Cybersecurity Knowledge Networks

Mark A. Clark, J. Alberto Espinosa, & Mariia Butina

This research is partially supported through the Kogod Cybersecurity Governance Center, Kogod School of Business, American University, Washington DC.

v.23 March 2018

EXECUTIVE SUMMARY

Cybersecurity, increasingly recognized as a critical issue for organizations seeking to protect vulnerable data, financial systems, and stakeholders, is a broad responsibility shared by individuals across multiple roles and organizational units. The knowledge and risk perspectives needed for effective cybersecurity governance will generally vary for members across organizational roles and units (e.g., technical, cybersecurity, management), organizational levels (e.g., board of directors, c-level, management, operational), and organizational boundaries (e.g., clients, outsourcing companies, suppliers), comprising multi-team networks. Understanding the areas of knowledge that are important for cybersecurity in organizations, and how that knowledge is distributed across roles and units in alignment with information system governance goals, is the purpose of this research.

This paper describes a knowledge network approach to understanding cybersecurity governance and its related outcomes. We outline a research program that assesses the configuration, fit, and effectiveness of knowledge within and across cybersecurity organizations with the goal of understanding how to achieve more effective cybersecurity practices in alignment with governamce goals of the organizationl and its information systems. In this article, we argue that effective cybersecurity practices require well organized collaboration rooted in knowledge sharing and social interaction, which can be effectively understood through the social network analytic perspective. We address specifically the human element of collaboration, which is a critical but understudied factor in existing cybersecurity research (Cavelty, 2010), building on prior research to develop quantitative and visual representations of knowledge relationships among key cybersecurity stakeholders in relation to multilevel performance outcomes (e.g., Espinosa & Clark, 2014).

Our exploration of how relevant knowledge is structured, distributed, aligned, and shared among the varied cybersecurity roles can help identify gaps, opportunities, and knowledge hubs that can be leveraged for increased coordination, effectiveness, and performance outcomes, including cybersecurity readiness, response, and resilience. We will build on theories of information system governance alignment (e.g, Tiwana, 2009) and test how various durable and fleeting team knowledge network structures (e.g., isolation, centralization, transitivity, reciprocity, clustering) interrelate to affect effective information sharing, communication and cybersecurity response within and across multiteam systems and organizations.

To introduce our approach to this cybersecurity knowledge network research, next we discuss cybersecurity knowledge domains and dimensions, then introduce the social network analysis approach as a way to understand whether and how knowledge sharing across key roles and organizational levels influence effective cybersecurity practices. We also describe the various phases of our research.

CYBERSECURITY KNOWLEDGE DIMENSIONS: CONTENT & STRUCTURE

The knowledge needed to successfully address cybersecurity issues can be understood in terms of both its ***content*** and its ***structure***, each of which have associated dimensions (Espinosa & Clark, 2011). Knowledge content can be classified in terms of knowledge domains. Consistent with team cognition research, we outline two domain types for organizational activity: ***taskwork*** (specialized and general understanding of the task), including the relevance of the knowledge to particular subtasks and incident phases; and ***teamwork*** (how individuals coordinate efforts across task, time, and units). Knowledge ***structure*** refers to the way in which content is distributed and organized among those involved (e.g., shared vs. unshared) and the ***durability*** of its relevance (fleeting vs. long-lasting) in relation to the task or team process. Below, we describe each of these knowledge dimensions with examples and applicability to organizational cybersecurity, with implications for organizational vulnerability if left unconsidered.

Content Domain: Taskwork and Teamwork

Taskwork knowledge (knowledge needed to carry out tasks) refers to the expertise and familiarity needed to accomplish the work-related goals. Taskwork knowledge may vary in its breadth, such as coverage of a number of disciplines or domains, and its depth, in terms of the extent of its specialization and detail. For instance, non-technical staff members of an organization may be required to understand cybersecurity practices such as password rules (e.g., length, characters, replacement schedule). Technical staffers, on the other hand, may need in-depth knowledge of how to program a system to enable two-factor authorization for system access. Understanding cybersecurity system effectiveness requires insights into aspects of taskwork knowledge that are needed for the various individuals filling roles across teams, units, organizations, and multi-team systems (inside or across organizations). While task knowledge domains can vary widely (e.g., technical, business, external environment, etc.), for cybersecurity research we can rely on domains articulated in popular cybersecurity frameworks like the one adopted by the National Institute of Standards and Technology, which articulated key cybersecurity functions – identify, protect, detect, respond and recover (NIST, 2014). Each of these functions rely on relevant functional knowledge categories (e.g., access management, access control) and sub-categories (e.g., information logs, data protection).

Teamwork knowledge (knowledge needed to collaborate with each other) refers to the familiarity about the expertise of others as well as to knowledge of team processes and member interaction preferences. It is sometimes referred to as ***transactive memory***, which is "knowing who knows what" (Wegner, 1986). For example, non-technical employees may know to report phishing attempts or other unusual cyber activity to experts on the cybersecurity response team, while a decision about purchasing a new anti-virus system might be referred both to technical experts and to the appropriate layer of management. Additionally, teamwork knowledge may be about processes such as preferred workhours and communication mode of a specific cyber response team member. Transactive memory combined with knowledge of how members interact or are likely to respond to situations is also referred to as ***shared mental models***. Together, considering specific aspects of taskwork and teamwork knowledge can help us

understand the "team within a team" which is most appropriate for completing particular tasks at the right time (Espinosa, Clark & Carter, 2018).

There will be particular taskwork and teamwork knowledge related to each phase of the work being completed. For instance, in the NIST "identify" and "detect" phases, relevant cybersecurity domains may include knowledge about policy adoption, preparation of systems, staff training, among other areas. In the NIST "respond" phase, relevant knowledge may be about response procedures, minimization tactics, gateway restrictions, and the like. NIST "recover" phase knowledge may be related to repair, policy and systems reformulation, retraining, and similar issues.

Team Knowledge Dimensions

Sharedness

Knowledge sharedness refers to two structural components: the knowledge held idiosyncratically by each individual that is not possessed by others, and the knowledge that is shared among members, which is important to coordinate and integrate task activities (Espinosa & Clark, 2011). Some aspects of task and team knowledge content are likely to be shared among the individuals and units involved, while other aspects will be unshared or individually held. Individuals will typically have unshared specialized knowledge, necessary for their role, which is important for efficient operation by minimizing unnecessary and costly duplication of resources and efforts. For instance, individuals within IT departments in organizations will typically have some specialized knowledge about technical systems which are not shared by non-technical staff, and even within IT staff there are likely to be differences in expertise. Members of IT departments could be expected to know about the cyber assets of their organization (i.e. computers, laptops, printers, wires, routers, sensors, etc.), how they operate, and how they are connected.

Individuals operating across roles and teams also benefit from a shared understanding of their responsibilities and how efforts will be coordinated, termed "shared knowledge." This knowledge, "an understanding among team members of the technologies and processes that affect their mutual performance" (Nelson & Cooprider, 1996), may be shared by all members of a unit, or just among a subset of members.

One example of shared cyber-related knowledge is the lexicon of an organizational unit or field. Those who work on cyber tasks requiring coordination should know and commonly define key cyber terms, especially when terminology is used in an idiosyncratic manner. Such common vocabulary is also referred to as "mutual knowledge" or "common ground" (Cramton 2001). The idea is that when two collaborators share knowledge and they know they share it, their communication will be better grounded on their shared vocabulary, leading to fewer episodes of miscommunication that will require communication repairs. For example, instead of the everyday meaning of "back door" as a backyard exit, teams should know that in cyber it means an undocumented way of gaining access to a program, online service or an entire computer system. Backdoors in cyber represent a large list of dangers from data theft and ransom to real-time surveillance or even remote control of an entire network. Therefore, a shared lexicon with knowledge of how to spot suspicious activity in an employee's computer (to be further reported

to an IT-department) is critical for a successful data breach identification and mitigation. This has practical consequences. According to an IBM security study, a backdoor is open for more than 2 months, on average, before it is usually detected (Ponemon, 2017).

Coupled with domain knowledge of taskwork and teamwork, described above, knowledge sharedness becomes an integral component of a "system [knowledge] directory" also termed "transactive memory" (Wegner, 1995). This knowledge of "who knows what" helps determine who to contact when access to others' individual knowledge is needed, and to assign task responsibilities to the appropriate specialists and coordinate task activities. Transactive memory is crucial for cybersecurity because it helps address the right question to the right person. For instance, having general shared familiarity about what a phishing email is will help to make an employee suspicious and forward a potentially malicious email to the IT department. The IT department in turn could analyze the threat and warn all the organizational levels of the possibility of a breach. A rise in general awareness is a rise in general cybersecurity governance effectiveness.

Durability

The usefulness of particular aspects of knowledge can be relatively ***durable*** or ***fleeting*** in terms of how long the knowledge will be relevant for a given task and coordination environment such as a team process). Durable knowledge is relevant to the task over long periods of time, such as for the entire duration of the task, and is increased "through experience with a task domain and by interacting and training with other team members" (Espinosa & Clark, 2011). For example, knowing the syntax of a programming language like Python is an example of durable knowledge – your knowledge of Python today will be as useful tomorrow. On the other hand, fleeting knowledge is situational. It is useful temporarily and only "immediately relevant for specific task situations" (Espinosa & Clark, 2011). Fleeting knowledge often loses relevance once the situation changes, such as the diminished need to recall early traffic conditions once that part of the trip is completed.

Both relatively durable and fleeting knowledge are important for a successful team performance. The degree to which this knowledge helps to understand the immediate environment is often termed "situation awareness," which has been defined as the understanding how aspects of environment such as task-related events and team member activity at a given point in time affect the operation of the task (Endsley, 1995). Endsley articulated the situational awareness is not just about being aware of something, but that it consists of three sequential components: (1) detecting a situation in the task environment; (2) developing an understanding of how this situation may affect the current task; and (3) being able to anticipate the state of the task going forward, given the current situation. In the cybersecurity context, these three components would map to: (1) threat identification; (2) risk assessment; and (3) response and recovery planning. Consistent with our discussion above, some fleeting knowledge is individual and some needs to be shared to work effectively as a coordinated unit (Wellens, 1993).

In cybersecurity, durable knowledge could be developed, for example, through cyber threat simulation games that may help to learn the sequence of actions in the event of a cyber crisis. Durable cyber knowledge will also be formed from previously experienced cyber incidents.

Fleeting cyber knowledge in the form of situational models is essential during a cyber incident to foster effective and timely information sharing and communication.

A NETWORK APPROACH TO MEASURE AND REPRESENT CYBERSECURITY TEAM KNOWLEDGE

Understanding the range of successful cybersecurity practices requires defining both high quality cybersecurity knowledge content and a well-organized network structure of the knowledge within an organization. We argue that knowledge work in collective collaboration is essentially a social phenomenon and, as such, it is best understood using a social network perspective. Social networks describe the relationships among a set of entities, such as friendships among a collection of people, where the fundamental unit of analysis is the "dyad" consisting of two "nodes" (e.g., persons in the friendship) connected by a "tie" (e.g., the friendship relationship, reciprocal or not). Nodes may be particularized to specific aspects of a person or thing, rather than just being the person as a whole, and a node may have differentiated ties with a variety of other nodes. Dyads may be aggregated to represent multiple aspects of nodes and ties, including network structures such as centralities, cliques, and isolates (Wasserman & Faust, 1994).

Thus, we use social network analytics to capture team knowledge across multiple dimensions, persons, and teams. Cyber knowledge networks are comprised of multiple "nodes", each representing a team member's knowledge content in a particular domain, which are linked through "ties" that represent various relationships among persons, dyads, and subgroups. These relationships can then be analyzed as network knowledge structures such as centralities (e.g., proportion of knowledge ties to other members), isolates (e.g., members with no knowledge ties to other members), and cliques (i.e., subgroups fully interconnected with each other in a given knowledge domain), which can help detect a team's ability to carry out tasks in ways that either individual or simple aggregate knowledge measures cannot.

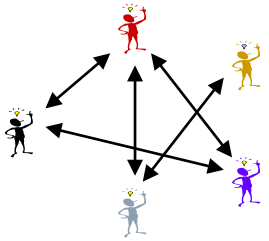
A network is typically represented as "sociomatrix" or a "sociogram." A sociomatrix (also termed "adjacency matrix") is a table where each cell represents the connection between two nodes, one node from the row of the cell, and one from its column. In the sociomatrix in Figure 1, if we presume that the nodes are people and the represented relationship is number of items answered similarly on a test, the relationship between node 1 and node 4 equals 3. A sociogram (also called "network graph") is a more visual representation of a network. As illustrated in Figure 2, each dot represents a node such as a team member, while the lines indicate the relationship between two nodes (e.g., their shared knowledge, in this case a bi-directional relationship as depicted by the two-headed arrow lines). Network graphs facilitate visual analysis, making evident aspects of the network knowledge structure that may be difficult to uncover with simpler measures.

The link connecting persons, denoted by the number value of the cell in the sociomatrix or the line in the sociogram, will represent the cyber-related knowledge relationship between these two persons. Networks can also be "valued" (i.e., "weighted") or "dichotomized". In a valued network the ties have a weighted attribute representing the strength of the relationship. In contrast "binary" or "dichotomized" networks contain a tie between actors if the relationship value exceeds a certain threshold deemed important – i.e., a network of 1's (if there is a tie) and

0's (if there are no ties). Sociomatrices and sociograms can each also be superimposed to represent more than one knowledge dimension at a time. For example, it could be useful to create a sociogram that represents the multiplicative interaction of three measures of knowledge: individual task knowledge, shared knowledge of particular domains, and knowledge of who knows what.

	1	2	3	4	5	6	7	8
1		0	0	3	8	8	8	3
2	0		0	3	8	8	8	3
3	0	0		3	8	8	8	3
4	3	3	3		3	3	3	0
5	8	8	8	3		0	0	3
6	8	8	8	3	0		0	3
7	8	8	8	3	0	0		3
8	3	3	3	0	3	3	3	

Figure 2. Sociogram



In sum, network analysis tools such as network graphs and adjacency matrices can be applied to the measurement of cybersecurity knowledge so as to account for multiple content and structure dimensions. Further, dyadic knowledge can be aggregated into team-level knowledge depictions without sacrificing valuable information about the distribution of the knowledge in individual members and subgroups. As such, this approach can measure and visually represent cybersecurity-related knowledge resident in multiple levels and units, within and across organizations, tracking the emergence, development and operation of cybersecurity knowledge networks.

CYBERSECURITY KNOWLEDGE ACROSS ORGANIZATIONAL LEVELS AND MULTITEAM SYSTEMS

Emergency situations, whether large in scale like the series of hurricanes (Harvey, Irma, Jose) that hit the southeastern United States in 2017, or more routine but precarious traffic accidents, often require expert response teams from multiple agencies. These teams perform as a multiteam system (MTS), coordinated by their overarching shared goal of saving human lives, even while being attuned to the proximal goals of their own team (Mathieu et al., 2001; Marks et al., 2005). However, is this system of shared and unshared goals enough to predict MTS success? The fire fighters, emergency medical technicians, hospital emergency room teams, and recovery teams are likely to also depend on their network of shared and unshared knowledge – a common understanding to go along with their common goal.

The cybersecurity effectiveness of an organization may be similarly achieved by a set of individuals and teams coordinated through their shared goals and shared knowledge, internal and external to the organization, as a cybersecurity MTS. The knowledge and goals of such MTSs will not be uniformly distributed, however. Some components of these MTSs, such as information systems (IS) staff, may be highly coordinated with priorities toward cybersecurity identification, detection, protection, response, and recovery. These members will have knowledge and proximal goals related to their organizational roles, such as IS executives concerned with cyber strategy and risk roadmaps, IS managers who use best practices to build

systems aligned with organizational goals and regulatory requirements, IS technicians who implement cyber system tasks (NIST, 2014).

Others in the MTS may be less attuned to cybersecurity priorities, but are still influential in the establishing the integrity of the system. Members of board of directors and executive teams, for example, establish the overall organizational cyber strategy and priorities, evaluate available resources, and calculate overall risk tolerance. Non-technical managers throughout the organization structure their unit's work in support of organizational cybersecurity guidelines, while non-technical staff members comply with protocols and procedures which reduce the risk associated with each person's status as a potential gateway to the organization's information system. Individuals and teams who are nominally external to the organization, such as contractors and customers, may also need to follow established cybersecurity guidelines to ward against the actions of malicious cyber actors. Together, the individuals in these varied roles comprise cyber knowledge networks working together as a MTS to keep cybercriminals out of their cyber information systems.

To be successful in their cybersecurity mission, the knowledge network components of an MTS should contribute to a hierarchy that includes proximal and distal goals, which structures a shared understanding of what the TMS members are supposed to do, and how they are going to do it together. They should know who knows what and who is able to do which specific tasks. Multiteam systems are not defined by organizational borders; instead they are built on interdependencies (Marks at el. 2005) and knowledge networks (Lee et al., 2016). It is important to note that cybersecurity relies upon this informational transparency.

The success of knowledge network components are also expected to vary according to their alignment of the knowledge content with the purpose of the governance system. Specifically, governance of information systems may be divided in "decision control" (ratification and monitoring) versus "decision management (initation and implementation) activities (Tiwana, 2009; 2012). Knowledge distributed across organizational roles and units that is aligned with the system need, or intended purpose, of that role or unit can be expected to more closely achieve optimal cybersecurity.

Through our research approach, we seek to understand the optimal alignment of specific cybersecurity knowledge areas across: (a) key organizational roles (e.g., technical, cybersecurity, management); (b) organizational levels (e.g., board of directors, c-level, management, operational), (c) teams organized in multi-team systems; and (d) with external stakeholders (e.g., partners, outsourcing firms, customers, supply chain) that will produce the best cybersecurity outcomes.

CYBERSECURITY KNOWLEDGE NETWORKS RESEARCH APPROACH

To build understanding of cybersecurity knowledge networks in context, we will employ a structured mixed-method, longitudinal research design to assess knowledge content and structure across organizational levels, roles, and individuals comprising a MTS, sampling multiple organizations with varying vulnerability to cybersecurity breaches. We will test how various durable and fleeting team knowledge network structures (e.g., isolation, centralization,

transitivity, reciprocity, clustering) interrelate to affect effective information sharing, communication and cybersecurity response within and across multiteam systems and organizations.

To this end, we will collect data through semi-structured interviews and multiple field surveys via a configurable, web-based tool. Following this, we will develop measures such as relational assessments of durable and fleeting knowledge about both "taskwork" and "teamwork" across dyads before and during cybersecurity incidents. We will then use network analysis to model the collection of dyadic relationships and actor attributes into multiplex team knowledge networks. Finally, we will analyze the data and create visual depictions through computational social science modeling.

Our approach will also measure differentiated cybersecurity-related knowledge across phases of cybersecurity work, such as the NIST functions of identify, protect, detect, respond and recover. Pre-incident cybersecurity knowledge, related to the identify and protect functions, requires strong shared familiarity with teamwork (knowing who knows what) and taskwork (different aspects of the task) developed over time, along with training in shared durable knowledge (i.e. cyber culture and terminology) and individual-specific content knowledge (i.e. coding, vulnerabilities, hardware). Incident-related cybersecurity knowledge, related to detect and respond functions, requires strong fleeting knowledge (who does what in a crisis) in the form of situational behavioral models developed by experience and practice to foster timely information sharing and communication. Finally, after-incident cybersecurity knowledge, related to the recovery function, needs strong durable knowledge in both teamwork and taskwork to speed up the recovery process and draw proper conclusions from the incident. After-incident knowledge, if properly organized, will become a part of organizational knowledge developed through cyber incident experience. It could then help to reinforce pre-incident and incident phases in the future.

CONTRIBUTION TO PRACTICE

Knowledge networks are essential to understanding and improving cybersecurity operations within organizations across public and private sectors. Through measuring critical knowledge held by key stakeholders involved in cyber security - technical staff, middle managers, top managers and the board of directors – our research identifies gaps, opportunities, knowledge hubs, and information system alignment which can be leveraged for increased collaboration effectiveness, coordination, and performance. To accomplish this, our research measures specific knowledge content relationships among group members across various dimensions (e.g., content knowledge similarity, team member familiarity, task awareness), then uses network analysis to detect overlap, centrality, clusters, outliers, and potential boundary-spanners in alignment with system goals. These patterns can then be depicted visually and quantitatively to better understand how knowledge is organized and shared, and related to more effective cybersecurity outcomes.

REFERENCES

Cavelty, M. D. (2010). Cyber threats. *The Routledge Handbook of Security Studies*, 180.

Cooke, N. J., Salas, E., Cannon-Bowers, J. A., & Stout, R. J. (2000). Measuring team knowledge. *Human Factors, 42*, 151–173.

Cramton, C, D, (2001). The mutual knowledge problem and its consequences for dispersed collaboration. *Organization Science,* 12, 346-371.

Endsley, M. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors, 37*, 65‑84.

Espinosa, J. A., Clark, M. A., & Carter, D. R. (2018). Understanding shared familiarity and team performance through network analytics. *Proceedings of the 51th. Hawaii International Conference on System Sciences*. Kona, Hawaii: IEEE.

Espinosa, J. A., & Clark, M. A. (2011). Team knowledge: Dimensional structure and network representation. In E. Salas, S. M. Fiore, M.P. Letsky (Eds.), *Theories of team cognition: Cross-disciplinary perspectives* (pp. 289-313). New York: Routledge/Taylor & Francis Group.

Klimoski, R. J., & Mohammed, S. (1994). Team mental model: Construct or metaphor. *Journal of Management, 20*, 403–437.

Lee, S. J. C., Clark, M. A., Cox, J., Needles, B. M., Seigel, C., Akpan, J. A., Balasubramanian, B. A. (2016). Achieving coordinated care for complex cancer patients: A multi-team system approach. *Journal of Oncology Practice, 12*(11): 1029-1038.

Lewis, K. (2003). Measuring transactive memory systems in the field: Scale development and validation. *Journal of Applied Psychology, 88,* 587–604.

Marks, M.A., DeChurch, L.A., Mathieu, J.E., Panzer, F.J., Alonso, A. (2005). Teamwork in multiteam systems. *Journal of Applied Psychology,* Vol. 90, No. 5: 964–971.

Mathieu, J. E., Marks, M. A., & Zaccaro, S. J. (2001). Multi-team systems. In N. Anderson, D. Ones, H. K. Sinangil, & C. Viswesvaran (Eds.), *International handbook of work and organizational psychology* (pp. 289–313). London: Sage.

National Institute of Standards and Technology. (2014). Framework for improving critical infrastructure cybersecurity (Version 1.0). Retrieved from https://www.nist.gov/

Nelson, K. M., & Cooprider, J. G. (1996). The contribution of shared knowledge to IS group performance. *MIS Quarterly*, 20, 409–432.

Ponemon Institute. (2017). Cost of data breach study: Global overview. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

Rentsch, J. R., & Hall, R. J. (1994). Members of great teams think alike: A model of the effectiveness and schema similarity among team members. In M. M. Beyerlein & D. A. Johnson (Eds.), *Advances in interdisciplinary studies of work teams: Theories of self-managing work teams* (Vol. 1, pp. 223–261). Greenwich, CT: JAI Press.

Tiwana, A. (2009). Governance-knowledge fit in systems development projects. Information Systems Research, 20(2): 180-197.

Tiwana, A. (2012). Novelty-knowledge alignment: A theory of design convergence in systems development. Journal of Management Information Systems, 29(1): 15-52.

Wasserman, S., & Faust, K. (1994). Social Networks Analysis: Methods and Applications. Cambridge: Cambridge University Press.

Wegner, D. (1986). Transactive memory: A contemporary analysis of the group mind. In B. Mullen & G. Goethals (Eds.), *Theories of group behavior* (pp. 185–205). New York: Springer-Verlag.

Wegner, D. (1995). A computer network model of human transactive memory. *Social Cognition, 13*, 319–339.

Wellens, R. (1993). Group situation awareness and distributed decision-making: From military to civilian applications. In J. Castellan (Ed.), *Individual and group decision making: Current issues* (pp. 267‑291). Hillsdale, NJ: Lawrence Erlbaum Associates.

Zaccaro, S. J., Tetrick, L. E., & Dahl, R. (Eds.) (2016). The Psychosocial Dynamics of Cyber Security. Taylor & Francis/Routledge, New York.

ABOUT THE AUTHORS

Mark A. Clark, Ph.D., Associate Professor of Management, and Research Fellow, Kogod Cybersecurity Governance Center
Dr. Clark has expertise in high performing teams, leadership, diversity, and strategic human capital. His current research projects include work in team knowledge sharing, cybersecurity knowledge networks, team adaptation, multiteam system innovation, leadership, and stigmatized occupations. His field research engages a variety of organizations, including medical, design, and sports teams, high-tech companies, and entrepreneurial startups. Dr. Clark's work has been published in top academic outlets, including the *Academy of Management Journal*, *Journal of Applied Psychology*, *Human Resource Management*, *Human Factors*, and *Group Dynamics*. Before earning his Ph.D. at Arizona State University, Dr. Clark gained a variety of experiences in public and private sector management, as a consultant, program director, trainer, treatment specialist, and board member. He has been a visiting scholar at Instituto de Empresa (Madrid), ISCTE (Portugal), and Erasmus University (Rotterdam). At Kogod, Professor Clark's courses include "Leading High Performance Teams," "Leading Organizational Change," "Organization and Social Network Analysis," and "Strategic Human Capital Management."

J. Alberto Espinosa, Ph.D., Professor of Information Technology and Analytics, and Research Fellow, Kogod Cybersecurity Governance Center
Dr. Espinosa holds doctoral and master's degrees in informational systems from the Tepper School of Business at Carnegie Mellon University. He also earned an MBA and is a mechanical engineer. His research focuses on coordination and performance along global boundaries, particularly distance and time zones. His work has been published in leading scholarly journals, including *Management Science*; *Organizational Science*, *Information Systems Research*, and *Journal of Management Information Systems*, among others. He is a co-author of two books: "Obtaining Value from Big Data for Service Delivery," Kaisler, S. H., Armour, F., Espinosa, J. A., & Money, W., (2016). New York, NY, Business Expert Press, and "I'm Working While They're Sleeping: Time Zone Separation Challenges and Solutions," Carmel, E. and Espinosa, J. A. (2011), Nedder Stream Press.

Mariia Butina, M.A.
Mrs. Butina is an International Service Master's Degree candidate at American University School of International Service. She earned her B.A. in Political Science at Altai State University, Russia, and holds a dual-master's degree in Political Science and Education from the same school. She was a featured panelist at the 72APTLD conference in Tbilisi, Georgia on the future of IoT policy. Mrs. Butina serves as a Graduate Research Assistant in the Kogod School of Business. Her research is focused on the Internet of Things implications for cybersecurity and the human element in cybersecurity.