Knowledge and Skills Needed to Craft Successful Cybersecurity Strategies

Mazaher Kianpour[0000−0003−2804−4630]

Department of Information Security and Communication Technology,
Norwegian Universtiy of Science and Technology, Norway
mazaher.kianpour@ntnu.no

Abstract. Daily advancing technologies and next-generation networks are creating entirely different digital environments for people, organizations, and governments within the next several years. Because cybersecurity provision in such environments involves many actors and must overcome many evolving threats and challenges, strategies must be responsive and multi-pronged. Development and execution of sufficiently savvy strategies to face the complex problems in this context necessitate identification of all the actors and operations that affect, directly or indirectly, on the cybersecurity of the digital ecosystems. In this study, we seek to provoke thinking about how actors and stakeholders could get better at crafting successful cybersecurity strategies, and identify and integrate specific types of skills required to formulation these strategies taking into account where decisions are actually made. This work provides an insight into cybersecurity education, calibrating and differentiating knowledge and skills to make the right demands on the right actors who have the authority and responsiveness to introduce change from multiple entry points. This enables practitioners to adopt more hands-on approaches that can be helpful to improve transparency, accountability and collaboration across levels of a socio-technical system.

Keywords: cybersecurity strategy · cybersecurity value chain · cybersecurity education · socio-technical system · cognitive-driven strategizing

1 Introduction

A revolution has begun in cybersecurity education. The world is constantly changing and is being affected by digital technologies. Certain strategies are emerging to cope with increasing challenges and embrace the transformations that lie ahead. On the face of it, cybersecurity education appears to be a very different, challenging issue that plenty of new scenarios, trends and organizations are emanating everywhere to impact this business. Moreover, the core idea of the globally interconnected societies is producing a dramatic change in the way people, organizations and governments interact and create value. The result is expanding the threat surface, uncovering gaps and slipping into the hyperconnected landscape the world is constructing [8].

A survey by Microsoft shows that cyber investment strategies focus on prevention, not resilience [26]. This suggests that many organizations continue to believe that they can eliminate or manage their cyber risks primarily through technology, rather that through a comprehensive range of planning, transfer, and response measures. Cybersecurity is full of misleading platitudes that seem obvious in the initial stages, however, more thoughtful consideration shows they are misinformed, ineffectual, or counterproductive [29]. Consequently, organizations cannot protect their assets in today's open socio-technical systems, overwhelmed by ever-increasing number of new cyber threats, without ensuring that each individual understands their roles and responsibilities and is adequately aware, trained and educated to perform them.

We argue that cybersecurity falls under Process Philosophy [31], as it is based on the premise that is dynamic and this should be primary focus of any comprehensive analytical and theoretical account of reality and our place within it. Hence, strategies formulated in cybersecurity discourse should be responsive and multi-pronged. The former focuses on flexible plans of actions that are developed and adapted in response to the changes and dynamics existing in the socio-technical systems. The latter focuses on the strategies that are developed by thoughtfully considering the interconnected elements, methods and actors in these systems from several points of view or directions. Kowalski acknowledges the multiparadigmatic view of cybersecurity and suggests that cybersecurity provision in open socio-technical systems requires a holistic approach that inspects both social and technical aspects of the system [19]. This agenda had been followed by both academia and industries in last two decades, however, it should advance toward the knowledge processes and cognitive aspects of the strategy tools in use. Accordingly, as Belmondo and Roussel discuss in [11], these tools would enable people to analyze and generate new knowledge, which directs them to develop their understanding and wisdom.

Following this introduction, we show how the cognitive and practical approaches are linked by the notion of cybersecurity strategizing. Therefore, Section 2 discusses the cognitive-driven process of developing responsive strategies. To develop multi-pronged strategies we present a value chain model in Section 3 to emphasis on the primary and supportive operations of cybersecurity provision considering the actors operating in this domain. In Section 4, we detail the knowledge and skills required to formulation of successful strategies that can expand strategy developers' thinking and lead to effective changes in their environments. Finally, this paper is concluded in Section 5 and offers suggestions for future studies.

2 Cognitive-driven process of cybersecurity strategizing

Formulation and implementation of strategies have long been a topic of debate. Leonardi discussed that the formulation and implementation of a strategy should not be split into two different isolated steps [22]. He also adds that to materialize a strategy is to focus on the materiality through which the strategy is

enacted. The increasing trend of employing cognitive technologies (e.g. Artificial Intelligence (AI), deep learning, etc.) shows that organizations need to rethink their approach of strategy formulation and implementation in the cybersecurity domain, as one of the most important domains in the digital transformation. Broadly speaking, cognitive technologies use data, information and knowledge to accomplish specific tasks. Hence, these capabilities should not be ignored in materializing the strategies. Figure 1 depicts a cognitive-driven process starting from intuiting to institutionalizing a strategy. We describe the process in a sequential way, although there are necessarily many feedback and feedforward among the steps. In the following discussion, we develop each of the steps in greater details.

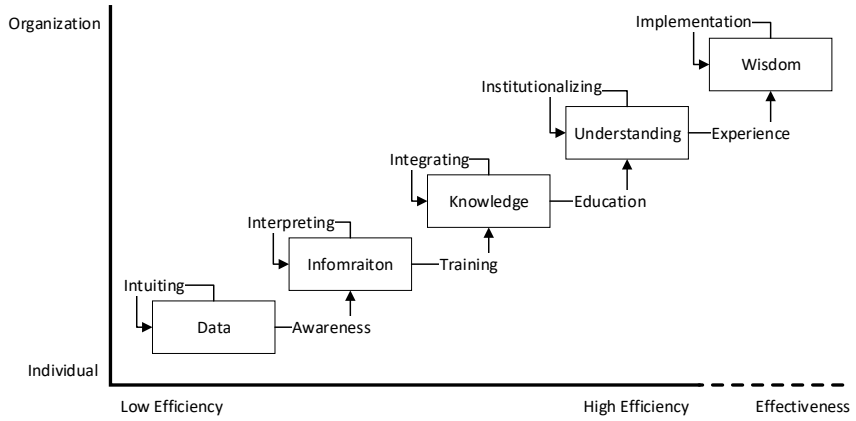

Fig. 1. Cognitive-driven process of strategizing

Today, we are overwhelmed by data. A data-driven intuition is a direct perception of truth or fact independent of any reasoning process. There are numerous similarities, differences, patterns, and possibilities in the data produced everyday. The intuiting is a process of pattern recognition and perception. Fundamentally, strategy all is about choice and inherently complex. The dense interdependencies among the choices makes the imitating winning strategies a failed strategy. The ability to make novel connections and to discern possibilities by observing situations and patterns is the key to intuiting.

Data-driven intuitions cannot be judged right or wrong as they are based on some possibilities and patterns. Therefore, in the next step, interpreting, we try to develop cognitive maps about the various domains involved in cybersecurity. The precision of interpretive process depends on how useful information is extracted from the data. The transition between data and useful information occurs through awareness. Cybersecurity awareness programs are intended to allow all individuals to recognize and retain cybersecurity concerns based on the collected data. These programs should be designed with the objective of incorporating new experiences into individuals' existing behavior pattern. Ac-

cordingly, they interpret situations based on their established cognitive maps. Some of these situations might be equivocal and have multiple, and often conflicting, interpretations. Therefore, we need to obtain the next level of cognition (i.e. knowledge) and resolve the issues through a group interpretive process.

As Underwood stated in [34], the links between information, knowledge and understanding is more complex than generally assumed. Ackoff stated that information is contained in descriptions, answers to questions that begin with such words as who, what, when, where, and how many. Knowledge is conveyed by instructions, answers to how-to questions. Understanding is conveyed by explanations, answers to why questions [9]. In the context of cybersecurity, training is the key enabler of gaining knowledge, skills, and abilities (KSA) applicable to protect assets. To formulate the coherent, collective strategies (i.e. strategies that enable organization to manage their interdependencies and create a partially endogenous social environment), the gained knowledge should be integrated through the communication among the actors and sharing practices. We discuss the actors and cybersecurity functions in Section 3. It should be noted that in this step, the distinctive feature is sharing. This ranges from data related to a vulnerability to cognitive map of managers and decision makers in different institutions. Integrating entails the development of shared knowledge and the coordinated actions taken by members of working group.

This integration of all the cybersecurity knowledge into a common body of understanding forms multidisciplinary concepts, issues and principles including politics, sociology, economic, technology and law. The number of these principles shows that formulation and implementation of cybersecurity strategies are too complex to successfully accomplished. As a result, education, due to its exploratory nature, provides the cybersecurity practitioners with a comprehensive understanding of the required fields for taking responsibility in an ever-changing environment. The institutionalization is a means for institutions to leverage these understandings and structure the system and processes to implement the formulated strategies. The favorable outcomes of this step are coherent actions of the individuals and institutions and regulated day-to-day routines by exploiting the current understandings.

As Ackoff argued, information, knowledge and understanding enables the practitioners to increase efficiency, not effectiveness. The efficiency of a behavior or an action is measured relative to an objective and the amount of resources required to achieve it. Whereas, the value of the objective is not relevant in determining efficiency, effectiveness is the efficiency for a values outcome. We can distinguish efficiency and effectiveness by two terms of tactical thinking (i.e. doing things right) and strategical thinking (i.e. doing the right things), respectively. Wisdom–thinking and acting using knowledge, experience, understanding, and insight–is the ability to increase effectiveness. A recent study by Targowski shows that wisdom can be acquired through experience [25]. Experiences reflect the complexity of actual and real world scenarios rather than abstraction taught in classrooms and laboratories. As this process evolves, richer understanding of the domain is developed and new integrated approaches to solving problems and

managing situations are created. Experiences themselves become the repository of wisdom and form a collective mind. The Strategies are effective when they are implemented across the environment and are executed by people. The greater wisdom about strategies, the better ability to manage the changes and situation effectively.

3 Cybersecurity Functions: The Value Chain Model

To effectively enhance the cybersecurity on which our digital ecosystems rely, it is important to understand the functions behind the cybersecurity provision and recognize the operations and activities associated with cybersecurity. The value chain model, developed by Michael Porter, is a powerful approach to understanding the value-added procedures embedded within an actor. This approach views an actor as a system, made up of subsystems each with inputs, transformation processes, and outputs, along with support activities. From a value chain perspective, we can identify activities that add value for cybersecurity, as presented in Figure 2. These value-added functions include any activity in the digital ecosystem that helps defenders increase the efficiency and effectiveness of the cybersecurity operations. Straightforwardly, the primary function that directly involve the cybersecurity provision are valuable for the defenders. The support activities, which are often overlooked, are also critical in the sustainability of cybersecurity as an essential property of the system.

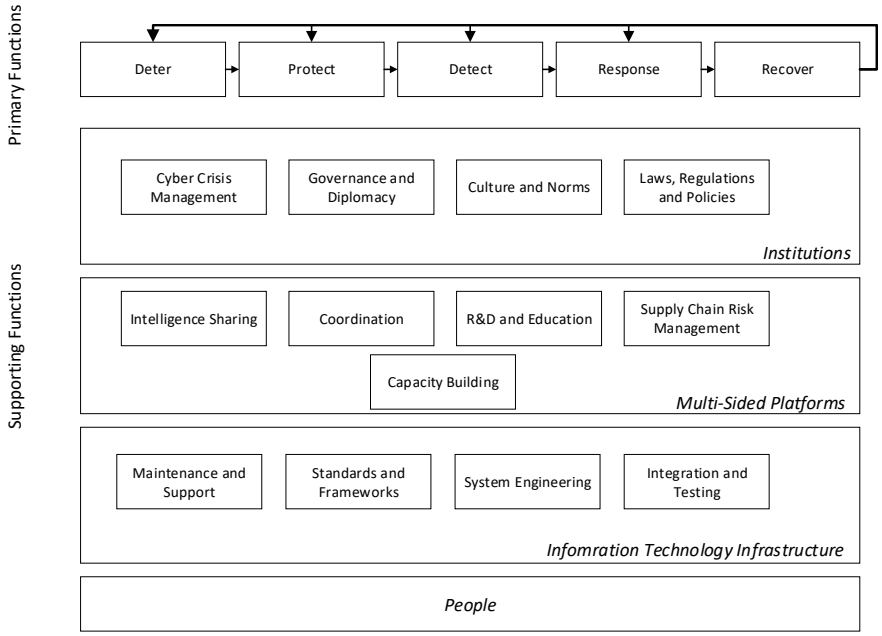

Fig. 2. Cybersecurity Value Chain Model

3.1 Primary Functions

In 2004, Kowalski proposed the concept of Security Continuum [20]. Then, he used a linear value chain to study the security spending mental models of different organizations in terms of the main security access control categories: Deter, Protect, Detect, Respond and Recover. The model further developed by The National Institute of Standards and Technology (NIST) as the Cybersecurity Framework (CSF) to organize the basic cybersecurity activities at their highest level [2]. This helps practitioners manage cybersecurity risks by organizing information, enabling risk management decisions, addressing threats, and learning from experience.

Deter. Deny adversaries and malicious users access to the information and other resources required to conduct an attack and dissuade them from conducting the attack through emphasis of the likelihood of failure and conviction. Defenders also can project an environment that makes an attack sufficiently difficult or too unachievable to progress.

Protect. Safeguard systems, networks and programs from malicious activities to access, change, or destroy sensitive information and interrupting normal business processes.

Detect. Identify the attack behaviours at every stage of the attack (i.e. planning, reconnaissance, deployment, etc.) and monitor for the loss of sensitive information or assets. Defenders also should initiate an appropriate response to a threat or attack as early in the attack as possible.

Response. Determine what internal and external response is required to the range of threats that the organization faces and ensure security measures are in place to initiate the response. Defenders also should carry out appropriate exercises, internally and externally, including communicating with other organizations and stakeholders.

Recover. Develop and implement the appropriate activities to conduct business recovery processes and reducing the impact of cyber-attacks. The aim of these activities is to sustain an acceptable level of performance during the cyber crisis management.

3.2 Support Activities

To supplement the primary activities outlined above, support activities are emerging in the digital ecosystem to provide cybersecurity at different levels of a socio-technical system efficiently and effectively: gaining greater benefits with less cost. To capture the complex relations within a system and the way in which the actors affect and are affected by another, we propose to classify the function into three groups: Institutions, Multiple-sided Platforms and Information Technology Infrastructure.

Institutions are established patterns of norms and interactions designed to meet societal goals [27]. Institutions are systems or subsystems within the society involving rather stable traditions, social organizations, and statuses, as well as norms developed to solve problems confronting the society. Such problems include the creation and reaffirmation of the values maintaining the system, protection of assets (e.g. people, data, networks, etc.), the definition of relationships, obligations and regulations in the system, and the coordination of the system. The complex interactions, relationships, and behavior that meet these needs in the context of cybersecurity are referred to as the major institutions of society: Crisis Management, Governance and Diplomacy, Laws, Regulations and Policies, and Culture and Norms. While we would expect to find these institutions in each society, their form might vary between societies.

- **Cyber Crisis Management.** Effective cyber crisis preparation goes beyond cyber incident response to address the entire crisis management life cycle of *readiness*, *response*, and *recovery*. Readiness involves not only 24/7 monitoring but also preparing team members to deal with an incident or crisis. Vigorous, coordinated responses to incidents limit damage and losses. Post-event recovery focuses on returning to normal operations, assessing the causes, and disseminating lessons learned [4].
- **Governance and Diplomacy.** According to Organization for Economic Cooperation and Development (OECD), governance is defined as the procedures and processes according to which an organization is directed and controlled [3]. Cyber governance, is a largely multilateral activity and is referred to as the process by which a number of state and non-state actors interact to manage the distribution of rights and responsibilities among the different participants in the organizations and lays down the rules and procedures for decision making. Cyber diplomacy also focuses on how diplomacy is adapting to the new global information order, and norms and standards for cyber behavior is promoted in the society. Both cyber governance and diplomacy aim for promoting confidence building measures between nations in cyberspace [30].
- **Laws, Regulations and Policies.** It has been recognized that technology can not fully protect assets in organizations. Hence, we require a set of laws, regulations and policies that would aid to protect assets, physical or digital, tangible or intangible. The cybersecurity laws, regulations and policies should be translated into specific, measurable goals to direct all decision makers to build a secure environment. They should offer guidance about the acceptable behavior and resource allocation in different situations. In 2017, a comprehensive guide for policy advisors and legal experts on how existing International Law applies to cyber operations drafted by NATO Cooperative Cyber Defence Centre of Excellence [6]. The United Nations Group of Governmental Experts also is one of the active working groups on cybersecurity international laws and policies.
- **Culture and Norms.** European Union Agency for Network and Information Security (ENISA) defines cybersecurity culture as the beliefs, knowl-

edge, perceptions, norms and values of people regarding cybersecurity and how they manifest themselves in people's behavior with information technologies [5]. Cybersecurity culture is needed at different levels [35]. Moreover, norms are collective expectations for the proper behavior of actors with a given identity and development of norms requires a shared belief about proper behavior for actors in a society.

Multi-Sided Platforms enable direct interactions between two or more distinct user groups, in which all user groups are affiliated with the multi-sided platforms (MSP) [28]. The MSP is related to the concept of value networks (i.e. a business mediation between members of a society), and the dependencies and network effects within user groups and between user groups make the dynamics of an MSP complex. In social dynamics, MSPs have to secure critical mass in a variety of contexts, including group dynamics, politics and technology, to create value. They are usually situated within broader ecosystems of organizations, governments, regulation, and other institutions [13]. They need to make sure that they can play well with any actor and make any required changes in the environment to do so.

- **Intelligence Sharing.** Cybersecurity intelligence is any processed information about incident data, cyber threats, cyber risks, security controls, coordinated defensive responses, good practices, and operational and tactical experiences. Intelligence sharing has its main focus on prevention, response and recovery. Moreover, these activities are mainly of operational and tactical in nature and build upon trust and value among the actors at different levels. It should be noted that intelligence sharing and information provisioning are different. While the latter concerns the situations that an actor is required by law to provide intelligence to the other actors, intelligence sharing is the mutual value adding exchange of information on cybersecurity with keeping the balance between transparency and secrecy.
- **Coordination.** The management of interdependent relationships that necessitates the exchange of information and cross-functional operations in order to align actors' pursuing similar goals and targets is known as coordination. Conflict of interests is a major challenge in coordination in the context of cybersecurity [33]. Duncan Snidal argues that a coordination problem arises when actors have a strong desire to coordinate but some differences over exactly where to coordinate [24].
- **R&D and Education.** Cybersecurity, at any level, will fail when there is an inappropriate level of cybersecurity awareness and education. Actors require developing strategic and operational programs to achieve an acceptable level of cybersecuriy awareness considering the ever-changing threat landscape. These programs need to span a wide range of actors and topics. This is notwithstanding the fact that Research and Development (R&D) on the field of cybersecurity is an integral part of the functions mentioned at the levels of *Institutions* and *IT Infrastructure*. R&D can include in-depth research into cyber attacks and methodologies that can be used in both defensive and offensive operations.

- **Supply Chain Management.** Since 2000s, information technology solutions supported business operations and changed their mechanisms of information sharing, process controlling, connection, etc. Although these changes in supply chains facilitated their connectivity and communication, it also increased the vulnerability exposure of the systems. Therefore, it is recognized that creating a secure and resilient environment for the actors requires a highly efficient and responsive supply chain which is capable of maintaining its operational performance when faced with cyber risks [15].
- **Capacity Building.** Broadly speaking, capacity building is the cybersecurity domains is aimed at developing the cross-functional and accountable institutions to effectively respond to cyber-crimes and to enhance cyber resilience of actors. This is an integral component of operations that can foster creating a secure, open and interoperable environment for the all actors. The European Union Institute for Security Studies (EUISS) established a task force aimed at promoting a strategic approach and understanding of cyber capacity building among EU stakeholders. This task force is composed of five experts in the field of cybersecurity, human rights, intelligence, internet governance, cybercrime, resilience and development [1]. This shows the necessity of adopting a holistic approach to face with the challenges in this domain.

Information Technology Infrastructure is broadly defined as all of the hardware, software, networks, facilities, etc., that are required to develop, test, deliver, monitor, control or support IT services. The term IT infrastructure includes all of the Information Technology but not the associated People, Processes and documentation [10]. IT infrastructures and operations are affected by the speed at which the globe is connected.

- **Maintenance and Support.** The pace of technology adoption is speeding up and the cybersecurity landscape is becoming more complex. Consequently, consistent and continuous maintenance and support of the product and services is not only required by the businesses to ensure they are secure against the vulnerabilities, but it is also a requirement of many regulatory agencies and compliance conditions.
- **Standards and Frameworks.** Adoption of standards and frameworks provides structure to the institutions and help them to manage the environment and other actors' expectations. Basically, cybersecurity frameworks and standards guides the actors to design the best possible products and services for businesses and improve the effectiveness of them. In the context of cybersecurity, Computer Emergency Response Teams (CERT) adopt different standards, both de facto and de jure, and frameworks in order to attain a certain level of proficiency in executing specific functions such as information sharing, communication, and situation management.
- **System Engineering.** As we discussed earlier, cybersecurity provision requires a collection of interdependent, autonomous systems that interoperate together to achieve additional desired capabilities and goals. Applying system engineering helps to understand the characteristics of these systems and

their implications in an environment. It is important to understand what constitutes a system of systems and how the context of cybersecurity affects which system engineering methods, tools, and techniques should be applied in order to maintain the effectiveness and security of the environment.
- **Integration and Testing.** Today, various services, and physical and digital components of organizations are integrating to facilitate the processes and accelerating revenue growth. These innovative solutions should be controlled and tested precisely as the smallest mistake and negligence can cause serious defects that exacerbate the cyber risks.

People execute and bring about the actual changes, no matter how smart the strategy and how well articulated the plan is [7, 18]. As Harold Leavitt argues, in order to implement real changes as a result of executing the strategies, you should never ignore people [21]. Many change efforts do not sustain themselves because they only focus on technology and processes. It is crucial to get people to understand what is expected of them and how they can be successful. From a sociological perspective, interactions among people affects their behavior, relationships, and experience. Psychologists also focus on individuals and personality factors, and anthropologists are concerned with the origins and evolution of human race and its culture. The intersection of these three disciplines might become interested in the context of cybersecurity and formulation successful strategies. Their approach to the problem would vary, however, with respect to the types of factor they chose to examine.

4 Knowledge and Skills

The purpose of this section is to present knowledge and skills that can instil proper approaches of formulation and implementation of successful cybersecurity strategies. Cybersecurity strategy developers should gain leverage from mastering these outlined knowledge and skills to provide sustainable cybersecurity at different levels of society. It should be noted that this is a non-exhaustive list and only outlines the knowledge and skills that are mostly overlooked in cybersecurity strategizing.

System Thinking is a scientific field of knowledge for understanding change and complexity through the study of dynamic cause and effect over time. This field is widely used for strategy formulation and testing at different levels highlighting areas of strategy including internal contradictions in a strategy, hidden strategic opportunities, and untapped strategic leverages [23]. System thinking, in general is the ability to see things as a whole, combining interconnections and explaining complexity [17]. It can help clarify mental models and study the critical success factors of strategies [37].

Adversarial Thinking is the ability to look at system rules and think about how to exploit and subvert them as well as to identify ways to alter the material,

cyber, social, and physical operational space [12]. In another word, adversarial thinking is the ability to embody the technological capabilities, the unconventional perspectives, and the strategic reasoning of hackers [14]. Adoption an adversarial mindset by the whole cybersecurity team allows the, to tackle the unique challenges of this domain. Understanding what the attackers are capable of and what their incentives might be is not easy and requires strategic awareness to enable the cybersecurity team form their belief about attackers' behavior.

Group dynamics and team learning , in the context of organizational change, study the need to be aware of the characteristics unique to the groups of actors and transferring knowledge within the organizations. Dialogue, as an essential requirement for group dynamics and team learning, results from generative conversations and shared vision among the institutions. In the context of cybersecurity teams, leaders and members should enhance the ability to extract very best from the collaboration intra- and inter-institutions. They need to identify the problems that have powerful detrimental impacts on groups to create effective learning environments.

Schoemaker et al. [32] identified six skills that, if mastered, enable the strategy developers to navigate the process discussed in Section 2 effectively. We believe that this is a comprehensive list that adaptive strategic leaders need to apply all six at once to be able to react strategically to environmental changes. Table 1 shows these skills and a short description of each skill.

Table 1. Essential Skills of Strategy Developers

Skill	Description
Anticipate	Gather information from a wide network of experts and sources both inside and outside your industry or function.
	Predict competitors' potential moves and likely reactions to new initiatives or products.
Challenge	Reframe a problem from several angles to understand root causes.
	Seek out diverse views to see multiple sides of an issue.
Interpret	Demonstrate curiosity and an open mind.
	Test multiple working hypotheses with others before coming to conclusions.
Decide	Balance long-term investment for growth with short-term pressure for results.
	Determine trade-offs, risks, and unintended consequences for customers and other stakeholders when making decisions.
Align	Assess stakeholders' tolerance and motivation for change.
	Pinpoint and address conflicting interests among stakeholders.
Learn	Communicate stories about success and failure to promote institutional learning.
	Course-correct on the basis of disconfirming evidence, even after a decision has been made.

Appropriate training and educating these knowledge and skills is an effective solution to tackle the evolving threat landscape and conflicts in the cyber domain and to fulfill the requirements of a successful strategy. Since each country or organization has a set of unique factors shaping their cybersecurity posture, cyber ranges can be leveraged to develop a stronger cybersecurity workforce and sustain critical skills for cybersecurity professionals [16]. A cyber range is a facility allowing a model of a digital system to run in a simulated environment to perform security tests, training and measurements that are applicable to the real world [36]. Since a well designed cyber range covers all the social and technical aspects in the cybersecurity domain, it can be a right and proper environment to contextually learn the required knowledge and skills.

5 Conclusion

Even if organizations have a clear understanding of their strategic goals and vision, translating these into daily routines is not obvious. This becomes more burdensome for areas like cybersecurity that are daily changing and require a balance between agility and consistency. In such areas, people routinely encounter complex situations and challenging decisions. To tackle these situations they need to use all the data, information and knowledge they have. In the real world situations, organizations have limited amount of, or limited access to, their required data and information in order to formulate responsive and multi-pronged strategies. Hence, in this paper, we presented a cognitive-driven process for strategizing in the cybersecurity domain. This is a twofold process highlighting the steps to transform available data to wisdom, and intuiting strategies to implementation of them through awareness to experience. This process aims to impact the actions decision makers might have on the future of their organizations.

Moreover, to elaborate the larger environment in which organizations are operating, we presented the cybersecurity value chain model outlining the primary and supportive operations in provision of sustainable cybersecurity. The supportive operations are categorized in four levels of institutions, multi-sided platforms, information technology infrastructure and people. The operations at each level are discussed briefly, however, in future we will explain this model in more details. Validation of this model is also one of the next steps in the future of this research. Finally, according to these discussions and elaboration of the complex domain of cybersecurity, we featured the required knowledge and skills to craft successful cybersecurity strategies. At the most basic level, strategy developers in this domain should be educated on these topics and use them in concert. Proper cybersecurity strategizing is a particularly critical task for ambitious managers who want to rise up the ranks of their organizations as cybersecurity has been recognized as one of the most important competitive advantages in recent years. As a result, learning how to take the all-embracing needs, to make decisions with the whole system in mind, and to align with the group of institutions help contribute to organizations' benefits and values.

References

1. Cyber Capacity Building Task Force — European Union Institute for Security Studies, https://www.iss.europa.eu/content/cyber-capacity-building-task-force-0
2. Cybersecurity Framework (CSF) Documents — NIST, https://www.nist.gov/cyberframework/framework
3. OECD Glossary of Statistical Terms - Corporate governance Definition, https://stats.oecd.org/glossary/detail.asp?ID=6778
4. Cyber Crisis Management. Tech. rep., Deloitte (2016), https://www2.deloitte.com/global/en/pages/risk/articles/cyber-crisis-management.html
5. Cyber Security Culture in Organisations (2017), www.enisa.europa.eu
6. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (2017). https://doi.org/10.1017/9781316822524, www.cambridge.org
7. Will, Skill, and Velocity: Survival Skills for a Digital World. In: Facing Up to Disruption. MIT Sloan Management Review (2018), https://learning.oreilly.com/library/view/facing-up-to/53863MIT60140/chapter006.html
8. Top 9 Cybersecurity Trends for 2020 (2019), https://www.boozallen.com/c/insight/publication/top-9-cybersecurity-trends-for-2020.html
9. Ackoff, R.: Ackoff's best: His classic writings on management (1999)
10. Adams, S.: ITIL V3 foundation handbook. The Stationery Office (2009)
11. Belmondo, C., Sargis-Roussel, C.: Negotiating Language, Meaning and Intention: Strategy Infrastructure as the Outcome of Using a Strategy Tool through Transforming Strategy Objects. British Journal of Management **26**(S1), S90–S104 (1 2015). https://doi.org/10.1111/1467-8551.12070
12. Dark, M., Privacy, J.M.I.S.., 2015, u.: Evaluation theory and practice applied to cybersecurity education. ieeexplore.ieee.org https://ieeexplore.ieee.org/abstract/document/7085972/
13. Evans, D., Schmalensee, R.: Matchmakers: The new economics of platform businesses. Harvard Business Review Press (2016)
14. Hamman, S.T., Hopkinson, K.M.: Teaching Adversarial Thinking for Cybersecurity. Tech. rep. (2016)
15. Khan, O., Estay, D.A.: Supply Chain Cyber-Resilience: Creating an Agenda for Future Research. Tech. rep. (2015), www.timreview.ca
16. Kianpour, M., Kowalski, S., . . . , E.Z..I.E., 2019, u.: Designing Serious Games for Cyber Ranges: A Socio-technical Approach. ieeexplore.ieee.org https://ieeexplore.ieee.org/abstract/document/8802499/
17. Kianpour, M., Kowalski, S.J., Øverby, H., Zoto, E.: From cyber incidents to training cognitive situation management:* work in progress. In: 2020 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA). pp. 163–166. IEEE (2020)
18. Kianpour, M., Øverby, H., Kowalski, S.J., Frantz, C.: Social preferences in decision making under cybersecurity risks and uncertainties. In: International Conference on Human-Computer Interaction. pp. 149–163. Springer (2019)
19. Kowalski, S.: IT insecurity: A multi-disciplinary inquiry. (1996), https://elibrary.ru/item.asp?id=6869736

20. Kowalski, S.: A Security and Trust Framework for a Wireless World: A Cross Issue Approach to. Tech. rep., Wireless World Research Forum (2004)
21. Leavitt, H.: Managerial Psychology. University of Chicago Press (1978)
22. Leonardi, P.M.: Materializing Strategy: The Blurry Line between Strategy Formulation and Strategy Implementation. British Journal of Management **26**(S1), S17–S21 (1 2015). https://doi.org/10.1111/1467-8551.12077
23. Maani, K., Cavana, R.: Systems thinking, system dynamics: Managing change and complexity (2007)
24. Malone, T.W., Crowston, K.: The Interdisciplinary Study of Coordination. ACM Computing Surveys (CSUR) **26**(1), 87–119 (1 1994). https://doi.org/10.1145/174666.174668
25. Manufacturing, A.T.A., 2020, u.: Cognitive informatics and wisdom development: Interdisciplinary approaches. igi-global.com
26. Marsh & Microsoft: 2019 Global Cyber Risk Perception Survey. Tech. rep. (2019), https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf
27. Martindale, D.: American society. RE Krieger Publishing Company (1960)
28. Overby, H., Audestad, J.: Digital Economics: How Information and Communication Technology is Shaping Markets, Businesses, and Innovation (2018), https://dl.acm.org/citation.cfm?id=3279279
29. Parenty, T.J., Domet, J.J.: A leader's guide to cybersecurity : why boards need to lead–and how to do it. Harvard Business Review (2019)
30. Potter, E.: Cyber-diplomacy: Managing foreign policy in the twenty-first century. McGill-Queen's Press-MQUP (2002)
31. Rescher, N.: Process metaphysics: An introduction to process philosophy. Suny Press (1996)
32. Schoemaker, P., Krupp, S., review, S.H.H.b., 2013, u.: Strategic leadership: The essential skills. Harvard Business Review (2019)
33. Shore, M., Du, Y., Zeadally, S.: A Public-Private Partnership Model for National Cybersecurity. Policy & Internet **3**(2), 168–190 (6 2011). https://doi.org/10.2202/1944-2866.1114
34. Underwood, B.: Studies in Learning and Memory: Selected Paper (1982)
35. Wen, S.F., Kianpour, M., Kowalski, S.: An empirical study of security culture in open source software communities. In: 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). pp. 863–870. IEEE (2019)
36. Winter, H.: System security assessment using a cyber range. In: IET Conference Publications. vol. 2012 (2012). https://doi.org/10.1049/cp.2012.1521
37. Zoto, E., Kianpour, M., Kowalski, S.J., Lopez-Rojas, E.A.: A socio-technical systems approach to design and support systems thinking in cybersecurity and risk management education. Complex Systems Informatics and Modeling Quarterly (18), 65–75 (2019)