Acting in the Unknown: The Cynefin Framework for Managing Cybersecurity Risk in Dynamic Decision Making

Josiah A. B. S. Dykstra, Stephen R. Orr, IV

***Abstract*—Researchers have shown that human decision making in complex environments like cyber is a significant risk factor. Unfortunately, much work on cyber situational awareness has been technology-focused, despite the ultimate importance of human decisions, especially in crisis situations like real-time cyber-attacks and data breaches. Cybersecurity practitioners and leaders require an appropriate framework to help decision makers at all levels guide and act while managing risk in unexpected and dynamic situations. Without such a framework, failure to enlighten the unknown leads to heightened risk, uncertainty, and insecurity. The ability to establish context, adapt, and apply the most appropriate decision-making style to unique situations increases the likelihood of security. We offer an application of the Cynefin Framework, a sensemaking solution, to cybersecurity which allows practitioners and leaders to identify the context and appropriate response type in complex situations using the cause-and-effect relationship. We also illustrate how orienting oneself in the five Cynefin domains – disorder, obvious, complicated, complex, and chaotic – can help manage risk. By comparing Cynefin to other decision-making frameworks, we show how this framework is uniquely appropriate for acting through complexity and risk in cyber.**

***Index Terms*—cybersecurity, Cynefin Framework, decision making, risk management, sensemaking, situational awareness**

I. Introduction

A preponderance of work related to cyber situational awareness has focused on technology to gather, analyze, and correlate data. The thinking, it seems, is that this information will help humans make better decisions more quickly. Unlike technology-focused decision making in cyber, the human counterpoint is rarely assessed [1]. Only recently has the community come to this realization, offering, for example, that "… cyber-cognitive situation awareness (CCSA) differentiates from the data fusion concepts to avoid confusion, and helps reiterate the importance of studying and improving the situation awareness of the human cyber defender" [2]. In crisis situations like real time cyber-attacks and data breaches, human decisions become paramount.

Today's cybersecurity operations are incredibly dynamic. Most cybersecurity activities require analysts and defenders to prepare, react, and respond to adversaries whose actions can change frequently and unpredictably. "Routine" attacks happen only inasmuch as attackers seek to exploit predictable vulnerabilities. In other domains like medical surgery and commercial aviation, experts can train for routine operations before extensive simulation and rehearsal of novel situations. Modern cyber defense paradigms tend to treat all decision making the same, regardless of the system they occur in. Uncertain, complex, and dynamic situations, like those on security watch floors, incubate risk. Dynamic reality demands dynamic decision making, and all too often decision makers rely on common approaches that work well in one set of circumstances but fall short in others.

Context is an important element of decision making. Erroneous mental models can unconsciously lead decisions astray, but deliberate self-awareness can improve decision making [3]. Snowden and Boone, architects of the Cynefin Framework, said, "A deep understanding of context, the ability to embrace complexity and paradox, and a willingness to flexibly change leadership style will be required for leaders who want to make things happen in a time of increasing uncertainty" [4]. It is the process of structuring the unknown to reveal context that enables us "to comprehend, understand, explain, attribute, extrapolate, and predict" [5] [6].

Cybersecurity, by its defensive nature, is fundamentally about the unknown because defenders must infer or deduce what adversaries are doing, thinking, and planning. Security comes from driving down unknown information enough to prepare and prevent surprise. A failure to enlighten the unknown leads to heightened risk, uncertainty, and insecurity. Technology and engineering for ordered, structured, and measurable problems are commonplace in government and business practices; cybersecurity is a complex ecology that cannot always be solved with engineering.

We propose a different approach to cybersecurity decision making, showing how weak signals of emerging risks are identified and interpreted within cybersecurity operations centers, and making the case for using the Cynefin Framework to understand risk in dynamic decision making. In Section 2, we present the Cynefin Framework and its application to cyber. We consider the interpretive work of risk analysis and the sensemaking processes employed to identify risks. In Section 3 we describe how Cynefin can help to manage risk,

Josiah A. B. S. Dykstra is with the Laboratory for Telecommunication Sciences, College Park, MD 20740 USA (e-mail: jdykstra@LTSnet.net).

Stephen R. Orr, IV is with the Department of Cyber Sciences, United States Naval Academy, Annapolis, MD 21402 USA (e-mail: sorr@usna.edu).

and in Section 4 discuss benefits and limitations. Related work is presented in Section 5 and we conclude in Section 6.

II. The Cynefin Framework for Cyber

Sensemaking [7] is a methodology and process for structuring the unknown and is part of the process of situational awareness [1]. The process involves coming up with a plausible understanding or map of the shifting world, testing this map with others through data collection, action, and conversation, and then refining, or abandoning, the map depending on how credible it is [8]. It is needed particularly when operating with little to no understanding of the environment, and when decisions must be made quickly. Sensemaking is an approach to figuring out what to do.

The Cynefin Framework is a sensemaking tool developed by Dave Snowden and first conceived in 1999 [9]. The Framework, pictured in Fig. 1, contains five domains that describe problems or situations and which guide action: disorder, obvious, complicated, complex, and chaotic. Before we describe each domain, consider a hypothetical scenario.

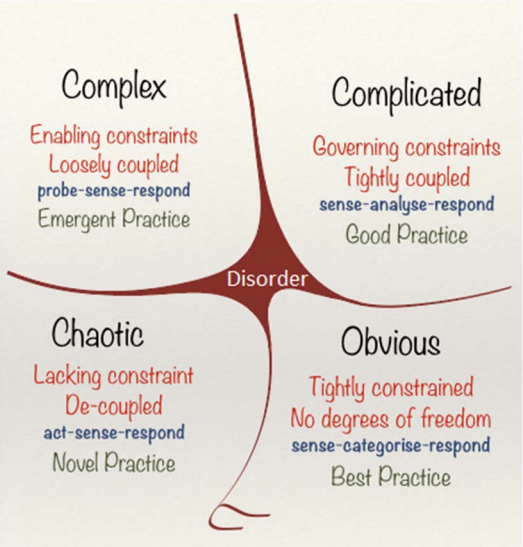

Fig. 1. Illustration of the Cynefin Framework showing the five domains of complex systems (including Disorder in the center). Adapted from [23].

Image an independent, medium-sized community hospital. The hospital IT staff is aware that they receive many phishing attempts each day. One morning, staff members begin to report that they are unable to access the hospital network. A closer investigation reveals that ransomware has spread across the network and locked out users, encrypting some computers until a ransom is paid.

A. Disorder in Cybersecurity

The domain of disorder describes the state of not knowing the relationship between cause-and-effect in a given problem or situation. In this state, people revert to their own comfort zone in making decisions. Disorder is the default state when you do not know which other domain you are in.

When the hospital IT team first receives calls that users cannot access the network in the scenario, the organization is in the domain of disorder because they do not know the cause of the issue. The team must contextualize the situation and gather information to help orient themselves into one of the Cynefin domains, after which they can take action. In this scenario, the key piece of information is learning that ransomware has infected some machines.

B. Obvious Domain in Cybersecurity

In the obvious domain (once called *Simple*), the relationship between cause-and-effect is clearly understood. The facts of the situation are assessed, categorized, and then a response based on established (best) practice is executed. Risk is lowest in this domain because it has the fewest unknowns. In the obvious domain, best practice governs action. While circumstances vary from case to case, there are established practices for reacting and responding to threats, and clear understanding about the effects of ones' actions.

When the hospital staff find that ransomware is the cause of network problems, the cause and effect of network outage is clear and there are few immediate options. The organization must identify and execute best practices for responding to the situation. Symantec, for example, recommends removing the infected systems from the network and exploring how data backups can restore impacted files [10].

C. Complicated Domain in Cybersecurity

In the complicated domain, the relationship between cause-and-effect is not necessarily well understood and requires the help of expert analysis. Several options should be investigated, expert advice taken into consideration, and then a response formulated based on the analysis.

After the hospital staff has executed best practices for stabilizing the network, they may find themselves facing several options. For example, they do not know how the cause of the attack which could be phishing, remote exploitation of an Internet-facing server, an insider, or other source. The hospital should seek expertise and analysis of subject matter experts in digital forensics or cyber security to help evaluate the situation and recommend next steps.

D. Complex Domain in Cybersecurity

In the complex domain, the relationship between cause-and-effect cannot be immediately understood, and often only in retrospection reveals the interrelationships between cause and effect. Several ideas are tested to see if they helped the situation. If those ideas did help, they are amplified; if not, they are dampened and other ideas are tested.

In the hospital attack, investigative and iterative forensic analysis may eventually reveal that an employee mistakenly opened a malicious email attachment that was actually a phishing attack. Client-side attacks, such as malicious attachments, can be complex when knowledge and defenses emerge only after experts explore the causes of the attack and possible mitigations. The hospital can identify and block the malicious email and malware in hindsight using exploration and experimentation. In the complex domain, emergent practice governs action.

E. Chaotic Domain in Cybersecurity

In the chaotic domain, there is no discernable relationship between cause-and-effect. Ad-hoc urgent decisions to stabilize the situation are the first priority, after which the next step to understand and respond to the root causes of the chaos can be determined. In the chaotic domain, novel practice governs action.

The hospital scenario did not present itself in the chaotic domain, but variations of it may have required the organization to act first and understand later. If the first indication of an attack had been the public release of personal or health data from the breach, and only later was phishing and ransomware found to be the cause, the chaotic domain would have suggested acting to stabilize the situation even before exploring the cause. In the Home Depot data breach, press releases on damage control preceded reports on analysis of the event [20].

The Cynefin Framework makes no value judgement about which domain is "best," other than that disorder should be avoided. The chaotic or complex domains are no more or less desirable than the complicated or obvious, and there is no inherent virtue in attempting to migrate from one domain to another. The boundaries between each domain are deliberately imprecise, indicating that there are transitional zones between them. A particular situation in question will reside primarily in one domain, though it may occupy a position that puts it at least partially in another zone, or in the transition area. Cynefin's value as a sensemaking framework lies in helping decision makers understand approximately where their systems and decisions lie among these domains, and by extension, what kinds of tools, approaches, processes, or methods are more likely to work successfully in a given system.

Decision makers who fail to recognize evolution during events, and therefore in the associated domain, risk falling behind the event without realizing it [10]. The reason the Cynefin Framework places the simple domain beside the chaotic is that the complacency resulting from entrained thinking significantly increases the risk of system collapse into chaos. Entrained thinking is also a risk for systems in the complicated domain, but in this case the ones at risk are not the leaders. Rather, it is the experts in functional areas who are most likely to fall into the trap of tradition, and they tend to dominate the complicated domain. The risk of entrained thinking in the complicated domain is that innovative ideas from non-experts may be disregarded by experts interested primarily in building and reinforcing their own knowledge. Profound knowledge must come from outside the system, and it must be invited in.

III. Cynefin for Managing Risk in Cybersecurity

Cybersecurity is an activity predicated on risk and Cynefin offers one approach to risk management. As may occur in cybersecurity work, risks are identified by constructing and enlarging small, fleeting moments of doubt, where current knowledge is questionable or suspect in some way. Sensemaking processes are supported by an analytical culture organized around assumptions that organizational knowledge is inherently limited, partial and fallible. Cynefin offers an approach to managing risk in cybersecurity.

Researchers have shown that decision making in complex environments is a risk factor. Cynefin has been applied to a variety of complex ecosystems, including medical knowledge [12], food chain risks [13], aviation [14], military ethics [15], and homeland security [16]. Even among expert physicians, complex cases have been associated with lower quality decisions and lower confidence in decisions [17]. Similarly, cyber operations have been shown to be cognitively demanding [18][19], and mental shortcuts are necessary to handle the load.

There have been many proposals for measuring and calculating risk in cybersecurity, but Cynefin manages some risk regardless of the risk management framework. By definition, a defending organization's risk increases as expected losses increase, and the risk decreases as the attacker's gains decrease. A critical element is the amount of time that the attacker can operate before the defender deploys a countermeasure. The Cynefin Framework decreases risk when the defenders recognize the operating domain and begin acting accordingly.

The Cynefin Framework offers an opportunity to drive down risk and enable contextual decision making in cybersecurity. In a sensemaking framework like Cynefin, the data precede the framework, unlike a risk categorization model where the framework precedes the data. Cynefin does not dictate how one acts; the framework for action and decisions is allowed to emerge with the data. The inherent assumption with Cynefin is that a one-size-fits-all decision-making framework is not sufficient for all problems. Cynefin provides a method to orient oneself to the situation at hand, analyze, and act according to a framework that emerges from data, not the other way around.

One tangential benefit of Cynefin is that it can help communicate and explain a complex situation to stakeholders. Even though data is now available nearly instantly and virtually for free, building the story is what makes information relevant. The ability to contextually understand events or facts presents an opportunity for decision makers to apply the most appropriate leadership style. By internally constructing the story, informed by context and action in the appropriate Cynefin domain, decision makers have the opportunity to make a defensible, risk-informed choice. Understanding and shaping situational context allows decision makers to influence outcomes.

Adopting the Cynefin Framework would allow cyber defenders to achieve at least three other tangible benefits:

1. **Cynefin Increases Knowledge Management**. There is a systemic problem in many operations centers with recording institutional knowledge [6]. Analysts and subject matter experts routinely amass knowledge that becomes lost when that individual leaves his or her job. Furthermore,

organizations also fail to learn and apply lessons from previous decisions given a lack of historical record. Future decision making would be less risky and more informed by a record that captured how the decision was made and why. Cynefin provides a framework and language to enable this goal.

2. **Cynefin Redefines Secrecy**. Risk is very high in unknown and disorderly situations. Historically, corporate and government security has used secrecy to protect information and decrease risk of its disclosure. Cynefin, as applied to sensitive information, redefines secrecy based on situational complexity. The more complex the situation, the less secret information must be in order to lower the situational risk. To the contrary, in the obvious and complicated domains, information can be protected more because decision making in response actions are more well defined.
3. **Cynefin Illustrates Risk**. It is tempting for humans to try and quantify risk levels with a number or a color or other concrete metric. Unfortunately, risk is too complicated to be simplified in such a manner. Cynefin provides a mechanism to visualize risk by showing risk as a function of uncertainty.

IV. Discussion

The obvious domain encompasses clear cause-and-effect relationships with known knowns. Defenders must be wary of complacency and comfort by recognizing the value and limitation of best practices. "The most frequent collapse into chaos occurs because success has bred complacency," said one author [1]. For example, if an intrusion detection system (IDS) alerts a false-positive, subject matter experts (SME) can review the suspected anomalous behavior and modify the signature as appropriate. A false positive occurs because the signature is written too broadly and encompasses both legitimate and illegitimate traffic. However, if the SME becomes complacent and does not modify the signature then false positives may flood the IDS and drown out any legitimate alerts. Thus, known knowns are drowned in a sea of information and chaos ensues.

The complicated domain is where cause-and-effect relationships are discoverable but not immediately apparent to everyone. In fact, there is more than one right answer possible within this known unknown context. Practitioners must not be overconfident in their own solutions or over analyze the current situation (e.g. analysis paralysis). In order to discover the cause-and-effect, it is important to challenge conventional or entrained thinking by listening to the advice of non-experts, even when it conflicts with the status quo. For example, troubleshooting the cause of a crashing application may require analysis from independent and unbiased evaluators. Unfortunately, opportunities for discovery are lost when an external team of non-experts is not considered, and organizations lose innovative suggestions and findings that may disrupt the status quo for the better. Leaders must consider the expert's deliverables, but also encourage and support opportunities and solutions from others.

The complex domain entails so-called "unknown unknowns" where no single right answer is evident. Whether they know it or not, many organizations find themselves in this domain. Innovation, dissent and diversity, and creative environments that allow patterns to emerge are required to achieve a successful outcome. Exploratory analysis in the search for insider threats is one example where solutions are unknown at the outset. It is important for organizations, especially leaders, to be transparent and maintain open communication with the intent of generating ideas. Barriers to success include a command-and-control organizational construct, impatience by the leadership to generate results, and jumping to conclusions rather than allowing patterns to emerge. The complex domain is uncomfortable to many leaders because there is no single right answer and many competing ideas. The complex domain requires experimentation, freedom to fail, and flexibility to operate beyond the normal constraints.

The chaotic domain can seem impossible to manage because the relationship between cause-and-effect has not been determined. Without predictable or identifiable patterns, order must be established through command-and-control, and then transform the situation from the chaotic to complex domain. Barriers to success result when leaders continue to apply the command-and-control approach after transition to the complex domain. Remember, the complex domain requires innovative approaches.

Adopting the Cynefin Framework requires that cyber defenders pay closer attention to their situations and thought processes. Humans are naturally anxious to act, especially in a crisis, even though consciously identifying the Cynefin domain where the decision resides would help us act more appropriately. Cynefin can increase conscious self-awareness in cyber.

V. Related Work

The Cynefin Framework is not the only decision-making and risk management framework for complex systems, but we believe it is best suited for the dynamic environment of cybersecurity. It is difficult to know which, if any, decision making frameworks are used by individuals, industry, or governments for cybersecurity operations today. There are other methods that may complement the Cynefin Framework and we present three for comparison.

A. Cynefin and the OODA Loop

The Cynefin Framework and the Observe-Orient-Decide-Act (OODA) loop both provide decision-making support with the intent of thriving in ambiguous situations. The Cynefin Framework presents different decision modes shifting us, intentionally or unintentionally between domains. The OODA loop is a decision-making cycle that rewards the user for exercising the stages of the framework the fastest. Both of these help us to understand uncertainty, but in different ways. Cynefin helps us become contextually aware while the OODA

loop encourages agility and speed to react to our opponents. Most presentations of the OODA loop convey the method in a four-step process but a deep study of the OODA loop would reveal a much more complex diagram. A primary difference between the two is that the Cynefin Framework presents a different decision mode in each of the domains, while OODA is a single, but repeatable process. There may be a complementary application of the two decision-making frameworks.

B. Cynefin and Panarchy

The Panarchy and Cynefin Frameworks both attempt to address complexity. However, the Panarchy Framework was developed to help decision makers understand the source and role of change in complex systems whereas Cynefin helps decision makers establish context. While both tend to be visually represented in a two-by-two matrix, Panarchy presents what is referred to as the adaptive system—exploitation, conservation, release, and reorganization—through which all ecosystems evolve. Panarchy is a different kind of option for understanding change in complex systems.

C. Cynefin and PDCA

Plan-do-check-act (PDCA) is a method for executing change in a complex environment. The goal of PDCA is to enable continuous improvement in processes, systems, and projects. The method has roots to the scientific method (e.g. hypothesis, experiment, evaluation) and can be used to identify root causes in any challenge or context. While the PDCA method has a role in complex environments, it is presented out of context when discussing risk and uncertainty. Finally, PDCA may be most applicable to the obvious domain within the Cynefin Framework whereby there is a clear cause-and-effect relationships and known knowns. PDCA could be used for improvement of existing processes and best practices.

It is difficult to infer how cyber incidents are handled today. Google, for example, never revealed how they discovered and acted in the early stages of "Operation Aurora," though cybersecurity experts widely acknowledged the complexity and sophistication of this attack. One might presume that the situation was initially in the domain of disorder, perhaps moving to the complex domain where decision makers desired to first probe for facts. In the 2014 Home Depot data breach, a press release stated that "The investigation began… immediately after the company received reports from its banking partners and law enforcement that criminals may have hacked its payment data systems. Since then, the company's internal IT security team has been working around the clock… to rapidly gather facts and provide information to customers" [20]. This suggests action in the chaotic domain as the company developed novel practice in their incident response.

VI. Conclusion

In interviews with 1,500 global chief executive officers, IBM found that successful leaders and organizations act despite uncertainty [22]. They fight the natural urge to wait for clarity and stability, taking calculated risks while others hesitate. Such leaders find a creative way to turn complexity into an advantage. Like cyber defenders, they rely on deeply felt values and a well-defined vision to provide the confidence and conviction to exploit narrow windows of opportunity. Cynefin provides a framework for integrating perspectives into a stronger, unified picture of risks. In particular, it can be used to review and appreciate multiple stakeholder views of cybersecurity risks without the prior assumption that analytic and social appreciations are fundamentally disjointed.

Cynefin empowers decision makers to recognize the context of cyber events and propose innovative solutions in complex situations. Innovative solutions which start as emergent practices may eventually transform to good practices in the complicated domain, and ultimately become best practices in the obvious domain. If a similar event occurs again, self-aware operators will spend less time characterizing the situation and more quickly orient to best practices.

Decision-making under conditions of risk and uncertainty necessitate decision making competencies that can help to make sense of the fluid environment. Cyber defenders face uncertainty on a day-to-day basis, and the Cynefin Framework is a powerful approach to leading through that complexity and reducing risk. Applying the Cynefin Framework allows individuals and organizations to define the context by the nature of the cause-and-effect relationship. By first establishing context, decision makers may apply the appropriate approach to the domain and unique situation they find themselves. The Cynefin Framework enables decision makers the flexibility to adapt accordingly to their situation. Moreover, it illuminates our inherent desire and helps us avoid our human nature by defaulting to a preferred leadership style. This approach will enable collaboration through contextual understanding, the reduction of risk, and lead to innovative solutions

Acknowledgment

The authors thank the anonymous reviewers for their helpful comments. The views and opinions expressed in this paper are solely those of the authors, and do not necessarily represent those of the Department of Defense or the U.S. government.

References

[1] F. T. Durso and A. Sethumadhavan, "Situation awareness: Understanding dynamic environments," *Human Factors*, vol. 50, no. 3, pp. 442–448, 2008.

[2] R. S. Gutzwiller, S. M. Hunt, and D. S. Lange, "A task analysis toward characterizing cyber cognitive situational awareness (CCSA)," *IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*, 2016.

[3] J. Mugan, *The Curiosity Cycle.* Buda, TX: Mugan Publishing, 2014.

[4] D. J. Snowden and M. E. Boone, "A leader's framework for decision making," *Harvard Business Review*, pp. 69–76, November 2007.

[5] R. H. Waterman, Jr., *Adhocracy: The Power to Change.* Memphis, TN: Whittle Direct Books, 1990.

[6] W. H. Starbuck and F. J. Milliken, "Executives' perceptual filters: What they notice and how they make sense," in *The Executive Effect: Concepts and Methods for Studying Top Managers*, D.C. Hambrick, Ed. Greenwich, CT: JAI, pp. 35-65, 1988.

[7] K. E. Weick, *Sensemaking in Organizations.* Thousand Oaks, CA: Sage Publications, 1995.

[8] D. Ancona, “Sensemaking: Framing and acting in the unknown,” in *Handbook of Leadership Education*, N. N. Snook and R. Khurana, Eds. Los Angeles: SAGE, pp. 3-19, 2011.
[9] D. J. Snowden, “The paradox of story: Simplicity and complexity in strategy,” *Scenario and Strategy Planning*, vol. 1, no. 5, November 1999, pp. 16–20.
[10] Symantec, “Ransomware Do's and Don'ts: Protecting Critical Data,” 2015. Available: http://www.symantec.com/connect/blogs/ransomware-dos-and-donts-protecting-critical-data.
[11] R. E. Bellman and L. A. Zadeh, "Decision-making in a fuzzy environment," *Management Science*, vol. 17, pp. B-141-B-164, 1970.
[12] J. P. Sturmberg and C. M. Martin, “Knowing in medicine,” *Journal of Evaluation in Clinical Practice*, vol. 14, pp. 767–770, 2008.
[13] R. Shepherd, G. Barker, S. French, A. Hart, J. Maule, and A. Cassidy, “Managing food chain risks: integrating technical and stakeholder perspectives on uncertainty,” *Journal of Agricultural Economics*, vol. 57, pp. 311–327, 2006.
[14] M. R. Endsley, “Situation awareness in aviation systems” *Handbook of aviation human factors.* D. J. Garland and J. A. Wise, Eds. Mahwah, NJ: Lawrence Erlbaum Associates, pp. 257–76, 1999.
[15] R. C. Gresser. (2014, September 1). “Macro ethics and tactical decision making,” *Military Review*. [Online]. Available: http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20141031_art013.pdf
[16] C. Bellavita. (2006). “Changing homeland security: Shape patterns, not programs,” *Homeland Security Affairs*, vol. 2, no. 3. [Online]. Available: https://www.hsaj.org/articles/680.
[17] V. Sintchenko and E. Coiera, “Decision complexity affects the extent and type of decision support use,” *AMIA Annual Symposium Proceedings*, pp. 724–728, 2006.
[18] J. Dykstra and C. Lyn Paul, “Stress and the cyber warrior: Cognitive workload in a computer operations center,” *Journal of Sensitive Cyber Research and Engineering*, vol. 3, no. 1, pp. 1-23, 2015.
[19] A. Amico, K. Whitley, D. Tesona, B. O’Brien, and E. Roth, “Cyber defense situational awareness: A cognitive task analysis of information assurance analysts,” *Proceedings of Human Factors and Ergonomics Society Annual Meeting*, vol. 49, no. 3, pp. 229-233, 2005.
[20] The Home Depot, “The Home Depot provides update on breach investigation,” September 8, 2014. Available: http://ir.homedepot.com/news-releases/2014/09-08-2014-014517970.
[21] E. Bertino, L. R. Khan, R. Sandhu, and B. Thuraisingham, “Secure knowledge management: Confidentiality, trust, and privacy,” *IEEE Trans. Syste., Man, Cybern. A, Syst. Humans,* vol. 36, no. 3, pp. 429-438, May 2006.
[22] IBM, “Capitalizing on complexity: Insights from the global chief executive officer study,” 2010, Available: http://www-935.ibm.com/services/c-suite/series-download.html.
[23] D. J. Snowden. (2014, July). Cynefin as of 1st June 2014. [Online]. Available: https://commons.wikimedia.org/wiki/File:Cynefin_as_of_1st_June_2014.png.