise the information we receive from feedback determines whether we are adaptive or maladaptive to our environment.

This is illustrated in the System Thinking Loop or ST Loop as shown in Figure 1.

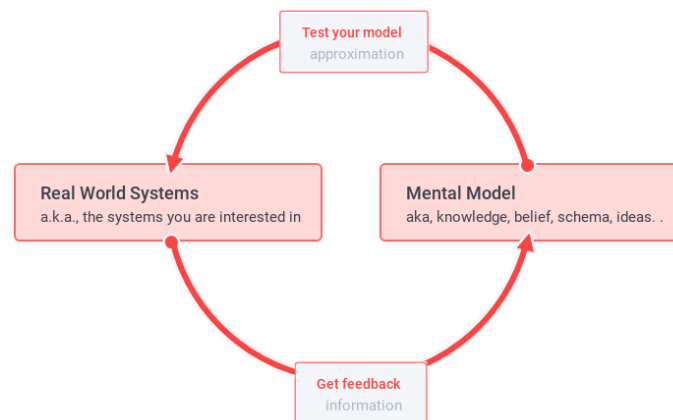


Figure 1- System Thinking Loop

Cybersecurity practitioners' adaptability and responsiveness to the environment is determined by their capacity to compare their current mental model to reality and modify it in light of new information. Failure to adapt their mental model in response to new information risks drifting even further from reality, with the potentially disastrous consequences of making judgements based on a nonexistent reality.

An example of this is known as confirmation bias, which is where the cybersecurity practitioner selectively accepts information that confirms their existing mental model regardless of its accuracy in relation to the current reality.

Closing the Gap with DSRP-483

This paper presents DSRP-483 Theory as a universal, evidenced based method for improving the cognitive capabilities of cybersecurity practitioners in response to the increasing complexity of their operational environments. DSRP-483 describes 4 Patterns of Organization, composed of 8 Elements, which are animated by 3 Dynamics as shown in Table 1 below.

4 Organizing Patterns	Equality Dynamic	4 Visible Elements	Co-implication Dynamic	4 Invisible Elements
Distinctions (D)	=	identity (<i>i</i>)	↔	other (<i>o</i>)
Systems (S)	=	part (<i>p</i>)	↔	whole (<i>w</i>)
Relationships (R)	=	action (<i>a</i>)	↔	reaction (<i>r</i>)
Perspectives (P)	=	view (<i>v</i>)	↔	Point (<i>p</i>)
* Simultaneity Dynamic				

Table 1- DSRP Structure and Dynamic

DSRP provides the cognitive tools for organising information in both the mind and nature so that mental models are more closely aligned with reality (14). With more empirical data than any other systems theory, its validity in both cognitive and natural contexts makes it an appropriate theory and practice for use in the field of cybersecurity, and research has shown that even using a limited number of DSRP-based techniques, known as cognitive moves, can result in considerable gains in thinking performance ranging from 280% to 500% (15-18,19).

Furthermore, validated edumetric assessments have been developed to evaluate the four organisational patterns that underpin systems thinking in individuals, providing a means for measuring improvements in their cognitive capabilities over time (20).

DSRP is ideal as it addresses deficiencies found in systems theories and methodologies that, despite demonstrating promise in specific scenarios, have not yielded universal application across the various disciplines within the cybersecurity domain (2).

Always, Everywhere, All at Once

The dynamism of DSRP means that each of the elements are interlinked, equally, always.

- a) Equality means that each of the four patterns and eight elements is needed every time. For example, we can't make a distinction without it being a perspective, in relation to other things, and part of a larger system.
- b) Co-implication means that if one element of a pattern exists then the other exists. There can't be an 'identity' without an 'other', or a 'part' without a 'whole'.
- c) Simultaneity means that any element is also all the other elements at the same time. Meaning a part is also an identity, an other, a whole, an action, a reaction, a point, and a view.

Most people's thinking patterns are dominated by the visible elements (i, p, a, v), and the invisible elements (o, w, r, p) are more likely to be disregarded or ignored, whether intentionally or unintentionally. Biases in thinking are prevalent within the broader context of Systems Thinking (21), and the inclination to favour one pattern or element over others increases the likelihood of overlooking critical knowledge regarding one's view of reality.

Highlighting Structure and Lowlighting Content

The concept of highlighting structure and lowlighting content is a crucial aspect of systems thinking (22) and involves temporarily setting aside specific details (lowlighting content) to focus on underlying patterns (highlighting structure). In the information-heavy world of cybersecurity, this skill is invaluable for helping practitioners cut through the 'fog of more'.

By lowlighting content, they can avoid getting bogged down in the minutiae of individual data points and instead focus on identifying broader patterns and relationships. This allows them to see connections between seemingly unrelated events that might otherwise go unnoticed.

Highlighting structure allows practitioners to organise the signal among the noise and construct mental models that are more closely related to the reality of their systems of interest.

Improving cognitive skills in cybersecurity practitioners through the application of DSRP has far-reaching implications, some of which are listed in Table 2 below.

Cognitive Skill	Application in Cybersecurity
Decision Making	the cognitive processes involved in evaluating risks and making informed choices to address security challenges and ethical dilemmas.
Situational Awareness	the cognitive ability to perceive, understand, and anticipate elements and events in the cyber environment for effective decision-making and response.
Risk Assessment	the cognitive process of identifying, analyzing, and prioritizing potential cybersecurity threats to inform decision-making and enhance security measures.
Threat Recognition	the cognitive ability to identify and analyze potential cyber threats through pattern recognition and understanding of unusual behaviors.
Learning and Adaptation	the cognitive process of acquiring knowledge and adjusting behaviors to improve awareness, response, and resilience against evolving cyber threats.
Problem Solving	the cognitive processes and skills used to identify and implement effective solutions to complex challenges in cybersecurity.
Cognitive Bias Management	strategies for recognizing and mitigating cognitive biases to improve decision-making in cybersecurity.
Pattern Recognition	the cognitive process of identifying patterns in data, essential for detecting malware, phishing attempts, and security vulnerabilities.
Incident Response	During a cyber incident, cognitive skills are crucial for quickly assessing the situation, determining the appropriate response, and executing a plan to mitigate damage.
Emotional Intelligence	a cognitive skill, that helps practitioners manage stress, communicate effectively, and maintain focus during crises.
Forecasting	the ability to forecast the choices and inclinations of attackers during live attack scenarios.

Table 2- Cognitive Benefits

Cognition, manifested through mental models and organized via the patterns of DSRP, is fundamental to modern cybersecurity practices. It enables practitioners to navigate complex challenges, make better informed decisions, and adapt to the emerging threat landscape, ultimately strengthening an organization's security posture.

Case Study: Threat Modelling

A threat model is an organized representation of all the information affecting a system's security. Threat modelling is the process of collecting, organizing, and analyzing all of this data.

In essence, it is a view of the application and its environment through the lens of security. In a threat modeling exercise for a large enterprise network, a cybersecurity practitioner can take the following steps to understand the approach.

1. Lowlighting content: To prevent being overwhelmed by the specifics of each device, application, or user in the network, the practitioner temporarily sets aside these

details.

2. Highlighting structure: Instead, they focus on identifying the different parts of the environment at a high level, emphasizing the relationships between different parts (e.g., DMZ, internal network, cloud services).
3. Applying DSRP:
 - a. Distinctions: Who is a potential threat actor and who is not? (e.g., nation-state actors, cybercriminals, insiders).
 - b. Systems: What are the parts of the environment, and what is the environment a part of?
 - c. Relationships: What is the relationship between the various parts? Map out potential attack paths and data flows.
 - d. Perspectives: From which points of view should we look at the system? Consider the viewpoints of different stakeholders (e.g., IT administrators, end-users, compliance officers).
4. Iterative refinement: As the practitioner gains insights from this structural view, they can begin to make “structural predictions” and then selectively "highlight" specific content areas that require deeper investigation with DSRP.
5. Comprehensive threat model: By alternating between structure and content, the practitioner develops a more robust mental model that captures both the big picture and critical details.

This approach allows the practitioner to create a more effective and adaptable threat model, avoiding the common pitfall of getting lost in technical details while missing broader systemic gaps in their thinking.

Patterns with Benefits

Training cybersecurity practitioners to apply DSRP through cognitive moves can yield significant advantages. Empirical research has demonstrated measurable enhancement in individuals' capacity for complex thinking and problem solving in everyday situations (14).

Pattern	Cognitive Move	Improvement	Outperform x % population
Distinction	What is x? and What is not x?	5.51x	50%
Systems	What are the parts of x? and What is x a part of?	2.66x	60%
Relationship	What is the relationship between x and y?	7.55x	85%
Perspective	From which points of view should we look at x?	4.47x	95%

Table 3- Performance improvements

By learning the skills of highlighting structure and lowlighting content using DSRP, cybersecurity practitioners can not only respond more effectively to complex security challenges but also accelerate their professional development and potentially "leapfrog" their peers (22).

Case Study: Vulnerability Management

A cybersecurity practitioner's initial mental model of vulnerability management involves a structured approach to identifying, assessing, and patching known vulnerabilities in systems and software. This model prioritizes regular scanning, risk assessment based on CVSS¹ scores, and scheduled patching cycles.

As part of the monthly vulnerability notifications information is received by the practitioner that a vulnerability released 3 months ago with a medium CVSS rating of 5 is now being actively exploited by cyber criminals in the wild and affects a widely used enterprise software. Already overwhelmed by the hundreds of vulnerabilities they receive each month, the practitioner's mental model focuses on the most recent round of vulnerabilities with higher scores, and they adhere to the standard operating procedures outlined below.

1. Conduct the next scheduled vulnerability scan to identify systems affected by the latest high rated vulnerabilities.
2. Perform a risk assessment using the CVSS scoring system to evaluate the severity of the vulnerability.
3. Prioritize the high rated vulnerabilities based on the risk assessment results.
4. Obtain the necessary patches or updates for the high rated vulnerability through the organization's regular software update channels.
5. Deploy the patches for the high rated vulnerability according to the organization's established patching cycle.

These actions show a more conventional approach to vulnerability management, in which the practitioner does not distinguish between the vulnerability's CVSS rating and the fact that it is being exploited in the wild. Instead, they continue to use their established procedures despite new information. Whilst this approach emphasizes consistency and adherence to existing procedures, it does not align to a reality where attackers may use a different mental model when looking at the same reality.

An attacker might view the new information differently than a defender:

1. Exploitation potential: While a defender prioritizes the vulnerability's CVSS score, an attacker makes a different distinction by focusing on how easily it can be exploited. They may prefer a lower rated vulnerability with readily available exploit code over a

¹ CVSS (Common Vulnerability Scoring System) is a standardized method for assessing the severity of computer system security vulnerabilities. It uses a scale of 0 to 10, with higher scores indicating greater severity. CVSS is intended to help organizations prioritize and manage their cybersecurity efforts.

higher one that increases their cost to attack.

2. **Target selection:** Attackers consider the vulnerability's prevalence across potential targets. Understanding the relationship between a vulnerability and the potential targets means they might prioritize a flaw affecting a higher number of possible target organizations over a more severe one limited to higher value targets.
3. **Detection evasion:** Attackers evaluate how long they can exploit the vulnerability before patches are widely deployed or detection mechanisms are updated. They may favor lower rated flaws that remain unpatched for extended periods.
4. **Chaining opportunities:** Attackers assess how the vulnerability can be combined with other known weaknesses to create more sophisticated attack chains, potentially increasing their impact or stealth.
5. **ROI consideration:** Unlike defenders, who prioritize risk mitigation, attackers weigh the effort required to exploit the vulnerability against the potential financial gain from data exfiltration or the sale of system compromise opportunities to other criminals.

This example demonstrates that the same information organized differently can result in different decisions, different actions, and different outcomes. It highlights the importance of defenders considering the attacker's mental models when prioritizing and addressing potential threats in their environments. The application of DSRP in organizing information related to a vulnerability not only improves decision-making but also leads to more effective actions. It enables the cybersecurity practitioner to develop a comprehensive, well-informed response strategy that addresses immediate risks while considering long-term implications for the organization's security posture.

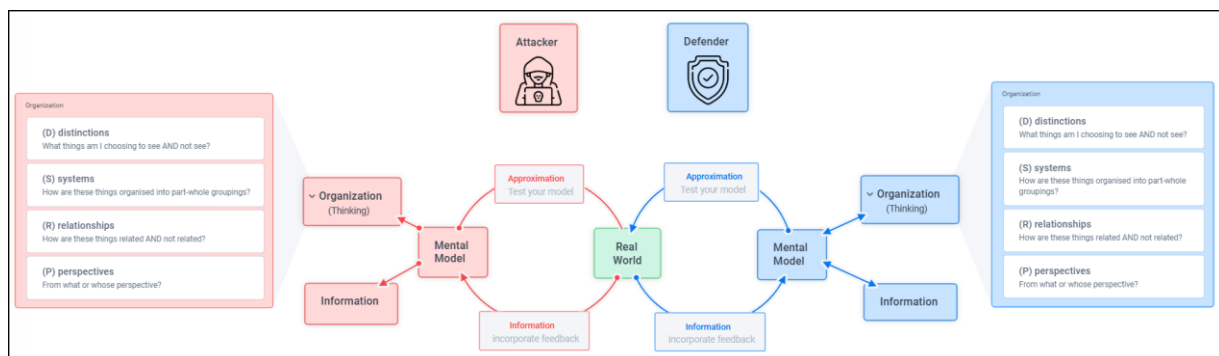


Figure 2- Systems Thinking for Cyber (ST4C) Loop

When defenders fail to consider an attacker's mental model, and that mental model more closely approximates reality, the attackers gain a competitive advantage. This discrepancy between mental models and reality allows attackers to exploit vulnerabilities and flaws that defenders may overlook, ignore or underestimate, increasing the likelihood of a successful cyberattack.

The use of DSRP in cognitive processes is analogous to the financial notion of return on investment (ROI), in which the benefit (or return) of an investment is divided by its cost. The outcome is expressed as a percentage or ratio (23). This comparison can be strengthened by

using the systems thinking formula $M = I \times O$, in which your Mental Model (M) is a product of Information (I) and Organisation (O). Both serve as measures of efficiency and effectiveness in their respective fields. Just as ROI calculates the profitability of an investment in relation to its cost, DSRP and the $M = I \times O$ model shown in Figure 3 provides a method for increasing "Return on Thinking" (ROT) by estimating the likelihood that a mental model fits reality (14). By aligning your mental model more closely with reality, you will be able to make better structural predictions about the results of your choices and actions. This means that whoever uses DSRP most effectively in any given situation will have a higher ROT.

This scenario can also be observed in predator-prey relationships in nature, where the ability to effectively use information provides a survival advantage. Consider the example of the Arctic fox and the lemming:

Arctic foxes have evolved to detect the faint sounds and subtle movements of lemmings beneath the snow. They've developed a keen ability to interpret these signals and use this information to their advantage when hunting. The fox's mental model includes an understanding of lemming behavior, habitat preferences, and movement patterns.

Lemmings, on the other hand, have a different mental model focused on finding food and avoiding predators. If lemmings fail to update their mental model to account for the fox's hunting strategies, they become more vulnerable to predation.

In this example, the Arctic fox's ability to gather and interpret information about its prey gives it a competitive advantage. Foxes that are better at using this information are more likely to survive and reproduce, passing on their enhanced information-processing abilities to future generations.

Similarly, in cybersecurity, attackers who can better interpret and use information about vulnerabilities and defender behaviors have a higher chance of successful attacks. Defenders who fail to adopt a similar mental model – understanding how attackers think and operate – are at a disadvantage, much like lemmings that haven't adapted to the fox's hunting strategies.

This natural world analogy underscores the importance of defenders continually updating their mental models to match those of potential attackers. By doing so, they can better anticipate threats, identify vulnerabilities from an attacker's perspective, and develop more effective defense strategies, ultimately improving their chances of "survival" in the digital ecosystem.

Conclusion

Systems thinking involves the development of mental models that accurately reflect real-world systems. This process includes structuring available information, testing it through feedback, and iteratively refining the model to enhance its alignment with reality. Feedback from the real world is essential; however, the way we organise this information is what constitutes a mental model.

The process of comparing our mental model to reality, known as the systems thinking loop or ST Loop, does not guarantee that our model is an accurate representation of reality. This is

especially true if the feedback we receive is false or incorrect. To avoid the "garbage in, garbage out" principle, it is crucial to have a procedure in place to evaluate the reliability and correctness of the feedback we receive.

DSRP-483 theory offers a scientifically proven method for improving how practitioners think about cybersecurity. By examining the distinctions, systems, relationships, and perspectives within their organizational context, practitioners can gain a deeper understanding of the complexities involved in protecting digital infrastructure. This approach enables them to more effectively address the challenges of cybersecurity in their organizations.

The growing success of threat actors in today's ever expanding digital world is evidence that their mental models have given them a competitive advantage when targeting organizations. Therefore, it becomes crucial that in order to defend oneself against these attackers we must see the world through their mental models and understand them more deeply in order to be able to adapt to their tactics to provide the best chance of successfully defending. DSRP provides practitioners with the tools to effectively organize information to achieve that outcome.

The rising costs of cybercrime, coupled with the expected exponential investment in cybersecurity solutions, should act as a wake-up call for a paradigm shift in our approach. We can stay on our current path, hoping that increased spending will eventually produce the desired results, or we can look beyond the fog of more and invest in equipping the next generation of cybersecurity practitioners with advanced thinking skills, effectively tipping the scales back in favor of the defenders.

References

1. J. Lambert, Defender's Mindset. Medium (2022). Available at: <https://medium.com/@johnlatwc/defenders-mindset-319854d10aaa> [Accessed 10 August 2024].
2. M. Collins, Systems Thinking in Cybersecurity; Ending with the Beginning in Mind. *Journal of Systems Thinking Preprints* (2024). <https://doi.org/10.54120/jost.pr000038.v1>.
3. November 2024 Web Server Survey. *Netcraft* (2024). Available at: <https://www.netcraft.com/blog/november-2024-web-server-survey/> [Accessed 13 December 2024].
4. A. Shamman, H. Alsadi, S. Ariffin, Z. Rasool, H. Ghani, Cost-effective Resource and Task Scheduling In Fog Nodes. *IJECS* 27, 466 (2022).
5. K. Schwab, *The Fourth Industrial Revolution* (Penguin UK, 2017).
6. GSMA, "The Mobile Economy 2023" (2023).
7. Ribeiro, Five Eyes' Critical 5 nations focus on adapting to evolving cyber threats to boost critical infrastructure security, resilience. *Industrial Cyber* (2024). Available at: <https://industrialcyber.co/critical-infrastructure/five-eyes-critical-5-nations-focus-on-adapting-to-evolving-cyber-threats-to-boost-critical-infrastructure-security-resilience/>. [Accessed 01 November 2024]
8. Significant Cyber Incidents | CSIS. Available at: <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>. [Accessed 5 December 2024]
9. Gartner forecasts global information security spending to grow 15% in 2025. *www.gartner.com* (2024). Available at: <https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025> [Accessed 7 December 2024].
10. Double-Digit Revenue Growth for Security Products in 2023 is Forecast to Continue Through 2028, According to IDC. *IDC: The Premier Global Market Intelligence Company*. Available at: https://www.idc.com/getdoc.jsp?containerId=prUS52392924&_gl=1*1bc7h8g*_up*MQ..*_ga*ODM4NDI3MTYzLjE3MzM1Mjk0MDQ.*_ga_Y7CNRMFF6J*MTczMzUyOTQwNC4xLjAuMTczMzUyOTQwNC4wLjAuMA..*_ga_541ENG1F9X*MTczMzUyOTQwNC4xLjAuMTczMzUyOTQwNC4wLjAuMA.
11. cognition | Etymology of cognition by etymonline. *Etymonline*. Available at: <https://www.etymonline.com/word/cognition>. [Accessed 28 November 2024]
12. S. M. Fleming, Metacognition Is the Forgotten Secret to Success. *Scientific American* (2024). [Accessed 28 November 2024]

13. Blog | Cyber Hygiene: It's Not Just Recommended; It's Essential. *CIS* (2021). Available at: <https://www.cisecurity.org/insights/blog/cyber-hygiene-its-not-just-recommended-its-essential>. [Accessed 5 December 2024]
14. D. Cabrera, A Mathematical Theory of Organization. *Journal of Systems Thinking* (2024). <https://doi.org/10.54120/jost.00000100>.
15. D. Cabrera, L. Cabrera, E. Cabrera, Distinctions Organize Information in Mind and Nature: Empirical Findings of Identity–Other Distinctions (D) in Cognitive and Material Complexity. *Systems* **10**, 41 (2022).
16. D. Cabrera, L. Cabrera, E. Cabrera, Systems Organize Information in Mind and Nature: Empirical Findings of Part-Whole Systems (S) in Cognitive and Material Complexity. *Systems* **10**, 44 (2022).
17. D. Cabrera, L. Cabrera, E. Cabrera, Relationships Organize Information in Mind and Nature: Empirical Findings of Action–Reaction Relationships (R) in Cognitive and Material Complexity. *Systems* **10**, 71 (2022).
18. D. Cabrera, L. Cabrera, E. Cabrera, Perspectives Organize Information in Mind and Nature: Empirical Findings of Point-View Perspective (P) in Cognitive and Material Complexity. *Systems* **10**, 52 (2022).
19. D. Cabrera, L. Cabrera, E. Cabrera, The “Fish Tank” Experiments: Metacognitive Awareness of Distinctions, Systems, Relationships, and Perspectives (DSRP) Significantly Increases Cognitive Complexity. *Systems* **10**, 29 (2022).
20. L. Cabrera, J. Sokolow, D. Cabrera, Developing and Validating a Measurement of Systems Thinking. *Journal of Systems Thinking* **3** (2023).
21. G. Di Marco, D. Cabrera, Common Biases in Systems Thinking. *Journal of Systems Thinking* (2024). <https://doi.org/10.54120/jost.pr000037.v1>.
22. D. Cabrera, L. Cabrera, H. Gibson, Leapfrog Leaders. *Journal of Systems Thinking* **3** (2023).
23. Beattie, ROI: Return on Investment Meaning and Calculation Formulas. *Investopedia* (2024). Available at: <https://www.investopedia.com/articles/basics/10/guide-to-calculating-roi.asp>. [Accessed 7 December 2024]