Computers & Security 92 (2020) 101761

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished

Bongsik Shin[a], Paul Benjamin Lowry[b,*]

[a] Fowler College of Business Administration, San Diego State University, 5500 Campanile Drive, San Diego, CA, 92182, USA
[b] Pamplin College of Business, Virginia Tech, Pamplin Hall Suite 1007, 880 West Campus Drive, Blacksburg, VA, 24061, USA

ARTICLE INFO

Article history:
Received 15 November 2019
Revised 3 February 2020
Accepted 13 February 2020
Available online 14 February 2020

Keywords:
Security
Organizational security (OrgSec)
Human factors of security
Cyberthreat intelligence (CTI)
Risk management
Triarchic theory of intelligence (TTI)
CTI capability model (CTI-CM)
Information security officer
CTI practitioner
CTI analyst

ABSTRACT

Given the global increase in crippling cyberattacks, organizations are increasingly turning to *cyberthreat intelligence* (CTI). CTI represents actionable threat information that is relevant to a specific organization and that thus demands its close attention. CTI efforts aim to help organizations "know their enemies better" for proactive, preventive, and timely threat detection and remediation—complementing conventional risk-management paradigms designed to improve 'general readiness' against known or unknown threats. Organizational security (OrgSec) and behavioral security research has lagged behind CTI's growing potential to address current cybersecurity challenges. Instead, CTI has largely been the purview of computer science from an algorithmic perspective. However, OrgSec and behavioral researchers can contribute a further combined knowledge of design for the organization, human factors, and organizational governance to foster CTI. In this theory-building and review manuscript, we propose the CTI capability model (CTI-CM) to prescribe the key capabilities necessary for a CTI practitioner to engage effectively in CTI activities. The CTI-CM defines a practitioner's CTI capability in terms of three highly interrelated but conceptually distinctive dimensions: analytical component capability, contextual response capability, and experiential practice capability. We further explain how these capabilities can be fostered, and the key implications for leading security practice in organizations.

1. Introduction

In response to increasing global security incidents, and the failure of general security readiness approaches, organizations have increasingly turned to *cyberthreat intelligence* (CTI) efforts (cf. Qamar et al., 2017; Samtani et al., 2017; Shackleford, 2018; Tounsi and Rais, 2018; Wagner et al., 2019). In short, CTI represents *actionable threat information* tailored to a specific organization that requires careful attention and prevention. CTI consists of activities designed to recover threat information germane to a specific organization to engineer more precise defense strategies. This information includes threat types, sources, actors, technologies, and attack vectors. Although organizations with first-rate security capabilities have engaged in forms of CTI for a number of years (Bejtlich, 2013; Heberlein et al., 1990; Stoll, 1988, 2005), dramatic developments in its supporting technologies have started relatively recently (Qamar et al., 2017; Seals, 2017).[1] CTI is already widely embraced in industry; a survey of 585 organizations by Brown and Lee (2019) showed that 72% of them were producing or consuming CTI in 2018.

CTI efforts can help an organization perform more *proactive, preventive*, and *timely* threat detection and remediation—complementing the conventional risk-management paradigm designed to improve *general readiness* against known or unknown threats (Khan et al., 2019). Thus, the purpose of CTI is to enable better decisions related to security threats and it is "consumed" at different levels for decision making throughout the organization, including at the strategic-, tactical- and operational levels. With its unconventional orientation, CTI information is frequently

[1] We observed a surge of scholarly CTI-focused publications since 2016 by computer scientists who have focused primarily on technical issues. On Google Scholar, a simple search of scholarly publications (on February 3, 2019) with "threat intelligence" and "cyber" in the title first appeared in 2012 with one result. From 2012 through 2015, there were 13 results. The publications have exploded to 97 since 2016. Although this a simple metric, the results reflect the growing traction of CTI as a new security paradigm.

* Corresponding author.
E-mail addresses: bshin@sdsu.edu (B. Shin), Paul.Lowry.PhD@gmail.com (P.B. Lowry).

https://doi.org/10.1016/j.cose.2020.101761
0167-4048/

characterized by such words as *timely, relevant, context oriented, evidence based, analytical, specific*, and *actionable* (Holland, 2013; Skopik, 2018). If executed well, CTI can offer many different benefits, including learning adversaries' attack methodologies; anticipatory and proactive problem-solving; timely decision-making and deployment of precise countermeasures; improved situational awareness and understanding of threat trends; adequate prioritization in risk remediation against a large number of agile adversaries; better damage containment; and collaborative problem-solving through CTI sharing (Ahrend et al., 2016; Fransen and Kerkdijk, 2018; Gschwandtner et al., 2018; Johnson et al., 2016; Leitner et al., 2018; Lutf, 2018; Skopik, 2018; Tounsi and Rais, 2018; Webb et al., 2014, 2016).

CTI practitioners are at the forefront of an organization's CTI efforts. In this paper, we propose an individual-level capability model called the *CTI capability model* (CTI-CM), which delineates the capability dimensions of effective CTI practitioners who protect their organizations. We leverage Sternberg's (1999, 2003) triarchic theory of intelligence (TTI) as the basis of the relevant CTI capability dimensions. Our model includes three interrelated but conceptually distinct capability dimensions necessary for performing CTI-related tasks successfully: an analytical component, contextual response, and experiential practice. The dimensions are sufficiently broad to reflect the practical circumstances of CTI tasks, which pose difficult challenges to anyone executing such tasks.

Organizational security (OrgSec) researchers can greatly contribute to CTI research beyond the highly technical challenges, because CTI requires unique interactions between security artifacts, organizations, processes, and people. The nontechnical issues include guiding CTI initiatives and capabilities and providing a theoretical foundation for promoting CTI efforts at the individual and organizational levels. This theory-based review proposes the CTI-CM to illustrate the key roles of practitioners in CTI activities.

The CTI-CM has strong potential for theoretical and practical importance in OrgSec research. First, despite its rapid rise as an important cybersecurity paradigm, CTI has been driven primarily by industry practitioners and computer scientists; organizational and behavioral scholarship in this area has been scant.[2] This paper lays a preliminary foundation for further OrgSec research, which can potentially take many directions and be applied at the individual or organizational level. Second, CTI practitioners' ability to conduct advanced threat analysis and plan countermeasures that scale vertically and horizontally is a pivotal organizational concern (Muckin and Fitch, 2015). Little has changed since Straub and Welke's (1998) determination that security practitioners are relatively weak in the 'intelligence' aspect of cybersecurity (Kwon and Johnson, 2014).

This paper is structured as follows: Section 2 briefly highlights differences between CTI and the conventional defense paradigm. Section 3 provides an overview of the literature to explain CTI practitioners' success conditions. Section 4 then describes Sternberg's theory and how it supports our development of the CTI-CM, which is further proposed in Section 5. The anticipated effects and implications of the CTI-CM are framed at both the individual and organizational levels in Section 6. Finally, in Section 7, we propose a research agenda for OrgSec and behavioral security scholars interested in testing and extending the CTI-CM.

[2] It is natural to wonder why there have been few organizational or behavioral publications on CTI. We can only speculate on two potential reasons. First, although the CTI concept has been around for years, only recently has there been an active development of technical solutions and large-scale industry adoption. Second, CTI involves highly technical details, about which most organizational and behavioral researchers are not knowledgeable. Moreover, CS researchers have naturally taken to the topic, and their publications tend to be published more quickly, given their focus on conference papers

2. The conventional security paradigm and CTI

In many organizations, although not deliberately planned, OrgSec efforts have ended up focusing on improving general *readiness* against potential threats that are poorly suited to defend against sophisticated cyber-attacks. This orientation is largely in line with the Baskerville et al. (2014) prevention paradigm that manages predicted threats based on such assumptions as threat persistency, a static relationship between threats and controls, and threat measurability. This mode of risk management may be rooted in (1) compliance culture, as it encourages organizations to adopt a tick-box mentality resulting in the watering down of risk management methods and the erection of conventional security defenses (Shedden et al., 2009; Tan et al., 2010) and (2) an underlying and deeply rooted belief that cyber security risk can be assessed and mitigated in probabilistic terms not possibilistic terms resulting in a strategy of investing in defenses that are generally of a higher quality but not aimed at combating specific attacks or threat agents (Baskerville et al., 2014).

Such defense practices tend to be passive, static, reactive, and curative, and they frequently rely on solutions that are uniform and standardized across organizations. Examples include timely patch management to remove software vulnerabilities; vendor-provided antivirus and antimalware; compliance with regulatory requirements; and security training of employees. These measures are vastly important in repelling attackers with poor to moderate skills. However, recent large-scale security breaches clearly demonstrate that the risk-management approaches are insufficient to anticipate and thwart serious attacks. Experienced adversaries know how to beat standard practices and defense solutions (Wernick, 2018). Consequently, highly dynamic and sustained attacks leveled by well-resourced hacking groups, organized crime rings, or rogue nations have been wreaking havoc on enterprises (Navarro et al., 2018; Tounsi and Rais, 2018). Such attacks include advanced persistent threats (APTs) (Ahmad et al., 2019), composite/blended attacks (Tounsi and Rais, 2018), and multistage attacks (Navarro et al., 2018). To fend off such transient, unpredictable and unmeasurable threats, Baskerville et al. (2014) suggested that organizations embrace the *response* paradigm more to elect emergent, rather than persistent, controls.

The 2400-year-old lesson of the legendary military strategist and philosopher Sun Tzu further offers a clue about why the rather conventional cybersecurity efforts have been only partially successful against sophisticated adversaries. In his timeless book *The Art of War*, he states that

> if you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle.

This metaphor implies that the general readiness cybersecurity measures lack the defense orientation specifically tailored to a particular organization. In the context of cybersecurity, knowing your enemies entails a situational awareness of the threats (Webb et al., 2014; 2016), and the details of the threats, *explicitly relevant* to an organization (Brown and Lee, 2019). This metaphor is the foundation of CTI, which shifts the focus of cybersecurity to actively uncovering explicit threat information pertaining to an organization.[3] CTI thus requires dynamic learning of the *particularities* of

[3] CTI activities do not require that organizations or individuals have the investigative authority of law enforcement agencies, the authority to counterattack attackers, or the legal jurisdiction to punish internal or external attackers. These activities belong to governments. Importantly, governments are increasingly adopting more aggressive measures to raise the cost of attacks (Ferran 2018). CTI activities are meant to create more effective lines of defense against targeted adversaries and threats.

threats to which an organization may be subject and that have the potential to produce crippling consequences. This way, CTI should be used not only to strike the balance between the prevention-oriented and response-oriented defenses (Baskerville et al., 2014) but also to significantly fortify both of them at an organization.

Although CTI may seem like a natural extension to how organizations currently deal with threats, it requires a different mindset and approach. A clear way to illustrate the chasm between the two approaches is through showing the difference in practice that occurs with ransomware, which is an increasingly sophisticated and pernicious attack. The conventional, general readiness approach to defend from ransomware attacks largely relies on deploying updated client and server-side anti-virus programs, executing backups, and providing employee training to avoid phishing. Nevertheless, this approach leaves organizations highly exposed to ransomware vulnerability. In fact, although 75% of companies infected with ransomware were running up-to-date endpoint protections, ransomware attacks have increased 97% in the last two years, and a new organization fell victim to ransomware every 14 s in 2019 and this will increase to every 11 s by 2021 (Dobran, 2019). Accordingly, ransomware continues to wreak havoc worldwide, pragmatically illustrating that traditional defenses are woefully inadequate. A CTI mindset adds to the conventional approach by underscoring that additional defense measures against ransomware must be actively deployed and tailored to such specific information as: (1) a knowledge of currently active ransomware and how it is used in a particular industry; (2) an active understanding of their attribution (e.g., signatures and hashes, source IPs, blacklisted domains); and (3) learning their infection vectors and tactics (e.g., spear phishing approaches and sources of this information). A CTI mindset also involves the timely sharing of ransomware information between firms in the same industry and a focus on predicting and preventing unknown but possible future ransomware attacks. Overall, this is a more active approach that strengthens traditionally reactive approaches.

To further understand the importance of knowing your enemies, imagine that a boxer trains to improve his/her defenses in advance of a match. First, the boxer can try to improve his/her general defense skills without regard to the upcoming opponent. Second, the boxer can also train in a manner tailored to the opponent's offensive style. A boxer can thus increase his/her odds of success by mastering both general defense and defense tailored to an opponent's unique offensive strengths. The latter approach is taken by CTI practitioners to compensate for the limitations of the traditional general readiness measures.[4]

3. Literature: CTI practitioners

Given that our manuscript proposes a CTI model of practitioner capability, this section offers an overview of general industry expectations of security practitioners who undertake CTI tasks. To identify CTI-related publications cited throughout this manuscript, we performed literature search of journal databases, Google Scholar, and scholarly books using keywords matching "CTI," "threat intelligence," or "cyber threat intelligence" included in the title or abstract. This relatively narrow search method was used as there are simply too many publications related to cybersecurity, information security, or organizational security. Given the existence of grey areas between CTI and traditional cybersecurity research domains, our search approach was used to ensure that authors were aware of their work's relevance to CTI. Because industry is significantly ahead of academia in CTI research and practice, we also searched the broader Internet to discover highly relevant, non-scholarly CTI articles using the same keywords.

3.1. Background: security practitioners and CTI practice

As the Sun Tzu's metaphor implies, the CTI professional is tasked to uncover threats specifically dangerous to his/her organization; and, depending on his/her responsibility scope, to come up with counter measures. The function of *learning the enemies (*i.e.*, threat agents including humans and software)* that are particularly dangerous to his/her organization complements the traditional, *general readiness-oriented* security functions. For this, CTI professionals carry out functions that have not been central to the conventional security staff's tasks. Among them are learning or uncovering: adversaries (threat actors) that target the industry his/her organization belongs to; TTPs (tactics, technologies, and procedures) used by the adversaries; where/how stolen information is being monetized; cyber-attack and attacker trends; active malware (e.g., malware hashes, procedure) used to target the industry of his/her organization; specific indicators of attacks (e.g., IPs, URLs, domains, hashes) to block; and particular software vulnerabilities targeted by adversaries (Brown and Lee, 2019).

Depending on the arrangement, CTI practitioners may perform the CTI tasks exclusively or as a part of their overall responsibilities, which include other tasks. Thus, those who practice CTI vary widely in their organizational role (Shackleford, 2018). It was reported that the majority of enterprises with a CTI function create CTI-dedicated positions and many mature organizations maintain a CTI-team (e.g., threat engineers, threat modelers, threat analysts and CTI lead) to focus on CTI tasks (Ahrend et al., 2016; Brown and Lee, 2019). Moreover, close to 30% of organizations reported that information security staff also share CTI responsibilities despite that they are already tasked to keep up with traditional controls and countermeasures to strengthen the general readiness (Brown and Lee, 2019). Regardless of the staffing arrangement, therefore, this paper assumes that there is a common body of cognitive, experiential, and learning components that contribute to the successful handling of CTI tasks by any CTI practitioner.

3.2. Competencies required of CTI practitioners

A successful CTI engagement requires practitioners to possess broad competence in various technical and nontechnical knowledge domains consumed across organizational ranks. This is because CTI has strategic, operational, tactical, and technical dimensions and associated values (Chismon and Ruks, 2015; Maglaras et al., 2019; Tounsi and Rais, 2018).[5] Further, CTI practitioners should be competent to comprehend and manage an organization's risk management tasks both from the prevention-oriented and response-oriented paradigms (Baskerville et al., 2014).

[4] Importantly, the traditional approaches designed to improve *general readiness* and CTI-enabled activities are not mutually exclusive but instead need to be closely coupled to be synergistic. For example, not only can firewalls and intrusion detection systems be used to deploy filtering rules commonly applicable to many organizations; they can also be configured with the CTI-derived intelligent rules unique to an organization. Thus, there is already a gradual convergence in commercial products. For example, the next-generation firewalls can add packet filtering rules (e.g., blacklisted domains and IPs, malware hashes) dynamically through cloud services. One significant challenge of deploying such dynamic rules in a timely manner is to automate the deployment of CTI-enabled rules to the defense system while minimizing the likelihood of false alarms.

[5] *Strategic CTI*, such as attack trends, represents nontechnical, high-level information necessary for such tasks as strategic planning, forming a security vision and road maps, incident-response planning, and determining financial impacts. *Operational CTI* focuses on the details of threats relevant to defense preparations (e.g., tactics, techniques, and procedures) (Ghazi et al. 2018; Maglaras et al. 2019). *Tactical CTI* is obtained from the real-time monitoring of organizational systems for timely incidence response (Maglaras et al. 2019). *Technical CTI* (e.g., malware hashes, threat domains, and IPs) involves the lower-level technical details of threat indicators (Chismon & Ruks 2015; Poputa-Clean 2015).

Thus, the more practitioners are well-rounded in the various domains, the more successful they will be in undertaking CTI (Ahrend et al., 2016; Pickett, 2018). Due to the broad knowledge base and skills required, CTI practitioners may need years of practical experience to become effective (Pickett, 2018).

Nevertheless, the division of labor or role division for CTI tasks is difficult. In many business information–processing tasks, roles are clearly divided according to hierarchical ranks or positions. For example, database system administrators, business data analysts, and business decision-makers who produce or consume information undertake distinctively different information-processing tasks. This level of division of labor, however, is difficult to apply to CTI due to (1) the highly specialized nature of the cybersecurity domain and of the skills involved, (2) the close coupling of technical and nontechnical domain knowledge consumed at different organizational ranks, and (3) the practical fact that the majority of organizations do not create a CTI team of different ranks and that many of them have only a single CTI employee (Brown and Lee, 2019) presumably due to practical reasons such as cost burdens. Given the demanding task circumstances faced by CTI practitioners, the next section introduces Sternberg's TTI, from which we derive a prescriptive CTI capability model.

4. Foundation: the triarchic theory of intelligence (TTI)

4.1. Background

To systematically delineate the core competency dimensions required to lead successful CTI efforts, we leverage Sternberg's TTI (1985, 1997, 1999, 2003). Here, we summarize the motivation for and contribution of TTI to our theorization: Sternberg was a leading psychology expert on human creativity and intelligence. The foundation of TTI was Sternberg's supposition that a one-score general approach did not properly represent human intelligence, and that the common IQ test ignored or downplayed crucial aspects of intelligence such as creativity; the TTI hence proposes that instead human have three distinct categories of intelligence: *practical, distinct*, and *analytical*, and each of these has a related subtheory in TTI (Shrestha, 2017; Vinney, 2019).

In this context, *practical or contextual intelligence* is explained by the practical or contextual sub-theory of TTI and can be loosely defined as common sense or "street smarts" (Shrestha, 2017). *Distinct or experiential intelligence* is explained by the experiential subtheory and is basically about one's creativity (Shrestha, 2017). Finally, *analytical* or *component* intelligence is explained by the analytical or subcomponent sub-theory and is loosely defined as "book smarts" (Shrestha, 2017).

It is natural to ask whether Sternberg's TTI is an apt framework from which to derive the CTI-CM, because the term "intelligence" has distinct meanings in CTI and the TTI. The TTI concerns *human intelligence*, which is the ***ability*** to acquire and apply knowledge and skills, whereas CTI concerns intelligence in the sense of obtaining valuable information in a cybersecurity context. Moreover, it could be argued that the TTI can describe the capability dimensions of any information-processing task. To address these potential criticisms, we clarify that the TTI is used not because both CTI and the TTI share the word "intelligence," but because the TTI is fundamentally about what gives humans their abilities and satisfies three important conditions of deriving CTI capability.

Fundamentally, our operating assumption in a CTI context and as the core our theorization is that one's *ability* to deftly obtain valuable cybersecurity information and to make good decisions on what to do with that information is paramount to the role of any CTI practitioner or leader. Consequently, we argue that phrases such as "cybersecurity intelligence" are often misused in practice and research. In raw form, a potential event is nothing but "data" that cannot become actionable "intelligence" without CTI practitioners' abilities to make good judgments as to what is a real threat, just how serious the threat is, and the best remedies for the threat now and in the future. Otherwise, a processed set of data easily becomes false negatives or false positives, resulting in "false intelligence" that can have catastrophic security and financial consequences. As an example, an internal host's access to an external malicious web site can be either flagged or blocked if deployed CTI has capacity to successfully correlate (in near real time) ongoing traffic and trusted external threat databases dynamically updated in the cyber space. Likewise, the needed abilities of a CTI practitioner are multifaceted, as the ability to correctly identify a threat alone is insufficient: A CTI practitioner may be able to correctly identify a true security threat in a sea of non-event data, but could then subsequently falsely classify the level of threat—causing a disproportionately excessive and expensive reaction or disproportionately too cautious of a reaction. Likewise, a practitioner may properly classify the level of a threat but not diagnose and apply the best security remedy for blunting the threat now and in the future.

These are no minor considerations because modern security organizations are awash in overwhelming external and internal event data that may or may not have to do with security. Crucially, in most cases, these are non-events; only a minority are actual true security threats; similar to checking for hidden bombs or guns at an airport checkpoint where there are few actual security threats. False positives in this context are a serious resource problem that can also distract attention to finding actual events; meanwhile, false negatives are catastrophic. Worse, there is no letup; while, efforts and resources are applied to one security event, many more may appear at any time and in any form, and they dynamically evolve to avoid known signatures. It is thus easy for an organization to be simply overwhelmed and then experience a serious breach because of the simultaneous and complex nature of the security events of which it simply cannot process adeptly and quickly enough. Knowing this fundamental principle, rogue actors and rogue states frequently use the brute-force approach of simply overwhelming the defenses of an organization in a virtual blitzkrieg (e.g., denial of service attacks, mass phishing), because many organization lack CTI practitioners and resources that provide the ability to process and deal with these approaches when in large volume.

Consequently, our theoretical assumptions and propositions around organizational CTI efforts applied to TTI go beyond mere training or giving CTI practitioners more "intelligence." These efforts alone will fail as they are at too superficial of a level for modern security threats. Instead, this is fundamentally about the need to foster a CTI practitioner's multi-faceted abilities so that they can deal with the disproportionate reality they work in of overwhelming events that need to be carefully processed to find a "true signal" of an actual threat. Again, sorting through the myriad of false positives, false negatives, and "true" signal is just the start. As a result, any limitation in any aspect of a CTI practitioner's or leader's abilities, represents an OrgSec vulnerability, as can be illustrated clearly by applying TTI: For example, a practitioner who has strong "book smarts" and "creativity" but lacks "street smarts" could be highly vulnerable to interpersonal human manipulation or deception. In security circles this is known as "social engineering" (cf. Hatfield, 2018; Mouton et al., 2016), which is a technique of choice of some of the best hackers and state agents because humans are prone to emotional decisions (e.g., people are easily persuaded by people they like) and multiple cognitive biases in decision making (Anderson, 2008). Likewise, a practitioner who has strong "street smarts" and "creativity" but lacks "book smarts" could be highly vulnerable to sophisticated techniques that require precise training, such as those involving encryption, multi-vector attacks, and

low-level hardware protocols—such as security vulnerabilities in industrial control systems like SCADA (cf. Cherdantseva et al., 2016). Finally, a practitioner who has strong "street smarts" and "book smarts" but has low "creativity," may be excellent at thwarting known attacks and techniques, but could be vulnerable to dynamic attacks for which there are no known signature and could lack the ability to forecast, predict, and pre-emptively plan for new attack possibilities. We formally explicate these points as follows.

First, the TTI provides a *comprehensive* map of the cultivated capabilities of a CTI practitioner necessary to undertake CTI tasks that can span the entire information-processing cycle across organizational ranks. CTI tasks demand a balanced understanding of security issues spanning strategic, operational, tactical, and technical levels (Maglaras et al., 2019; Tounsi and Rais, 2018).[6] To reflect these conditions, we needed a theory that defines a person's broad capability dimensions in the CTI context, and the TTI's analytical, context-response, and experiential intelligence lenses provide a solid theoretical basis for doing so.

Second, the TTI's emphasis on *dealing with the environments* enables us to derive personal capability dimensions that drive a CTI practitioner's success in facing ever-changing cyberthreat environments. In the TTI, a person's intelligence reflects his/her cognitive capacity for information processing to effectively deal with the environments. People become more successful by capitalizing on their strengths and correcting or compensating for their weaknesses in information-processing skills to adapt to environments. Similarly, CTI demands the capacity to scan dynamically and rapidly evolving threat environments and digest relevant threat information in time to successfully adapt to them.

Third, the TTI emphasizes *learnable intelligence*, underscoring the role of cognitive rather than psychometric attributes. It explains the success of a person from the perspective of his/her *cultivated and nurtured capability* in creating, adjusting, and adapting to the person's dynamic environment. The TTI is thus starkly different from traditional theories of human intelligence that focus on inborn capacities. According to the TTI, there is more to life success than being naturally smart or the generic ability to score high on IQ tests. Thus, two-thirds of the TTI is not about native 'smartness' but about a person's ability to grow capabilities through learning efforts (Sternberg et al., 1998). Similarly, a CTI practitioner needs to gain strength in the three capacity domains to keep up with ever-shifting threat landscapes (Wernick, 2018).

4.2. Explicating the TTI

In this section, we summarize the TTI's structure to lay a groundwork for deriving the capability dimensions for successful CTI at the individual level, which would then have a positive influence at the organizational level. The TTI maintains that human intelligence comprises three distinct but interrelated information-processing skills: *analytical or componential intelligence, practical or contextual intelligence*, and *experiential intelligence* (see Fig. 1). Per Sternberg (1999, 2003), individual success is achieved by balancing the three information-processing skills, which can be taught and cultivated.

The TTI defines *analytical intelligence* as one's ability to solve problems using comparison and analysis strategies that manipulate

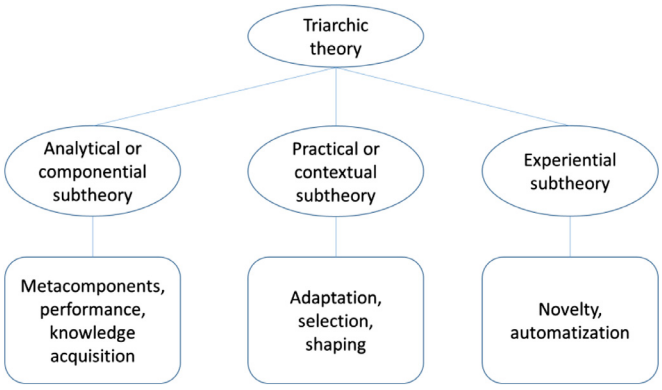

Fig. 1. Structural elements of the TTI.

the elements of a problem or the relationships among such elements. The TTI's *analytical sub-theory* proposes that the *meta, performance*, and *knowledge acquisition* components constitute a set of mental processes that underlie all aspects of intelligence. The *meta components*, or executive processes, enable a person to recognize the existence of a problem, define its nature, decide on a problem-solving strategy, monitor the solution, and evaluate the solution after the problem is resolved.

The *performance components* represent a person's ability to execute the instructions of meta components and thus the execution-level capacities of meta capabilities. The *knowledge-acquisition components* involve a person's ability to acquire problem-solving and/or declarative knowledge. The key aspects are *selective encoding*, which is the relevant information in the context of one's learning; *selective comparison*, which involves bringing old information to bear on new problems; and *selective combination*, which involves combining the selectively encoded and compared information into a single, insightful solution.

Practical or *contextual intelligence* represents a person's ability to *use* information-processing skills in accordance with the context of everyday problems. The *practical or contextual sub-theory* explains a person's *use* of information-processing skills to deal with a specific sociocultural environment. Aside from common sense and street smarts, this form of intelligence can be explained as "The ability of a person to adapt in an environment or change it accordingly to best suit the personal needs" (Shrestha, 2017). The TTI explains that people with high degree of practical intelligence can leverage three different approaches to do this: (1) *adapting* to an environment, (2) *shaping* an environment to make it more suitable to their own competence and goals, and (3) *selecting* existing or *finding* new environments that are better aligned with their skills, values, or desires. Balancing the three types of competence improves the chances for personal success, because doing so results in a better fit between people and their environments.

Experiential intelligence reflects a person's competence in bringing 'personal experience' to bear on situations that demand a solution. Thus, depending on the nature of the problem, a solution may be divergent or convergent or may demand either a novel solution or automated processing. The TTI's *experiential sub-theory* refers to a person's ability to perform a task with varying levels of experience or familiarity with that task. Here, experience is understood on a continuum from novel to highly familiar tasks or situations. In a *novel* situation, people have no prior experience and their information processing represents their ability to think within new conceptual systems and apply what they learn to already existing knowledge. In a highly familiar situation, complex verbal, mathematical, and other types of tasks can be executed with minimal deliberation, because many of the operations have become automatic.

[6] TTI is somewhat inadequate in modeling a person's capability dimensions related to a variety of information-processing tasks *in the organizational context*. First, the TTI dimension of *dealing with continuously changing environments* may not be critical at the middle or lower levels of organizations (e.g., data analysts, database administrators), because they are not high-level business decision-makers. Second, the *simultaneous* ownership of such diversified capabilities that spans organizational ranks may not be crucial for a person to effectively undertake assigned duties due to the division of roles.

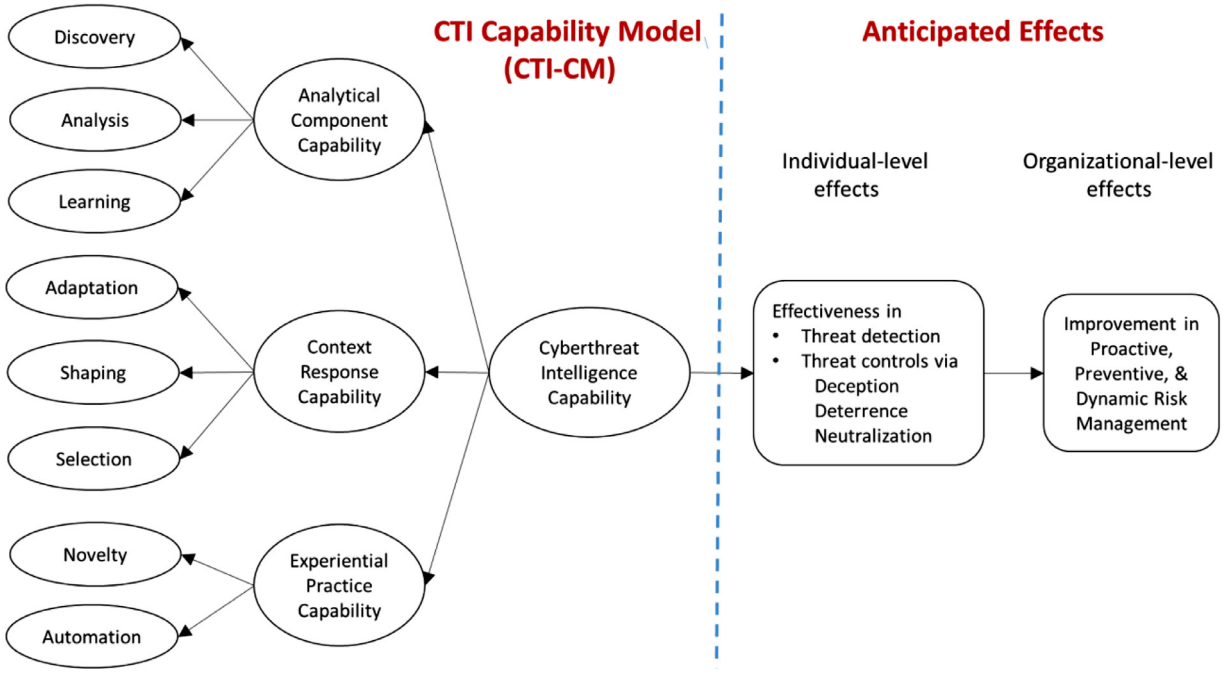

Fig. 2. The CTI capability model and anticipated effects.

5. Proposing the CTI capability model (CTI-CM)

We now propose the individual-level CTI-CM, a theoretical framework based on the TTI but heavily contextualized to CTI. The CTI-CM explains how practitioners can capitalize on their strengths while compensating for weaknesses in skills of leveraging information processing for threat detection and deploying countermeasures as responses. Based on the TTI, we define the CTI *capability* of a practitioner in terms of analytical component capability (ACC), contextual response capability (CRC), and experiential practice capability (EPC). ACC is an ability to *manage the analytical aspects* of CTI tasks. CRC represents a CTI practitioner's competence in *managing business and security environments* to respond to continuously evolving threats (Chen et al., 2012). EPC is a proficiency in *formulating solutions* (on the continuum from novel to automated) to threats of recognized severity. We expect the personal CTI capability to have many different effects at both the individual and organizational levels. Fig. 2 illustrates the CTI-CM and anticipated effects for individuals and organizations. Appendix Figure A1 further summarizes the three major components of the CTI-CM.

The three capability types differ in terms of their emphasis on CTI activities. A key assumption of the CTI-CM is that each of the capability dimensions has unequal strategic, operational, tactical, and technical elements. ACC involves primarily analytical competence in threat detection through various data gathering and analytical approaches. CRC, as a primarily strategic and operational competence, facilitates threat mitigation through the conception of different management approaches—such as adaptation, shaping, and selection strategies—in business and security environments. Dealing with functional (i.e., operational, tactical, and technical) competence, EPC facilitates the creation and operationalization of countermeasures at different levels of automation to deter and neutralize threats and/or to deceive attackers, drawing on experiential knowledge.

CTI practitioners need a balanced competence in handling both strategic and functional CTI issues. Thus, another key assumption of the CTI-CM is that they should strive for balance in cultivating competence in the three CTI dimensions and subdimensions, although the actual priority could vary according to their organizational rank and the arrangement of CTI tasks (Brown and Lee, 2019). It has been repeatedly emphasized that security professionals have both hard and soft skills in terms of products, processes, people, policy, and the like (e.g., Bagchi-Sen et al., 2010; Posey et al., 2014). This is the case because information security is no longer only a technological concern (Ransbotham and Mitra, 2009) but also a broad governance concern that involves even boards of directors (Andriole, 2009; Bart and Turel, 2010; Ernst and Young, 2014).

5.1. Analytical component capability (ACC)

CTI-driven threat detection is natively more proactive, anticipatory, and dynamic than traditional risk-management activities, which tend to be static, rigid, and more reactive, although the two orientations are complementary. The CTI-CM proposes that ACC consists of three distinct but interrelated capability dimensions that facilitate (1) discovery, (2) analysis, and (3) learning: The *discovery capability* consists of understanding the internal environment and external environment. The *analysis capability* is about establishing procedures, categorizing data sources, and deriving actionable intelligence. The *learning capability* can be described by discovery-based learning, knowledge acquisition, and learning through sharing.

5.1.1. Discovery capability dimension of the ACC

The primary activity of the *discovery* phase is to understand an organization's internal and external environments across the organizational levels to map CTI requirements. A fundamental condition of CTI initiatives is to understand CTI requirements to establish a clear focus of the CTI drive (Brown and Lee, 2019). Defining CTI requirements amounts to understanding the internal and external environments by identifying attractive targets such as intellectual property, customer data, and any other business operation–related information (Securosis, 2015) and thus to comprehending the system's and asset's vulnerabilities (Gschwandtner et al., 2018). The threat space is vast, and not all threats are relevant

to an organization. Threats become dangerous when they are designed to exploit a specific organization's system, software, or structural/configurational vulnerabilities. Thus, to lay the groundwork for the planning and development of a CTI program optimized to the needs of an organization, a CTI practitioner needs to understand its internal and external business environments.

5.1.1.1. Discovery of internal environment. This includes the understanding of organizational goals and missions, identifying critical assets, defining the relevant attack surface, and decomposing potential target systems (Muckin and Fitch, 2015; Shedden et al., 2016). Discovery involves both strategic and functional elements. At the strategic level, organizations struggle to effectively link business goals and objectives to the benefits of the CTI process (Townsend et al., 2013). Applying a strategic lens to a CTI program is instrumental not only to developing a program adequately tailored to a particular business but also to getting the leadership on board, obtaining necessary resources, and achieving better returns on investment (Townsend et al., 2013).

At the functional level, CTI practitioners develop an understanding of critical assets that aggressors may target in order to locate and correlate the related vulnerabilities and threats so they can conceptualize adequate countermeasures. Muckin and Fitch (2015) categorized critical assets in terms of business assets and security assets. The former category represents the data, functionality, intellectual property, and operational-information assets that are crucial to business missions, and the latter includes assets of special value to adversaries (i.e., "know your enemies"). This process is best served by developing a platform with which to manage asset profiles and configuration information of data, hardware, software, networks, and procedures. CTI practitioners can facilitate the creation of an asset rule base, which includes predetermined asset dependency; asset values as a function of confidentiality, availability, and integrity; and basic and specific asset rules tailored to asset values. The internal target surface can be defined in terms of any applications, systems, and environments that directly or indirectly communicate with or provide access to the assets that require protection. These applications, systems, and environments can be deconstructed and evaluated in terms of both managerial concerns regarding policies and controls and technical concerns such as communication protocols and application-programming interfaces.

In mapping vulnerable internal assets and their target surface, CTI practitioners recognize that serious threats originate not only from outsiders but also from insiders with malicious intent (Crossler et al., 2013; Willison et al., 2018). Organizational factors like excessive access privileges or weak data-management policies are associated with internal threats (Costa et al., 2016), and the need for internal CTI can be assessed through methods such as behavioral modeling (Cole, 2014; Santos et al., 2008). As such, the CTI effort at this stage overlaps substantially with traditional vulnerability- and risk-assessment and management practices (ISO, 2018; Webb et al., 2016). The vast majority of the requirements that enable adequate design of a CTI program can be fulfilled through the internal-environment discovery process.

5.1.1.2. Discovery of external environment. This external environment discovery is directly related to TTI's analytical or componential sub-theory as well as the "know your enemies." In this realm, CTI practitioners understand the external environment to become aware of external threats and threat entities at both the strategic and functional levels. This includes threat trends, threat actors, publicly shared vulnerabilities, intrusion or network attack vectors. tools used by threat actors, and other external factors, like movements in the Dark Web, that could affect the firm's services or products (Lutf, 2018). The profile information of adversaries includes malware and attack tools, command and control infrastructure, spear-phishing tactics, common targets, motivations, and profiting methods (Irwin, 2014). A strong grasp of the external-threat space, especially active threat elements, supports the development of threat-oriented and situational-awareness-driven data-gathering efforts tailored to organizational contexts and thus improves the overall effectiveness of a CTI program. Townsend et al. (2013) suggested that high-performing CTI programs have built profiles of serious cyberthreats and followed the evolution of attackers' tactics, techniques, and procedures.

5.1.2. Analysis capability dimension of the ACC

An organization's CTI analytical efforts can be tailored to its internal and external environments. The *analysis* phase involves activities related to identifying the internal and external sources of threat (and to a lesser degree, vulnerability[7]) information, establishing a data-gathering strategy, preprocessing, triaging, synthesizing data from various sources, and performing data analysis. The findings of the discovery stage are leveraged in the analysis phase. Without the inputs from the discovery stage, analysis-stage activities become disorganized, and scope management may fail, resulting in the gathering of either excessive or insufficient internal and external data. Very often, the analysis tasks mobilize advanced forms of statistical, machine-learning, visual, and heuristics methods to overcome the challenges of sifting through a large, messy volume of data (Cardenas et al., 2013; Los et al., 2014; Lowry et al., 2017; Navarro et al., 2018). Traditional data-monitoring and analysis techniques, often relying on the manual process, are inadequate in this respect, because they cannot keep up with the volume, variety, and messiness of source data (Suthaharan, 2014).

5.1.2.1. Procedure. The entire procedure of this phase can be guided by a high-level framework such as that developed by Holland (2013) or Gschwandtner et al. (2018). The framework of Holland (2013) includes descriptions of CTI requirements, internal and external gathering of data, processing of raw data, data analysis, and CTI dissemination. Each dimension of the high-level framework can be amplified in activities such as accompanying CTI processes, methods of accessing data sources, data-gathering and -sharing tools, raw-data processing, and analysis platforms that aggregate data sources (Los et al., 2014). Battle-tested approaches to modeling cyberthreats, such as the Cyber Kill Chain from practice (Kime, 2016; Pahi and Skopik, 2018; Sager, 2014) and the more recent and theoretically rich APT operation line model (APTOL) from academia (Ahmad et al., 2019), may be overlaid to dissect the high-level procedural framework (e.g., Holland, 2013) and enhance the structure of CTI analytical-modeling tasks.

5.1.2.2. Data sources. Several taxonomy schemes have been introduced as CTI data sources. Johnson et al. (2016) categorized them in terms of *internal* (e.g., live and log data from internal nodes) and *external* sources (e.g., intelligence-sharing communities, open source intelligence, product vendors, law-enforcement agencies). The data sources can be from open source intelligence (OSINT),

[7] Although "threat" and "vulnerability" are similar, in cybersecurity, they are treated as two distinct notions, because one can happen without the other even though many threats take advantage of the victim's vulnerabilities. For example, phishing is a threat, but its targets may or may not be vulnerable to phishing. To take another example, attackers may not exercise an "exploit" as a threat on a company even though it may have vulnerabilities (e.g., an unpatched operating system), simply because it is not an attractive target. Many conventional measures of *general readiness*, such as user training, software patch management, and regulation compliance, are intended to remove internal vulnerabilities that can be exploited by internal or external threats.

human intelligence (HUMINT), social media intelligence, technical intelligence, intelligence from the Deep Web and Dark Web, and counterintelligence (Holland, 2013). OSINT is intelligence gathered from publicly available sources such as public-information feeds and the comments of potential threat actors/hacking groups. HUMINT is collected from human resources or via personal contacts. Counterintelligence sources can be internal (e.g., honeypots, decoys), government provided (e.g., InfraGard, European Network and Information Security Agency), and industry related (e.g., Information Sharing and Analysis Centers). Los et al. (2014) categorized CTI sources in terms of intelligence about threat actors; intelligence obtained from the analysis of massive quantities of malware; targeted malware intelligence gained from the analysis of particular code samples; and reputation intelligence that can be provided through blacklisted IP addresses, URLs, and known command-and-control servers. CTI demands consumption of reliable threat data; thus, practitioners need to determine data sources that can be trusted (Wagner et al., 2018) and evaluate them in terms of service quality dimensions including relevance, timeliness, and accuracy (Qiang et al., 2018).

5.1.2.3. Deriving actionable intelligence. The threat-related data obtained from various internal and external sources become actionable intelligence through analysis (Brown et al., 2015). The analytical approaches may take the form of signatures, stateful analysis, ontologies, cross-layer analysis, and anomaly detection (Friedberg et al., 2018). Deriving actionable intelligence that helps manage uncertainties is no small feat. Among the forms of CTI recovered in this stage are threat vectors revealed through security exploits and vulnerabilities, the listing of germane threat-actor types, and adversary profiling. The development of threat profiles (Irwin, 2014) and threat models that illustrate how threats execute operations (Kime, 2016) is a key activity of this stage. Another core element of CTI involves internal assets (Friedberg et al., 2018), which includes triangulating and establishing correlations among assets, threats/attacks, controls, and vulnerabilities. The Pyramid of Pain model (Bianco, 2013; Harrington, 2014; Swart, 2015) not only suggests various intelligence types that can be obtained and their potential usefulness, but also indicates the difficulties of obtaining such intelligence.

A critical aspect of the analysis phase is assessing the degree of potential negative impact and confidence of the CTI. For this, existing models such as the confidence matrix may be used to support decision-making (Poputa-Clean, 2015; Townsend et al., 2013). The CTI with the higher impact and confidence will be taken more seriously, demanding immediate forms of remediation, such as blocking via the firewall and intrusion-prevention system. As for the threat-rating mechanisms, open standards such as the Common Vulnerability Scoring System and Common Weakness Scoring System can provide the basis for assessing the overall significance of threats. They are widely accepted standards designed to automate the security controls and also flexible as the *environments* of an organization can be contextualized. The combination of their quantitative scores and/or qualitative ranks can assess the impact, confidence, and overall risk of assets vulnerable to threats. A CTI program becomes more effective when threats are ranked and prioritized in a tiered model in terms of their severity and the potential targets of threat actors (Gschwandtner et al., 2018; Townsend et al., 2013).

CTI practitioners may assess the integrity and effectiveness of existing analytical models and methodologies and make continuous adjustments to augment the responsiveness of CTI efforts to the evolving landscape of cybersecurity threats (Poputa-Clean, 2015). None of the three key CTI inputs remains static, and threats are particularly dynamic and protean. Furthermore, as the technology horizon continues to expand, especially with the spread of mobile and Internet-of-things technologies, the attack surface continues to grow, necessitating flexibility in organization-level defense efforts.

5.1.3. Learning capability dimension of the ACC

To augment CTI capabilities, CTI practitioners need to be effective learners (Wernick, 2018) not only to foster individual- and organization-level CTI maturity but also to respond in a timely manner to evolving threats. For this, they should be conductive to both single-loop and double-loop learning to effectively tackle the tasks of both minor fixes/adjustments and complex problems (Baskerville et al., 2014). The TTI implies that personal learning is fundamental to shaping a successful career—thus the importance of a virtuous feedback loop in which CTI activities and subsequent learning continuously augment CTI capabilities. Active engagement in individual learning also can help turn a firm into a "cognitive enterprise" whose members continuously learn and create knowledge—an important condition for business success (Argote and Miron-Spektor, 2011). CTI capability cannot be purchased; it must be nurtured and built over time through knowledge acquisition and the consequent growth in maturity (Holland, 2013).

5.1.3.1. Learning in discovery and analysis phases. The importance of learning and knowledge acquisition during the *discovery* and *analysis* phases does not require extensive elaboration. In fact, the entire CTI life cycle, including post-analysis activities, contains learning components. For example, CTI practitioners can learn from past threats and incidents to implement controls that ensure the organization will not fall victim to them again. They can help an organization gradually advance CTI capabilities by promoting such continuous learning. Today's threats are highly dynamic in nature, propagating much faster than the threat information is revealed (Archer and Wick, 2013). When cyber tools have a short shelf life (Ferran, 2018), it makes it all the more important for CTI practitioners to be active and effective learners (Wernick, 2018). CTI practitioners can lead the advancement of learning through an effective feedback loop between *analytical-component, context-response*, and *experiential-practice* activities, which will boost their CTI competence.

Moreover, the personal learning capability likely supports the success of an organization's CTI program. Whereas organizations with mature threat/vulnerability life-cycle management processes reduce remediation time, the absence of such processes increases susceptibility by as much as four times (NTT Group, 2014). CTI initiatives inevitably run into problems of inaccuracy in the form of false positives and false negatives (Securosis, 2015). Thus, an element of CTI success is the filtering of irrelevant noise, because such noise will not only waste corporate resources but also distract frontline workers from actual dangers. Recent research has suggested that the risk-score and matrix approaches currently promoted by many organizations are flawed and that organizations should instead adopt simple probabilistic methods (Hubbard, 2009; Hubbard and Seiersen, 2016). Those with long-term CTI experience and knowledge can make sound judgments regarding which measurement approaches best address the inaccuracy problems in their organizational context.

5.1.3.2. Learning through sharing. Learning can be vastly amplified through active interorganizational CTI sharing, in which practitioners can play facilitating roles. CTI sharing provides several benefits to practitioners and organizations, including shared situational awareness (Webb et al., 2014, 2016), enhanced threat understanding, improved defensive agility, and better decision-making (Fransen and Kerkdijk, 2018; Johnson et al., 2016; Leitner et al., 2018; Skopik, 2018). National Institute of Standards & Technology

(NIST) Special Publication 800–53 (2017), an internationally popular risk-management framework, also emphasizes the importance of interfirm sharing to advancing a CTI program for state-of-the-practice controls. Other publications have underscored it as a precondition of the successful CTI drive, partly because the same cyberattacks often target multiple organizations in the same industry (Chismon and Ruks, 2015; Johnson et al., 2016; Muckin and Fitch, 2015; Ring, 2014; Townsend et al., 2013; Vance et al., 2015). Sillaber et al. (2018) proposed that interfirm CTI sharing can be characterized in terms of six different maturity stages: unstructured, monitoring, social sharing, automated data provision, full integration, and optimizing.

To facilitate CTI sharing, various architectural approaches have been proposed. CTI sharing can have centralized, peer-to-peer, or hybrid architecture, each of which has strengths and limitations (Fransen and Kerkdijk, 2018; Johnson et al., 2016). The peer-to-peer setup may be better than the client–server approach (Archer and Wick, 2013), because the former facilitates quicker CTI sharing, making it easier for defenders to deploy countermeasures in time.

Despite the multifaceted benefits and growing technical maturity of CTI sharing, there are significant behavioral, psychological, economic, legal, and cultural barriers to learning (Chismon and Ruks, 2015; Gal-Or and Ghose, 2005; Hsu et al., 2012; Ring, 2014; Schroers and Clifford, 2018). First, there appears to be a lack of motivation and social infrastructure. Often, constituents of organizations believe they have nothing worth sharing (Chismon and Ruks, 2015). Organizations may also lack an understanding of what information can be shared. Many firms are reluctant to share information because doing so has legal and privacy implications as well as potential risks, including negative publicity (Tounsi and Rais, 2018). Moreover, there are issues related to interfirm trust and the trustworthiness of CTI data sources, which include equity in CTI sharing, mistrust between industry rivals, and trustworthiness of data quality (Tounsi and Rais, 2018; Wagner et al., 2018). If practitioners can overcome these challenges, they can promote CTI sharing for collective learning. To do so, they can identify reliable and active CTI sources, evaluate available options, promote organizational buy-in, and enact the equitable sharing process to augment learning at the personal and organizational levels.

5.2. Contextual response capability (CRC)

CRC represents a practitioner's competence in identifying countermeasures with which to respond to various threats and threat environments, either passively or actively. From the counterintelligence perspective (Prunckun, 2014), activities in this stage are generally related to developing solutions, devising deceptions, deterring adversaries, and neutralizing threats. Depending on the nature of potential threats, an organization can be relatively aggressive in countering them with law enforcement or may resort to less confrontational measures. Much of the decision-making regarding the mode of interaction with the environment rests on situational factors, such as the expected severity and urgency of threats obtained during the analytical phase, the conception and assessment capability of strategies and tactics, and the practical ability to operationalize countermeasures to mitigate threats. Drawing on the TTI, we argue that practitioners can marshal three different approaches to fend off internal and external threats and adequately respond to threat environments: (1) *adaptation*, (2) *shaping*, and (3) *selection*.

5.2.1. Adaptation capability of the CRC

We define *adaptation capability* as a practitioner's ability to formulate both strategic and operational/functional CTI responses with which to adapt to internal and external threats and threat environments. Pragmatically, the external-threat environment and its threats are beyond the practitioner's control; thus, she/he has to find ways to actively adapt to them. In conceiving an adaptation strategy, information such as the profiling of grave threats obtained at the analysis phase becomes crucial (Townsend et al., 2013). Most technical measures of access, vulnerability, traffic, and audit controls (Ransbotham and Mitra, 2009) at the functional level are established in the spirit of adaptation. They include quick—preferably automated—threat remediation through the patch of just announced software vulnerability and the blocking of blacklisted IPs, domains, and malware hashes. Such measures are intended to counter threats or offset attack vectors while keeping the organizational and system environments largely intact.

CTI responses are therefore primarily intended to reinforce an organization's traditional adaptation capability for timely defense (Fonash and Schneck, 2015; Los et al., 2014). Ideally, CTI practitioners can strive to help their organization reach the adaptive tier of the NIST (2014) framework, the highest level of risk-management maturity. For adaptation, the Pyramid of Pain model (Bianco, 2013; Harrington, 2014; Swart, 2015) may aid the development of defensive measures an organization can deploy to cause more 'pain' to the aggressors and better negate their threats. For example, a spear phishing scheme with a Trojaned PDF file (Bianco, 2013) and a tool that establishes command and control belong to the pyramid's top layers and are thus difficult to identify. However, once discovered and adequately blocked, the tool's incapacitation will inflict more pain on the attacker. This is because developing a new exploit of similar capability is definitely harder than moving the same exploit from one blacklisted domain to another. At the operational/functional level, such adaptation capability is strengthened when actionable CTI is effectively tied to the defense system in an automated rather than manual fashion (Poputa-Clean, 2015).

5.2.2. Shaping capability of the CRC

Shaping capability is a CTI practitioner's competence in erecting barriers to threats through *structural changes* of the organizational and/or system environment. This capability is about reshaping the *environment*—both internal and external—such that it becomes less conducive to threats, and thus may demand his/her competence to challenge established beliefs or altering governing assumptions (Baskerville et al., 2014).

Perhaps the most practical avenue for *shaping* is the alteration of an organization's internal business and system environments to make them less prone to vulnerabilities and to increase the cost of attacks to perpetrators. Such restructuring may be achieved by reengineering business processes (e.g., Kokolakis et al., 2000), reforming security through fair and clear insider policies (e.g., Lowry et al., 2015), and better-protected information flow between trusted business partners. (D'aubeterre et al., 2008). Shaping facilitates a shift from an "as is" environment to a "to be" environment to offset threats (Vaughn, 1996) through the formation of a responsive risk-management process and an awareness-propelled integrated risk-management program (NIST, 2014). Among practical methods, the overarching strategic threat analysis (Townsend et al., 2013) can become a springboard for conceiving effective ways to shape internal environments. While growing their shaping capabilities, practitioners can use CTI not only to adaptively protect the current business and systems infrastructure but also to transform the internal environment into one that is more resistant to threats over the long term. Thus, the shaping initiatives tend to be more strategic, difficult, and resource intensive than those of adaptation, which tend to be more functional.

As for reshaping the external-threat environment, it is practically beyond the control of CTI practitioners at the moment. However, there are initiatives such as The Bright Internet (Lee, 2015) and source address validation (Liu et al., 2016), both of which aim to re-engineer current Internet technologies to fundamentally discourage cyberattacks. The Bright Internet (Lee, 2015) aims to

reduce cybercrimes by implementing preventive and preemptive cybersecurity solutions based on the principles of origin responsibility (e.g., message senders), deliverer responsibility (e.g., ISPs), traceable anonymity, and rule-based digital search warrants. Similarly, the source address validation aims to develop technology solutions to uncover or authenticate message sources when necessary (Liu et al., 2016). Although such initiatives could be game changers in the external-threat environment, their implementation requires massive joint efforts by industries, academia, and governments. Thus, any meaningful implementation of the technical and nontechnical measures is not expected to occur anytime soon. Besides, Internet service providers are now taking cybersecurity more seriously and becoming more proactive against security threats, because they are not immune from attacks (Rowe et al., 2011; Vratonjic et al., 2010). In fact, they are in a prime position to act as a first line of preventive and preemptive defense in partnership with government authorities. Despite the strong potential of this approach, it faces serious practical hurdles, including cost burden, policy issues, technical difficulties in detecting attacks, and liability issues (Lichtman and Posner, 2006; Rowe et al., 2011; Vratonjic et al., 2010).

5.2.3. Selection capability of the CRC

The *selection capability* of CTI practitioners is their competence in making adequate choices regarding countermeasures in light of recovered threat details, such as expected impact, urgency, and certainty. To make these choices, they conceive and weigh the options pertaining to the adaptation and shaping approaches. Many adaptation countermeasures are expected to be short-term solutions and thus less costly to implement than shaping countermeasures. The majority of the adaptation-oriented moves may be more effective in offsetting short-lived threats relatively quickly. By contrast, shaping-based moves may result in defense that better withstands more sophisticated threats, such as APTs, composite/blended attacks, and multistage attacks (Hutchins et al., 2011).

However, shaping approaches are expected to be slower and costlier in implementation than adaptation approaches. From this perspective, CTI practitioners can engage in choosing or balancing defense strategies and tactics and facilitate their implementation in support of other security professionals. Depending on the threat details, either an adaptation or shaping measure may be enough to neutralize the threat potential, whereas other situations may demand both for more sustained impact. The choice could have major organizational implications in terms of return on investment, successful risk management, and so on. For instance, imagine that CTI detects an unprecedented incident in which an enterprise's confidential information is being sold in the Dark Web's marketplace by a hacker (or an insider). A relatively quick *adaptation* to the threat would be finding and arresting the hacker in collaboration with the legal authority. However, this does not address the fundamental question of how the hacker was able to obtain the sensitive information. Depending on the threat's root cause, the firm may also need to *reshape* its technology infrastructure by reviewing and overhauling its current access control policies and systems (Anderson and Choobineh, 2008).

5.3. Experiential practice capability (EPC)

EPC involves applying cybersecurity experiences to forge defense barriers that range from novel (Wernick, 2018) to automated solutions. EPC thus reflects a practitioner's ability to deploy or implement actionable solutions to operationalize or act on CTI, primarily at the *functional* (e.g., operational, tactical, and technical) level. Threats have different levels of familiarity: on one end of the spectrum lie emergent or unfamiliar threats, and on the other lie familiar, routine, and recurring threats. Virtually all threats fall somewhere on the continuum between the two types. In deploying countermeasures, the anticipated impact (e.g., benign, medium, critical) and confidence (e.g., low, medium, high) of threats and the subsequent tolerance for false positives and/or false negatives (Poputa-Clean, 2015) are important factors.

To mitigate unfamiliar threats identified by CTI, security practitioners must devise creative solutions and execute them (Wernick, 2018). This may demand assumption-defying changes in the absence of the static relationship between the implicated risks and safeguards (Baskerville et al., 2014). The continuous evolution of the threat landscape, including adversaries' tactics, techniques, and procedures, forces defenders to develop competence in responding with original approaches. Depending on the threat situation, there may be no obvious answers, so practitioners should have the ability to conceive a response bolstered by experiential knowledge (Ernst and Young LLP 2014; Poputa-Clean, 2015). Experiential knowledge is expected to empower the development of original approaches that may go beyond current limitations in resources. Depending on the nature of the threat, there could be multiple courses of action with differing implications. In the case of the Dark Web incident, for example, practical experience could be crucial to remedy unprecedented acts. For instance, if an act was in the form of an outside intrusion (rather than an insider act), an analysis of the presumably massive data log gathered by various networked devices could be conducted to uncover the root source of the problem. Depending on the findings, different technical options, such as revamping data access control and monitoring, may be implemented to remove the vulnerabilities. More likely, these are not small tasks and CTI practitioners may need to closely work with other information security staff.

Conversely, threats of familiar types require CTI practitioners to facilitate automated information processing, integration, and response (Montesino et al., 2012; Samtani et al., 2017; Securosis, 2015). In integrating actionable CTI with a defense system, including blocking and alerting mechanisms, an organization's success depends strongly on its maturity in automating the relevant activities (Poputa-Clean, 2015). Automation, however, has certain drawbacks (Brown and Lee, 2019), especially due to the disruptive nature of false positives. Moreover, depending on the type of security control, certain controls, such as blacklisted domains, are better positioned for automation; however, according to Montesino et al. (2012), only about 30% of security controls are subject to automation. With rapid technology advancement, more controls should be subject to more automation by now; however, this basic statistic highlights fundamental challenges of automating security, and that not all of it can be fully automated. From the perspective of the five control dimensions of access, vulnerability, feature, traffic, and audit (Ransbotham and Mitra, 2009), the configuration-management aspect is relatively easy to automate, because configuration applies to defense systems like firewalls and intrusion detection systems that provide application program interfaces for automatic updates. By contrast, other control functions such as determining availability of software patches and finding their locations in cyberspace are not necessarily implemented in systems, making them more challenging to automate.

Despite these challenges, automating security functions in uncovering and attributing threats, assessing risk scores, identifying remediation, and deploying countermeasures offers huge benefits. It is especially effective when attacks and intrusions must be mitigated at machine speeds (Fonash and Schneck, 2015). Automation is a key success condition, because organizations with a CTI program are inundated with intelligence data, which poses challenges of data triage and analysis and operationalizing actionable CTI (Brown and Lee, 2019). Moreover, the automation of countermeasures not only introduces consistency into the anti-threat process but also frees practitioners to focus on value-adding tasks that

demand more attention, like threat-data analysis. Defense based on the automated interoperability between technical and nontechnical elements will boost rapid and consistent response (Fonash and Schneck, 2015). This produces compelling opportunities and challenges for practitioners with respect to strengthening the organization's defense architecture.

CTI Practitioners may facilitate automated information processing even for unstructured security functions by reapplying experiential knowledge. For example, CTI effectively augments the defense system's learning and thereby reduces repeated investigations triggered by similar false alarms (Bhatt et al., 2014). The advanced functions include the creation of a baseline for the environment's normal activity; prioritization of threats and alerts; management of overlaps in intelligence feeds; searchability through natural language processing of unstructured CTI data sources and a flexible scoring mechanism for urgency; and determination of CTI relevance from different perspectives, such as reliability, the attack surface, or the usefulness of intelligence feeds (Ghazi et al., 2018; Gschwandtner et al., 2018). Automation demands that both internal- and external-context information are factored into the integration process. A conceptual framework may guide the rapid and automated integration of both existing and future CTI. One example of such a framework is the Integrated Adaptive Cyber Defense conceptual architecture proposed by Fonash and Schneck (2015). Lakbabi et al. (2012) maintained that such an integrated environment can be created through a network access control architecture in which a central policy server serves the orchestration function.

6. Endogenous effects of CTI capability

As shown in Fig. 2, we propose that an individual's CTI capability will affect his/her CTI task performance and naturally the organization-level performance as well.

6.1. Individual-level effects

Enhanced CTI capability in the analytical component, context response, and experiential practice is expected to benefit practitioners in many ways. To frame the diverse effects, we turn to Prunckun's (2014) theory of counterintelligence. *Counterintelligence* represents organized activities "designed to prevent or thwart spying, intelligence gathering, and sabotage by an enemy or other foreign entity (source: dictionary.com)"; such goals closely resemble CTI objectives. Counterterrorism and law enforcement techniques are already widely used in the operational setting of cybersecurity (Shakarian, 2018). Thus, we insist that a counterintelligence theory can provide a high-level structure with which to frame the benefits of CTI.

According to Prunckun (2014), the objectives of counterintelligence are (1) *detection* of threats and threat sources; (2) *deterrence* of threats from adversaries; (3) *threat neutralization*, which blocks intelligence gathering or causes loss of interest, enthusiasm, or confidence in carrying out threat operations; and (4) *deception*, in which an adversary is misled about certain aspects of the target's operations. The four objectives can be grouped into (1) detecting threats and their sources and (2) controlling the threats via measures pertaining to deterrence, neutralization, and deception. Thus, we expect that a person's CTI capability in the analytical component, context response, and experiential practice strengthens his/her overall competence for *detecting threats* and *devising & deploying threat control measures* to facilitate *deterrence, neutralization*, and *deception*. We briefly discuss each of the outcomes below.

Threat detection: Timely detection of highly relevant threats, threat sources, and their specifics in terms of an adversary's goal, strategy, execution plan, and method have become crucial in deploying countermeasures. A practitioner's CTI capability will certainly facilitate his/her tasks of detecting actionable threats or threat indicators.

Threat deterrence: A well-rounded CTI capability is expected to strengthen a practitioner's ability to conceive deterrence measures. This will better prevent adversaries from attempting attacks by impressing upon them that the attack's high cost or risk outweighs its potential benefits (Davis, 2014). Because it is inherently difficult to hold external attackers accountable, deterrence approaches are expected to be more effective for internal than for external threats. Regarding external threats, scholarly efforts such as Bright Internet (Lee, 2015) and source address validation (Liu et al., 2016) have been proposed as deterrence solutions. However, they have yet to gain significant followings.

Threat neutralization: Threat neutralization blocks the adversary's' intelligence gathering or confidence in carrying out hostile operations. In cyberspace, surgically targeted countermeasures can be overlaid on traditional defense solutions including network firewalls and intrusion detection/prevention systems. For example, precision-guided filtering rules (e.g., blacklisted IPs, domains, malware hashes) bearing CTI findings can be dynamically added either automatically or manually to neutralize threats. As a further measure, CTI practitioners may engage in interfirm CTI sharing, introduce nontechnical anti-threat measures, and conceive preemptive solutions tailored to CTI-recovered threats and threat sources.

Threat deception: A more fine-grained understanding of threats may facilitate the conceptualization of deceptive moves against them. For example, using techniques (e.g., honeypots) and materials (e.g., falsified documents) of *deception* can create a false sense of confidence in attackers, increasing the likelihood that they will make a mistake or reveal their personal information (McFarland, 2015). The *tar pit*, a special type of honeypot, may be used to greatly decelerate an attack and frustrate the attacker (McFarland, 2015). Moreover, revealing fictional information, such as in the form of decoys, constitutes an essential part of the deception strategy. The same types of deception can be used for insider threats. Based on CTI, information with watermarks or realistic but fake data may be seeded to identify moles or leakers (Papadimitriou and Garcia-Molina, 2011; Tharaud et al., 2010).

6.2. Organization-level effects

CTI programs are expected to engender many short- and long-term organizational benefits (Fransen and Kerkdijk, 2018; Johnson et al., 2016; Leitner et al., 2018; Skopik, 2018). From the perspective of counterintelligence (Prunckun, 2014), individual CTI competence will more likely translate into the growth of organizational CTI capability and maturity in terms of the timely detection of threats and attacks (i.e., threats in action) and the effective conception and deployment of threat neutralization, deterrence, and deception measures. Such improvements will further the organization's 'defense-in-depth' and raise the financial and other costs of attacks (Iasiello, 2014). For example, when a targeted organization detects a vulnerability in its DBMS software asset through a CTI program and removes it in time (e.g., vulnerability to SQL injection), the adversary who attempts to steal the firm's valued data will forced to find another attack vector to compromise the hardened DBMS. As another example, CTI enables an organization to set up precision-guided defense against active ransomware (e.g., their attribution, preemptive alerts & training against attacker TTPs) on top of its general readiness measures (e.g., updating endpoint anti-virus programs, executing backups, conducting phishing training). This way, an organization's overall risk management becomes more proactive, preventive, and dynamic, driven by the *know-your-enemies* principle, which complements the conventional

defense orientation intended to improve general readiness via passive, static, and remedial solutions.

7. Discussion

Despite CTI's rapid ascendance and great potential to address current cybersecurity challenges, related OrgSec and behavioral security research has been seriously lagging, especially in our context where most of the CTI focus has been technical. Consequently, most of the extant work on CTI is found in CS and practitioner publications with a stronger emphasis on important technical issues. There are pressing research issues on many fronts with respect to unlocking CTI's potential (EY, 2016; Lee, 2017; Seals, 2017), and OrgSec and behavioral security researchers can contribute to addressing these issues. We argue that OrgSec researchers can contribute to CTI research because its success requires unique interactions between the technology artifacts, organizations, processes, and people. Among the nontechnical issues is the lack of theoretical frameworks than can guide CTI initiatives and capabilities and foster CTI efforts at the individual and organizational levels. In this theory-building and review manuscript, we proposed the CTI-CM, which outlines the key capabilities a practitioner may develop to effectively engage in CTI activities. The CTI-CM starts with a practitioner's cognitive capability. This capability is represented as a high-level abstraction, the first level of which comprises three interrelated domains of CTI capability—the analytical component, contextual response, and experiential practice—and the second level of which represents key aspects of the first-level capability domains.

Although CTI is as much an organizational as an individual capability, this manuscript focused on the individual level**.** Because no CTI-related theory has been established, we derived a capability model at the individual level to provide a starting founding. After all, an individual's CTI capacity becomes a critical building block for much of an organization's CTI capability, as illustrated in Fig. 2. Thus, understanding the CTI capability structure at the personal level is a natural approach to advancing CTI research. We anticipate that once a solidly defined individual capability model is in place, researchers can extend theoretical and empirical efforts to devise an organizational capability model and a maturity model relying on organization-level theories.

In terms of key contributions, *first*, because it is based on the TTI, the CTI-CM can best be described as a prescriptive theory of the key constructs that foster CTI capability. Such efforts, along with taxonomies (e.g., Posey et al., 2013), are highly important steps in theory building to set a foundation for the discourse and products of theory in an emerging area; otherwise, deeper theorizing and research in an emerging area is stymied (Hassan et al., 2019). Such efforts are particular crucial in organizational and behavioral security research involving CTI, because there are so many organizational-level, individual-level, and technology artifacts involved, that we assert that this kind of research is the ideal representation of what luminary and Nobel prize winner, Herbert A. Simon, termed as the "sciences of the artificial" (Simon, 2019): That is, these kinds of security problems are bounded by human involvement, bounded rationality, and dizzying array of artifacts humans create (e.g., hardware, software, AI, Big data, cloud computing, Internet of Things, cyberthreats, policies, procedures, politics, ethics, law, and organizations). Moreover, culture itself, adds an additional layer of consideration, because it can be individual-level, organizational-level, or national-level (Wiley et al., 2020).

Second, the CTI-CM can shed light on HR management related to cybersecurity, such as hiring and training. Despite the rapid embrace of CTI among medium and large organizations (Shackleford, 2018), little research has investigated the success conditions of CTI practitioners. Industry emphasizes the importance of a balance between CTI knowledge/skills and practical experience (Ahrend et al., 2016; Pickett, 2018). However, no formal frameworks or theories exist that can guide the search for practitioners with adequate qualifications or the design of training programs for existing employees. Our manuscript can provide a roadmap for the CTI training of current employees, which is especially pressing because recruiting qualified CTI experts is one of the most acute problems faced by industry (Shackleford, 2018).

Given these assumptions and contributions of the CTI-CM, we propose there are three natural corollaries that emerge that have further meaningful applications to practice and research:

First, every CTI practitioner and leader must actively work to increase their abilities in terms of security related "book smarts," "street smarts," and creativity; otherwise, they will be personally exploitable to security threats or vulnerable to not detecting them. These abilities are thus a form of organizational social capital that is not easily created, shared, or copied. We thus expect these abilities on an organizational level to contribute to long-term operational and strategic advantage. Likewise, developed on an individual level, we expect these capabilities will lead to greater marker value and increased career success of security practitioners that have them and use them wisely.

Second, despite the first corollary, few CTI practitioners and leaders will strongly possess all three of these TTI-based abilities; hence, carefully selected teams of CTI practitioners and leaders are paramount to OrgSec to ensure that collectively, an organization has high levels of TTI-based abilities in all crucial aspects of security. Consequently, having one person in charge of or leading security is a colossal mistake in large organizations. Namely, having a chief security officer who is the sole person with full responsible for security is a security vulnerability in of itself and an organizational governance failure. Although, we agree it is important to have a chief security officer in large organizations, from a governance perspective and to increase TTI-base abilities, there must be organizational-wide redundancy of equal levels of responsibility for security, including but not necessarily limited to the board of directors, the CEO, the chief operating officer (COO), and the chief finance officer (CFO), and the chief information officer (CIO).

Third, this leads to the final corollary: developing TTI-based abilities to thwart OrgSec threats is an organizational governance concern in which such abilities must be foster, supported, measured, and developed top-down and organization wide. Thus, redundancies in TTI-based abilities must also be fostered not just in organizational leadership, but in functional practice outside of security. This way, organizational insiders can help shore up some of the weakest links in security (cf. Hina et al., 2019; Posey et al., 2013), and help do so beyond the usual security policies around passwords and file sharing.

7.1. Limitations and future directions CTI-CM research

This section provides an overview of limitations and additional research ideas that can be explored on the basis of our preliminary theoretical work and around CTI in general.

First, it is crucial to emphasize that CTI itself is not an organizational security "silver bullet," and will certainly not resolve all organizational security issues (and is not intended to do so). This is particularly true of issues that are heavily behavioral, internal, strategic, or that involve external partners. CTI is simply a key piece of a bigger security governance puzzle. In fact, we lament that a current problem in organizational security is that we still have corporate boards who do not have enough technical, behavioral, and organizational knowledge of security to govern it properly. There also continues to be a trend of outsourcing and trusting key technical and organizational security governance decisions to lower committees or to lower roles—such that there is a lack of

overall communication, strategy, and integration of such decisions. CTI does not solve such organizational governance issues. Any time a key security governance piece is "outsourced" to a specific role or operational group, it opens up other blind spots and vulnerabilities. Communication, openness, integration, alignment with strategy, negotiation and sharing with partners are all things that are required for the most effective organizational governance—and CTI is not going to provide these. Instead, these elements would make CTI and other organizational security efforts dramatically more effective. Instead, CTI is a key piece in a broader organizational security governance that is core to organizational governance. Accordingly, we insist all aspects of security must be governed at the firm-level, from top down, starting with the Board and CEO. Thus, these are perhaps the most challenges issues to be addressed by future research and leading practice, and in that light, the CTI-CM can be leveraged as one of the pieces in this highly important discussion.

Second, and likewise in respect to greater organizational security governance, because it is based on the TTI, the CTI-CM can best be described as a prescriptive theory of the key constructs that foster CTI capability. Such efforts are particularly crucial in organizational and behavioral security research involving CTI, because there are so many organizational-level, individual-level, and technology artifacts involved. Again, CTI has a natural technical focus, and thus better integrating it with non-technical considerations (e.g., governance, strategy, communication, transparency) is a compelling challenge. Moreover, the next step is to theoretically and empirically elaborate, extend, contextualize, and test the CTI-CM's completeness, utility, and generalizability. For example, it is important to explore whether the three CTI capability domains furnish a comprehensive representation of the necessary components of a practitioner's CTI capability. Such efforts will also require substantial parallel efforts in developing psychometric and objective measures for CTI capability in organizational settings.

Third, given the broader consideration of organizational governance, considerations of "levels" should inspire multiple directions of future research. For example, researchers should investigate whether the second-level factors of each first-order domain are inclusive and distinct. Likewise, each of the second-level factors can be further deconstructed in terms of its structural elements and relationships with other elements. Moreover, additional CTI-relates security research needs to consider the implications at the individual-level of the practitioner, the group/department, the organization, extra-organizational/industry (cf. Skopik et al., 2016), and nation. This is aside from the fact that security researchers have long recognized that some of the most vexing technical issues of security are inherently multilevel, as well (e.g., Harn and Lin, 1990; McHugh and Thuraisingham, 1988). Modern security-related infrastructure is inherently even more multilevel because of platform-based business models mixed with IoT devices that are poorly designed for security (e.g., Coulter and Pan, 2018; Waraga et al., 2020), decentralized Blockchain technology (e.g., Hammi et al., 2018), Cloud computing (e.g., Modic et al., 2016), and so on. Likewise, aside from technical architecture, organizational and behavioral security research is also inherently multilevel and longitudinal; yet because of its complexity almost no multilevel longitudinal security research is presently conducted, with rare exception (cf. D'Arcy and Lowry, 2019).

Given the vexing complexity of security threats to actual organizations, we argue that security researchers must not shy away from the multilevel and longitudinal complexity, but instead embrace it as a compelling and profound research opportunity. As illustration, building on the idea of sharing intelligence problems with an outside organization for better resolution (cf. Skopik et al., 2016), Wagner et al. (2019) recently published a study on the importance of extra-organizational sharing of CTI information but pointed out the added issues in doing so because of laws and organizational impediments. That alone, provides three levels that must be addressed, at a minimum to solve the CTI-information sharing problem: organization, extra-organization, and nation/law.

Fourth, and related to the previous point, many of the empirical efforts will require that each construct be defined in its concept space, operationalized, and instrumented. Such conceptualization and measurement become inherently more complex and compelling when considering multilevel and longitudinal effects. Moreover, if firm-level constructs are used for endogenous variables, ecological validity will be a key research consideration in dealing with actual organizational conditions (Lowry et al., 2017). Thus, we suggest that researchers consider conducting not just traditional self-report studies, but also organizational, extra-organizational (cf. Wagner et al., 2019), and system secondary data surrogates that can be leveraged to triangulate, challenge, and validate the CTI-CM. Through an iterative process that will ideally involve a security-research community, the theoretical structure of the CTI-CM can be empirically validated and adjusted over time to become a reliable framework that can guide practitioners in growing their CTI competence. Ongoing empirical testing may identify constructs that should be dropped from the capability model.

Fifth, recall in the introduction, we set up the importance of CTI being an overall effort is to enable better decisions related to security threats and thus its information is "consumed" at different organizational levels for decision making, including at the strategic-, tactical- and operational levels. Building on the opportunity of these different decision-making levels in organizations, we expect there to be many organizational effects related to the CTI-CM, and thus further expound on the organizational-level research opportunities in this regard. In our model, organizational impact is framed as improvements in *proactive, preventive, and dynamic risk management*, in contrast to the traditional cybersecurity orientation of general readiness. Under the high-order framing, many lower-level consequence variables can be defined, and the majority of them should be directly and indirectly related to improved threat detection and threat control (Prunckun, 2014). Our literature review suggests that the expected improvements include learning about adversaries' methodologies, anticipatory and proactive problem-solving, timely decision-making and defensive agility, situational awareness, prioritized risk remediation, damage containment capability, collaborative problem-solving, and the maturity of CTI activities (Ahrend et al., 2016; Fransen and Kerkdijk, 2018; Gschwandtner et al., 2018; Johnson et al., 2016; Leitner et al., 2018; Lutf, 2018; Sillaber et al., 2018; Skopik, 2018; Tounsi and Rais, 2018; Webb et al., 2014, 2016). Brown and Lee (2019) reported that industry's current CTI focus is primarily on strategic analysis of the adversary, digital footprint or attack surface identification, understanding threat behaviors and adversary tactics, tradecraft, and procedure, and identifying indicators of compromise, such as threat IPs and domains. Related future research efforts should result in new theoretical models and subsequent empirical research.

Sixth, another related opportunity is to expand this work into the organizational "life-cycle." Organizations likely need to effectively perform all the activities related to the CTI-CM's three high-level components. In doing so, organizations will likely need to take a "life-cycle" approach to gradually advance CTI capability, while repeating the following generic steps in a continuous cycle: aligning CTI requirements with business requirements, gathering internal and external data according to the requirements, preprocessing raw data for subsequent analysis, analyzing data to derive actionable intelligence, and disseminating intelligence for timely decision-making. Like individual-level CTI capability, organizational CTI capability cannot be purchased from a vendor or simply amplified by subscribing to information services (Holland, 2013). This is

especially true because CTI available from service vendors is not necessarily tailored to the unique circumstance of a client organization (Samtani et al., 2017). The soft and hard CTI infrastructure—including internal and external data sources, data aggregation, enrichment, and analytics platforms (cf. Qamar et al., 2017), as well as response systems that enable the manual or automated actions necessary to mitigate threats (Los, et al., 2014)—need to be built up gradually. The CTI process could therefore be considered an effort to strengthen an organization's cognitive competence (Argote and Miron-Spektor, 2011; Yang, 2014). Because cybersecurity is highly specialized, a practitioner's CTI competence is expected to have a strong influence on advancing organizational CTI capability. Thus, we foresee multilevel modeling between a practitioner's individual capabilities and organizational outcomes.

Finally, future research should contextualize the importance of each capability dimension, because its importance could differ depending on the appointed position of a CTI practitioner. For example, the analytical capability may be central to the CTI analyst, but the capacity to plan and drive CTI-enabled defense and threat control may be more important to the CTI director (if an organization maintains a CTI team). Additional circumstantial factors may need to be factored in. One such factor is the CTI practitioner's scope of responsibility at an organization. Currently, a CTI practitioner's organizational role typically takes one of three forms: a single dedicated CTI practitioner, a member of a CTI team, or shared CTI responsibility on top of conventional duties (Brown and Lee, 2019; Shackleford, 2018). Finally, these considerations point to the importance of training related to CTI and adapting it to the needs of the practitioner audience.

8. Conclusion

As the technology horizon expands, especially with the spread of mobile and IoT technologies, the cybersecurity attack surface continues to swell, posing great challenges to organizations. To make matters worse, adversary actions in cyberspace (i.e., threats) inevitably propagate faster than the related information (i.e., threat alerts or feeds) (Archer and Wick, 2013). Although this conundrum makes it very difficult for defenders to keep up with threats, a well-developed CTI program can help narrow this gap. In the wake of the worsening situation, *knowing one's enemies* has not been a main orientation of risk management. However, Sun Tzu's lesson implies that, unless the traditional orientation of improving general readiness is balanced with activities tailored to the characteristics of specific enemies, success in risk management will remain low. The rapidly growing traction of CTI initiatives is a clear indication that a CTI program engineered for the timely deployment of precision-guided defense measures is becoming essential. This is especially true for medium-to-large enterprises, because security breaches can lead to staggering losses. Nevertheless, because the concepts of CTI initiatives and capabilities are nascent, there is little guidance on what it takes to be a successful practitioner. Accordingly, our paper proposes a prescriptive theoretical model, the CTI-CM, which explains and defines the structure of the CTI capability necessary for cybersecurity experts to succeed. This model not only provides a guide for practitioners but also establishes a theoretical basis for further construct development, measurement, theory building, and many other research opportunities for OrgSec and behavioral security scholars.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.cose.2020.101761.

References

Ahmad, A., Webb, J., Desouza, K.C., Boorman, J., 2019. Strategically-motivated advanced persistent threat: definition, process, tactics and a disinformation model of counterattack. Comput. Secur. 86 (September), 402–418.

Ahrend, J.M., Jirotka, M., Jones, K., 2016. On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit threat and defence knowledge. Cyber Situat. Aware. Data Anal. Assess. (CyberSA) 1–10.

Anderson, E.E., Choobineh, J., 2008. Enterprise information security strategies. Comput. Secur. 27 (1–2), 22–29.

Anderson, R.J., 2008. Security Engineering: A Guide to Building Dependable Distributed Systems (2nd ed.). Wiley, Indianapolis, IN.

Andriole, S.J., 2009. Boards of directors and technology governance: the surprising state of the practice. Commun. Assoc. Inf. Syst. 24 (1), 22.

Archer, D.W., Wick, A., 2013. Peer-to-peer enclaves for improving network defence. Technol. Innovat. Manage. Rev. 3 (7), 19–24.

Argote, L., Miron-Spektor, E., 2011. Organizational learning: from experience to knowledge. Organ. Sci. 22 (5), 1123–1137.

Bagchi-Sen, S., Rao, H.R., Upadhyaya, S.J., Chai, S., 2010. Women in cybersecurity: a study of career advancement. IT Prof. 12 (1), 24–31.

Bart, C., Turel, O., 2010. IT and the board of directors: an empirical investigation into the 'governance questions' Canadian board members ask about it. J. Inf. Syst. 24 (2), 147–172.

Baskerville, R., Spagnoletti, P., Kim, J., 2014. Incident-centered information security: managing a strategic balance between prevention and response. Inf. Manage. 51 (1), 138–151.

Bejtlich, R., 2013. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. Starch Press.

Bhatt, S., Manadhata, P., Zomlot, L., 2014. The operational role of security information and event management systems. IEEE Secur. Priv. 12 (5), 35–41.

Bianco D. (2013) The pyramid of pain. (accessed

Brown R., Lee R.M. (2019) The evolution of cyber threat intelligence (CTI): 2019 Sans CTI survey. (accessed April 7, 2019).

Brown, S., Gommers, J., Serrano, O., 2015. From cyber security information sharing to threat management. In: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security. ACM, pp. 43–49.

Cardenas, A.A., Manadhata, P.K., Rajan, S.P., 2013. Big data analytics for security. IEEE Secur. Priv. 11 (6), 74–76.

Chen, H., Chiang, R.H.L., Storey, V.C., 2012. Business intelligence and analytics: from big data to big impact. MIS Quart. 36 (4), 1165–1188.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., Stoddart, K., 2016. A review of cyber security risk assessment methods for SCADA systems. Comput. Secur. 56 (Feburary), 1–27.

Chismon D., Ruks M. (2015) Threat intelligence: collecting, analysing, evaluating. MWR infosecurity (accessed March 14, 2017).

Cole E. (2014) Insider threats in law enforcement. The sans institute (accessed March 17, 2017).

Costa, D.L., Albrethsen, M.J., Collins, M.L., Perl, S.J., Silowash, G.J., Spooner, D.L., 2016. An Insider Threat Indicator Ontology. Software Engineering Institute. Carnegie Mellon University (accessed March 14, 2017).

Coulter, R., Pan, L., 2018. Intelligent agents defending for an IoT world: a review. Comput. Secur. 73 (March), 439–458.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R., 2013. Future directions for behavioral information security research. Comput. Secur. 32 (February), 90–101.

D'aubeterre, F., Singh, R., Iyer, L., 2008. Secure activity resource coordination: empirical evidence of enhanced security awareness in designing secure business processes. Eur. J. Inf. Syst. 17 (5), 528–542.

D'Arcy, J., Lowry, P.B., 2019. Cognitive-affective drivers of employees' daily compliance with information security policies: a multilevel, longitudinal study. Inf. Syst. J. 29 (1), 43–69.

Davis, P.K., 2014. Toward theory for dissuasion (or deterrence) by denial: using simple cognitive models of the adversary to inform strategy. Rand National Security Research Division (NSRD). working paper (accessed November 12, 2016).

Dobran B. (2019) Terrifying ransomware statistics & facts you need to read. Phoenix-NAP global it services (accessed January 13, 2020).

Ernst & Young LLP (2014) Achieving resilience in the cyber ecosystem. (accessed December 11, 2015).

EY (2016) How do you find the criminals before they commit the cybercrime? A close look at cyber threat intelligence. (accessed December 29, 2017).

Ferran L. (2018) US hacker squads constantly on the attack in new cyberwar strategy. (accessed Feburary 11, 2019).

Fonash, P., Schneck, P., 2015. Cybersecurity: from months to milliseconds. Computer (Long Beach Calif) 48 (1), 42–50.

Fransen, F., Kerkdijk, R., 2018. Cyber threat intelligence sharing through national and sector-oriented communication. In: Skopik, F (Ed.), Collaborative Cyber Threat Intelligence, Detecting and Responding to Advanced Cyber-Attacks At the National Level. CRC Press, Boca Raton, FL, pp. 187–224.

Friedberg, I., Wurzenberger, M., Al Balushi, A., Kang, B., 2018. From monitoring, logging, and network analysis to threat intelligence extraction. In: Skopik, F (Ed.), Collaborative Cyber Threat Intelligence, Detecting and Responding to Advanced Cyber-Attacks At the National Level. CRC Press, Boca Raton, FL, pp. 69–128.

Gal-Or, E., Ghose, A., 2005. The economic incentives for sharing security information. Inf. Syst. Res. 16 (2), 186–208.

Ghazi, Y., Anwar, Z., Mumtaz, R., Saleem, S., Tahir, A., 2018. A supervised machine learning based approach for automatically extracting high-level threat intelligence from unstructured sources. 2018 Int. Conf. Front. Inf. Technol. (FIT) 129–134.

Gschwandtner, M., Demetz, L., Gander, M., Maier, R., 2018. Integrating threat intelligence to enhance an organization's information security management. 13th International Conference on Availability, Reliability and Security. ACM.

Hammi, M.T., Badis, H., Bellot, P., Serhrouchni, A., 2018. Bubbles of trust: a decentralized blockchain-based authentication system for IoT. Comput. Secur. 78, 126–142 (September).

Harn, L., Lin, H.-Y., 1990. A cryptographic key generation scheme for multilevel data security. Comput. Secur. 9 (6), 539–546.

Harrington, S.L., 2014. Cyber security active defense: playing with fire or sound risk management? Richmond J. Law Technol. 20, 12–14.

Hassan, N., Mathieson, L., Lowry, P.B., 2019. The process of is theorizing as a discursive practice. J. Inf. Technol. 34 (3), 198–220.

Hatfield, J.M., 2018. Social engineering in cybersecurity: the evolution of a concept. Comput. Secur. 73, 102–113 (March).

Heberlein, L.T., Dias, G.V., Levitt, K.N., Mukherjee, B., Wood, J., Wolber, D., 1990. A network security monitor. In: Research in Security and Privacy, 1990. Proceedings., 1990 IEEE Computer Society Symposium, pp. 296–304.

Hina, S., Dominic, D.D., Lowry, P.B., 2019. Institutional governance and protection motivation: theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. Comput. Secur. 87, 101594 (November):Article.

Holland, R., 2013. Five steps to build an effective TRI capability. Forrester Res. (accessed March 13, 2017).

Hsu, C., Lee, J.N., Straub, D.W., 2012. Institutional influences on information systems security innovations. Inf. Syst. Res. 23 (3–part–2), 918–939.

Hubbard, D.W., 2009. The Failure of Risk Management: Why It's Broken and How to Fix It. John Wiley & Sons, Hoboken, NJ.

Hubbard, D.W., Seiersen, R., 2016. How to Measure Anything in Cybersecurity Risk. John Wiley & Sons, Hoboken, NJ.

Hutchins, E.M., Cloppert, M.J., Amin, R.M., 2011. In: Ryan, J (Ed.). Leading Issues in Information Warfare & Security Research, pp. 80–106.

Iasiello, E., 2014. Is cyber deterrence an illusory course of action? J. Strateg. Secur. 7 (1), 54–67.

Irwin, S., 2014. Creating a Threat Profile For Your Organization. The SANS Institute (accessed March 17, 2017).

ISO, 2018. ISO/IEC 27005: 2018: Information Technology — Security Techniques — Information Security Risk Management.. International Organization for Standardization/International Electrotechnical Commission, Geneva, Switzerland.

Johnson, C., Badger, L., Waltermire, D., Snyder, J., Skorupka, C., 2016. Guide to Cyber Threat Information Sharing. National Institute of Standards and Technoloy (NIST), U.S. Department of Commerce (accessed March 13, 2017).

Khan, T., Alam, M., Akhunzada, A., Hur, A., Asif, M., Khan, M.K., 2019. Towards augmented proactive cyberthreat intelligence. J. Parallel. Distrib. Comput. 124, 47–59.

Kime, B.P., 2016. Threat Intelligence: Planning and Direction. The SANS Institute (accessed March 17, 2017).

Kokolakis, S., Demopoulos, A., Kiountouzis, E.A., 2000. The use of business process modelling in information systems security analysis and design. Inf. Manage. Comput. Secur. 8 (3), 107–116.

Kwon, J., Johnson, M.E., 2014. Proactive versus reactive security investments in the healthcare sector. MIS Quart. 38 (2), 451–471.

Lakbabi, A., Orhanou, G., El Hajji, S., 2012. Network access control technology—proposition to contain new security challenges. Int. J. Commun. Netw. Syst. Sci. 5 (8), 505–512.

Lee, J.K., 2015. Guest editorial: research framework for AIS grand vision of the bright ICT initiative. MIS Quart. 39 (2), iii–xii.

Lee R.M. (2017) Getting the nost out of cyber threat intelligence. *DarkReading: informationweek* informationweek (accessed Feburary 9, 2018).

Leitner, M., Pahi, T., Skopik, F., 2018. Situational awareness for strategic decision making on a national level. In: Skopik, F (Ed.), Collaborative Cyber Threat Intelligence, Detecting and Responding to Advanced Cyber-Attacks At the National Level. CRC Press, Boca Raton, FL, pp. 255–276.

Lichtman, D., Posner, E., 2006. Holding internet service providers accountable. Supreme Court Econ. Rev. 14 (2006), 221–259.

Liu, B., Bi, J., Zhou, Y., 2016. Source address validation in software defined networks. In: Proceedings of the 2016 ACM SIGCOMM Conference. ACM, pp. 595–596.

Los, R., Robinson, J., Clark, J., Brooks, R., Brown, W., 2014. Solution Primer: Threat Intelligence. Accuvant (accessed March 14, 2017).

Lowry, P.B., Dinev, T., Willison, R., 2017. Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda. Eur. J. Inf. Syst. 26 (6), 546–563.

Lowry, P.B., Posey, C., Bennett, R.J., Roberts, T.L., 2015. Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: an empirical study of the influence of counterfactual reasoning and organisational trust. Inf. Syst. J. 25 (3), 193–230.

Lutf, M., 2018. Threat intelligence sharing: a survey. J. Appl. Sci. Comput. 8 (11), 1811–1815.

Maglaras, L., Ferrag, M.A., Derhab, A., Mukherjee, M., Janicke, H., Rallis, S., 2019. Threats, protection and attribution of cyber-attacks on critical infrastructures. ICST Transact. 2019(forthcoming).

McFarland, B., 2015. Ethical Deception and Preemptive Deterrence in Network Security. SANS Institute (accessed April 26, 2017).

McHugh, J., Thuraisingham, B.M., 1988. Multilevel security issues in distributed database management systems. Comput. Secur. 7 (4), 387–396.

Modic, J., Trapero, R., Taha, A., Luna, J., Stopar, M., Suri, N., 2016. Novel efficient techniques for real-time cloud security assessment. Comput. Secur. 62 (September), 1–18.

Montesino, R., Fenz, S., Baluja, W., 2012. SIEM-based framework for security controls automation. Inf. Manage. Comput. Secur. 20 (4), 248–263.

Mouton, F., Leenen, L., Venter, H.S., 2016. Social engineering attack examples, templates and scenarios. Comput. Secur. 59 (June), 186–209.

Muckin, M., Fitch, S., 2015. A Threat-Driven Approach to Cyber Security. Lockheed Martin Corporation (accessed March 14, 2017).

Navarro, J., Deruyver, A., Parrend, P., 2018. A systematic survey on multi-step attack detection. Comput. Secur. 76 (July), 214–249.

NIST, 2014. Framework For Improving Critical Infrastructure Cybersecurity (Version 1.0). National Institute of Standards and Technology (NIST) (accessed December 12, 2016).

NTT Group, 2014. 2014 Global Threat Intelligence Report. NTT Innovation Institute (accessed.

Pahi, T., Skopik, F., 2018. A systemtic study and comparison of attack scenarios and involved threat actors. In: Skopik, F. (Ed.), Collaborative Cyber Threat Intelligence, Detecting and Responding to Advanced Cyber-Attacks At the National Level. CRC Press, Boca Raton, FL, pp. 19–68.

Papadimitriou, P., Garcia-Molina, H., 2011. Data leakage detection. IEEE Trans. Knowl. Data Eng. 23 (1), 51–63.

Pickett P. (2018) Cyber intelligence analyst: career overview. (accessed Feburary 16, 2019).

Poputa-Clean, P., 2015. Automated Defense Using TRI to Augment Security. The SANS Institute (accessed December 11, 2015).

Posey, C., Roberts, T.L., Lowry, P.B., Bennett, R.J., Courtney, J., 2013. Insiders' protection of organizational information assets: development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. MIS Quart. 37 (4), 1189–1210.

Posey, C., Roberts, T.L., Lowry, P.B., Hightower, R., 2014. Bridging the divide: a qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. Inf. Manage. 51 (5), 551–567.

Prunckun, H., 2014. Extending the theoretical structure of intelligence to counterintelligence. Salus J. 2 (2), 31–49.

Qamar, S., Anwar, Z., Rahman, M.A., Al-Shaer, E., Chu, B.-T., 2017. Data-driven analytics for cyber-threat intelligence and information sharing. Comput. Secur. 67, 35–58 June.

Qiang, L., Zhengwei, J., Zeming, Y., Baoxu, L., Xin, W., Yunan, Z., 2018. A quality evaluation method of cyber threat intelligence in user perspective. In: 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 269–276.

Ransbotham, S., Mitra, S., 2009. Choice and chance: a conceptual model of paths to information security compromise. Inf. Syst. Res. 20 (1), 121–139.

Ring, T., 2014. Threat intelligence: why people don't share. Comput. Fraud Secur. 2014 (3), 5–9.

Rowe, B., Wood, D., Reeves, D., Braun, F., 2011. Economic Analysis of ISP Provided Cyber Security Solutions. Institute for Homeland Security Solutions (accessed March 14, 2017).

Sager, T., 2014. Killing Advanced Threats in Their tracks: An Intelligent Approach to Attack Prevention. The SANS Institute (accessed March 14, 2017).

Samtani, S., Chinn, R., Chen Jr., H, JFN, 2017. Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. J. Manage. Inf. Syst. 34 (4), 1023–1053.

Santos Jr, E., Nguyen, H., Yu, F., Kim, K., Li, D., Wilkinson, J.T., Jacob, R., 2008. Intent-driven insider threat detection in intelligence analyses. In: Proceedings of the 2008 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, 02. IEEE Computer Society, pp. 345–349.

Schroers, J., Clifford, D., 2018. Legal implications of information sharing. In: Skopik, F. (Ed.), Collaborative Cyber Threat Intelligence, Detecting and Responding to Advanced Cyber-Attacks At the National Level. CRC Press, Boca Raton, FL, pp. 313–354.

Seals T. (2017) Threat intelligence strategies suffer from data overload. *Infosecurity Magazine.com* (accessed December 29, 2017).

Securosis (2015) Applied threat intelligence. (accessed December 11, 2015).

Shackleford D. (2018) CTI in security operations: SANS 2018 cyber threat intelligence survey. (accessed April 1, 2019).

Shakarian, P., 2018. Dark-Web cyber threat intelligence: from data to intelligence to prediction. Information 9 (305).

Shedden, P., Ahmad, A., Smith, W., Tscherning, H., Scheepers, R., 2016. Asset identification in information security risk assessment: a business practice approach. Commun. Assoc. Inf. Syst. 39 (Article 15).

Shedden, P., Smith, W., Scheepers, R., Ahmad, A., 2009. Towards a knowledge perspective in information security risk assessments—an illustrative case study. In: The 20th Australasian Conference on Information Systems, Melbourne, Australia. Monash University, pp. 74–84.
Shrestha, P., 2017. Triarchic theory of intelligence. Psychestudy (accessed November 9, 2019).
Sillaber, C., Sauerwein, C., Mussmann, A., Breu, R., 2018. Towards a maturity model for inter-organizational cyber threat intelligence sharing: a case study of stakeholders' expectations and willingness to share. Multikonferenz Wirtschaftsinformatik (accessed Feburary 1, 2019).
Simon, H.A., 2019. The Sciences of the Artificial, 3rd Edition MIT press, Cambridge, MA.
Skopik, F., 2018. Introduction. In: Skopik, F. (Ed.), Collaborative Cyber Threat Intelligence, Detecting and Responding to Advanced Cyber-Attacks At the National Level. CRC Press, Boca Raton, FL, pp. 1–18.
Skopik, F., Settanni, G., Fiedler, R., 2016. A problem shared is a problem halved: a survey on the dimensions of collective cyber defense through security information sharing. Comput. Secur. 60 (July), 154–176.
Sternberg, R.J., 1985. Beyond IQ: A Triarchic Theory of Intelligence. Cambridge University Press, Cambridge.
Sternberg, R.J., 1997. A triarchic view of giftedness: theory and practice. In: Coleangelo, N, Davis, GA (Eds.), Handbook of Gifted Education. Allyn and Bacon, Boston, MA, pp. 43–53.
Sternberg, R.J., 1999. The theory of successful intelligence. Rev. Gen. Psychol. 3 (4), 292–316.
Sternberg, R.J., 2003. A broad view of intelligence: the theory of successful intelligence. Consult. Psychol. J. 55 (3), 139–154.
Sternberg, R.J., Torff, B., Grigorenko, E., 1998. Teaching for successful intelligence raises school achievement. Phi Delta Kappan 79 (9), 667–669.
Stoll, C., 1988. Stalking the wily hacker. Commun. ACM 31 (5), 484–497.
Stoll, C., 2005. The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. Simon and Schuster, New York, NY.
Straub, D.W., Welke, R.J., 1998. Coping with systems risk: security planning models for management decision making. MIS Quart. 22 (4), 441–469.
Suthaharan, S., 2014. Big data classification: problems and challenges in network intrusion prediction with machine learning. ACM SIGMETRICS Perform. Evaluat. Rev. 41 (4), 70–73.
Swart, I.P., 2015. Pro-active Visualization of Cyber Security On a National Level: A South African Case Study. Rhodes University.
Tan, T.C., Ruighaver, A.B., Ahmad, A., 2010. Information security governance: when compliance becomes more important than security.. In: IFIP International Information Security Conference. Springer, Berlin, Heidelberg, pp. 55–67.
Tharaud, J., Wohlgemuth, S., Echizen, I., Sonehara, N., Muller, G., Lafourcade, P., 2010. Privacy by data provenance with digital watermarking-a proof-of-concept implementation for medical services with electronic health records. In: Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on. IEEE, pp. 510–513.
Tounsi, W., Rais, H., 2018. A survey on technical threat intelligence in the age of sophisticated cyber-attacks. Comput. Secur. 72 (January), 212–233.
Townsend, T., Ludwick, M., McAllister, J., Mellinger, A.O., Sereno, K.A., 2013. SEI Innovation Center Report: Cyber Intelligence Tradecraft Project: Summary of Key Findings. Carnegie-Mellon University, Pittsburgh PA Software Engineering Institute (accessed March 13, 2017).
Vance, A., Lowry, P.B., Wilson, D., 2015. Using trust and anonymity to expand the use of anonymizing systems that improve security across organizations and nations. Secur. J. 2015. doi:10.1057/sj.2015.22.
Vaughn, R.B., 1996. A practical approach to sufficient infosec. National Information System Security Conference.
Vinney C. (2019) Understanding the triarchic theory of intelligence. thoughtco. (accessed November 9, 2019).
Vratonjic, N., Manshaei, M.H., Raya, M., Hubaux, J.-P., 2010. ISPs and ad networks against botnet ad fraud. A T., B L., B J.S., eds. In: International Conference on Decision and Game Theory For Security (GameSec 2010), Lecture Notes in Computer Science, 6442. Springer, Berlin, Heidelberg, pp. 149–167.
Wagner, T.D., Mahbub, K., Palomar, E., Abdallah, A.E., 2019. Cyber threat intelligence sharing: survey and research directions. Comput. Secur. 87 (November):Article 101589.
Wagner, T.D., Palomar, E., Mahbub, K., Abdallah, A.E., 2018. A novel trust taxonomy for shared cyber threat intelligence. Secur. Commun. Netw. 2018 (Article ID 9634507).
Waraga, O.A., Bettayeb, M., Nasir, Q., Talib, M.A., 2020. Design and implementation of automated IoT security testbed. Comput. Secur. 88 (January):Article 101648.
Webb, J., Ahmad, A., Maynard, S.B., Shanks, G., 2014. A situation awareness model for information security risk management. Comput. Secur. 44, 1–15.
Webb, J., Ahmad, A., Maynard, S.B., Shanks, G., 2016. Foundations for an intelligence-driven information security risk-management system. J. Inf. Technol. Theory Appl. (JITTA) 17 (3), 25–51.
Wernick G. (2018) Why creativity is key to security. (accessed April 1, 2019).
Wiley, A., McCormac, A., Calic, D., 2020. More than the individual: examining the relationship between culture and information security awareness. Comput. Secur. 88 (January):Article: 101640.
Willison, R., Lowry, P.B., Paternoster, R., 2018. A tale of two deterrents: considering the role of absolute and restrictive deterrence in inspiring new directions in behavioral and organizational security. J. Assoc. Inf. Syst. 19 (12), 1187–1216.
Yang, N., 2014. The impact of the organizational innovation on strategic change: cognitive and learning perspectives. In: 2014 International Conference on Management Science & Engineering (ICMSE). IEEE, pp. 408–416.

Bongsik Shin, Ph.D: is a Professor of MIS at San Diego State University (SDSU). He earned a Ph.D. from the University of Arizona. For 20+ years, he has been teaching cybersecurity, enterprise network management, business intelligence (data warehousing & data mining, statistics), decision support systems, electronic commerce, and IT management & strategy both for undergraduate and graduate students. He has published 30+ research articles in such top quality journals as MIS Quarterly, IEEE Transactions Engineering Management, IEEE Transactions on Systems, Man and Cybernetics, Communications of the ACM, Journal of Association for Information Systems, European Journal of Information Systems, Journal of Management Information Systems, Information Systems Journal, Information & Management, and Decision Support Systems. His recent research efforts have been all about cybersecurity on such subjects as cyber threat intelligence and threat modeling. In 2017, he (along with 2 Co-PIs) was given a 3-year $310k grant from the Department of Defense to conduct research on "Actionable Intelligence-Oriented Cyber Threat Modeling" and develop a prototype system. Since 2019, his research to design an anti-ransomware solution has been supported by the Phase 1 and Phase 2 STTR grant from the US Air Force. Besides, funded by the US Navy, he has been involved in designing an augmented reality-powered equipment manintenance system.

Paul Benjamin Lowry, Ph.D: is the Suzanne Parker Thornhill Chair Professor and Eminent Scholar in Business Information Technology at the Pamplin College of Business at Virginia Tech, where he is the BIT Ph.D. and graduate programs director. He is a former tenured Full Professor at both City University of Hong Kong and The University of Hong Kong. He received his Ph.D. from the University of Arizona and an MBA from the Marriott School of Management. He has 233+ publications, including 130+ journal articles in Computers & Security, MIS Quarterly, Information Systems Research, J. of MIS, J. of the Association for Information Systems, Various IEEE Transactions, Information System J., European J. of Information Systems, Information & Management, Decision Support Systems, and others. In 2020, 2019, and 2018, he was recognized as the most productive scholar in the world for the top-6 information systems journals in the previous 5 years. He is a department editor at Decision Sciences J. He also is also on the senior editorial board at J. of Management Information Systems, and an SE at J. of the Association for Information Systems and Information System J., and an AE at the European J. of Information Systems. His research interests include (1) organizational and behavioral security and privacy; (2) online deviance, online harassment, and computer ethics; (3) HCI, social media, and gamification; and (4) business analytics, decision sciences, innovation, and supply chains.