Issues in Information Systems
Volume 16, Issue II, pp. 246-254, 2015

INNOVATING KNOWLEDGE MANAGEMENT IN CYBER WARFARE

Quinn E. Lanzendorfer, Robert Morris University, qelst1@mail.rmu.edu
Scott C. Spangler, Robert Morris University, scsst295@mail.rmu.edu

ABSTRACT

Cyber warfare is the fifth and most recent domain of warfare. The use of information in warfare is as old as warfare itself. The challenges that cybersecurity organizations face are different than those of traditional warfare. Knowledge must be shared more dynamically by governments and industry partners. Cyber warfare's unique demands place more need for knowledge management and information sharing than the demands of traditional warfare. Cybersecurity organizations need to share knowledge amongst many organizations for real-time information about cyber attacks. Real-time knowledge management will be a critical success factor for sharing information between government and industry. Scholarly research on the practice of knowledge management and innovation in cybersecurity is vacuous. Using an expert participant base from government and industry research cybersecurity organizations, this paper analyzes the unique nature of cyber warfare and establishes a basis for research on the practice of knowledge management and the usage of innovation in cybersecurity organizations.

Keywords: Cyber Intelligence, Knowledge Management, Information Sharing, Innovation, Cyber Warfare

INTRODUCTION

Organizations strive to implement knowledge management systems in order to retain knowledge from past successes and failures. This collective non-competitive polling of information empowers communities of practice to journey from an "I" segregated institution to "we" community of practice.

Government organizations struggle with knowledge management more than corporate organizations [1]. Cybersecurity organizations have even more difficulties with knowledge management due to the speed of attacks and unique challenges [2]. Cyber warfare's unique demands require more need for knowledge management and information sharing than the demands of traditional warfare. Within the next ten years, cybersecurity organizations will need to share knowledge amongst many organizations for real-time information about cyber attacks. Real-time knowledge management will be a critical success factor for sharing information between government and industry.

RESEARCH QUESTIONS

RQ 1: Does the speed of information and unique demands of cyber warfare present more challenges to intelligence and operations than other types of warfare?

RQ 2: Is knowledge management in U.S. Government (USG) cybersecurity organizations a practice that is well-understood and consistently used?

RQ 3: Does U.S. industry's expertise and practice of knowledge management in cybersecurity services exceed the expertise and practice of knowledge management in USG cybersecurity organizations?

RQ 4: Is the innovation of cybersecurity products and services more difficult for industry partners than other types of products and services procured by the USG?

LITERATURE REVIEW

Cyberspace

Cyberspace is the fifth and newest domain of warfare [3]. The established domains of warfare that precede cyberspace are land, sea, air, and space [3]. Cyberspace is "composed of the now two billion computers existing, plus servers, routers, switches, fiber-optic cables, and wireless communications that allow critical infrastructures to

work" [3]. Cyberspace is "increasingly used as a theater of conflict as political, economic, and military conflicts are ever more often mirrored by a parallel campaign of hostile actions on the internet [sic]" [3].

Cyberspace lacks an identity when compared to the other domains of warfare. Thus, a cyberspace lacks a definite or common definition. Cyberspace "is not a physical place–it defies measurement in any physical dimension or time space continuum"[4]. Thus, the cyberspace domain of warfare lacks both physicality and identity [4]. For the sake of this research, cyberspace is defined as "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information–communication technologies" [5].

Information Warfare and Cyber Warfare

The Defense Science Board (DSB) defines cyber as term used to "address the components and systems that provide all digital information, including weapons/ battle management systems, information technology (IT) systems, hardware, processers, and software operating systems and applications, both standalone and embedded" [6]. The DSB defines resiliency as "the ability to provide acceptable operations despite disruption: natural or man-made, inadvertent or deliberate" [6].

The concepts of cyber warfare and information warfare are often used interchangeably. Both cyber warfare and information warfare are typically at the beginning stages of full-scale war [7]. Information warfare covers five key areas: psychological elements, military deception, operations security, computer network operations, and electronic warfare [3]. Information warfare is "any action to deny, exploit, corrupt or destroy the enemy's information and its functions; protecting ourselves against those actions and exploiting our own military information functions" [8]. Information warfare incorporates the psychological, social, and human factors, whereas cyber warfare is focused attacks and technologies [7]. Cyber warfare is "any act intended to compel an opponent to fulfill our national will, executed against the software controlling processes within an opponent's system" [8]. Cyber warfare includes the following modes of cyber attack: cyber infiltration, cyber manipulation, cyber assault, and cyber raid" [8].

The terms information warfare and network warfare are sometimes used interchangeably, as well. Information as a type of warfare was most prevalent in the Gulf War, yet the use of information in warfare is as old as warfare itself [9, 10]. The concept of a Digital Pearl Harbor started with then Secretary of Defense Leon Panetta in his address regarding the Stuxnet virus and acknowledgement of the future of cyber warfare. Panetta stated that " the next Pearl Harbor we confront could very well be a cyber-attack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems" [11]. This led to numerous articles, documentaries, and interviews using this concept of a Digital Pearl Harbor to address the new capabilities that technology and terrorism are moving towards. The documentary *We Are Legion,* on the other hand, opened the eyes of many to the Hacktivists' movement and their abilities and motives [12]. The Hacktivists are a group of computer hackers that use their talents towards activism, blackmail, and revolution. This transformation was significant, as there has never been a confluence of computer hacking and activism so powerful and threatening.

Intelligence and Operations

The use of intelligence encompasses military, political, economic, social, environmental, health, and cultural aspects [9]. Intelligence is defined as "the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information such as foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations" [13]. Cyber intelligence is "a cyber-discipline that exploits a number of information collection and analysis approaches to provide direction and decision to cyber commander and cyber operation units" [13]. Collecting intelligence from cyberspace is "any valuable information that we can collect from cyber operations environment" [13]. The effects of information operations may take longer than other types of intelligence to produce any sort of usefulness, which typically requires long-term commitments to effectively employ information [3].

For the sake of this research, it should be known that intelligence and operations in cyber and information warfare are a work in progress [9]. In creating successful organizational structures and enabling various levels of

information sharing, agencies need effective policies. The relationship between policy maker and intelligence officer has been historically less than harmonious in nature, but it is a necessary one. The relationship between these two "is not one of equals", yet policy and policy makers can exist without the intelligence community, but the opposite is not true" [9].

Successful intelligence requires that an organization has achieved a contextual comprehension of the information. The cultural differences in any organization, tribal community, or grouping can cause conflicts in measured outcomes of success. Sternberg describes these conflicts or differences through our own personal heuristics of representation [14]. The population then describes the degree of difference or acceptability through the "salient features of the process" [14].

Knowledge Management

Knowledge "derives from information as information derives from data" [15]. This ultimately means that information is the successful transformation into a state in which the data become useful. Furthermore, "If information is to become knowledge, humans must do virtually all the work" [15]. This transformation occurs through comparison of situations, the consequences and implications for decisions and actions, the connection of how information relates to knowledge, and how people converse what they think about information [15].

Knowledge can be divided into two types: tacit and explicit. Tacit knowledge is information, such as lived experiences, that have not been codified [16]. Tacit knowledge is typically spoken or acquired through experience, but the step to record this knowledge into a database, book, or transcription has not been made [15]. Such knowledge is seemingly useless to future generations that have not had these experiences. The tacit knowledge spiral of learn-teach-learn constructs a collaborative process. The collaborative or learned process spiral depends on a community of practice to assemble and disseminate the information [17].

Explicit knowledge, on the other hand, is knowledge that has been transformed into a recorded and codified state [15]. Future generations can educate themselves on the successes and failures of past generations when explicit knowledge is available on a subject. Information derived from sensors or other information gathering "resides in the information domain… this information is transformed into awareness and knowledge in the cognitive domain and forms of decisionmaking [sic]" [17]. This captured tacit information or data is–at the point of transformation–readily transcribed into easily disseminated knowledge. Prior to this transformation, the information was a silent core asset to the community of practice. Although the information is a central asset, it may have been invisible to the community and its collective knowledge pool. Thus, this transformed knowledge readily becomes a collaborative and non-competitive body of knowledge [18].

Once knowledge has been captured and codified, innovation becomes a new goal for expanding the value of that information. Innovation makes products, services, and situations better. Ideals are regarded as much as ideas, which creates and incentivizes innovation [19]. Nonaka describes the essence of innovation as "to re-create the world according to a particular vision or ideal" [19].

The information sharing initiatives and other information systems concepts discussed in this study have some emphasis on usefulness and management of knowledge flows. Management controls the central distribution of knowledge, information, or directives. The style in which managers transmit the knowledge can either stymie or instigate the community's success rate. General Omar Bradley, Alexander Graham Bell, Thomas Edison, and Edwin Land all provide examples of how a conceptual style of managerial leadership can be followed. Their methods allowed individuals to invest information into innovative concepts that were not previously comprehended by the community. The creative or conceptual freedom allowed for new technology and marketplace openings [20]. In the case of cybersecurity, knowledge is centralized within the community of practice.

Cybersecurity operations rely heavily on intelligence. This intelligence is formed by the collection of information and its codification and capture into knowledge. Furthermore, governments are demanding industry to be innovative more now than ever by placing contractual obligations on this subject. In short, successful knowledge creation is an output of effective information sharing. Information sharing "is critical because intellectual assets, unlike physical assets, increase in value with use. All learning and experience curves have this characteristic. A basic tenet of

communications theory states that a network's potential benefits grow exponentially as the nodes it can successfully interconnect expand numerically" [21].

METHODOLOGY

The sample for this study was 17 USG officials and industry research professionals that had strong backgrounds in various dimensions both of domestic and international cybersecurity areas. The participants represent USG and industry research cybersecurity organization. Their backgrounds included policy, strategy, research, industrial controls, program management, and knowledge management. The USG organizations represented are the Department of Homeland Security (DHS) and several Department of Defense agencies, which are the Defense Security Service (DSS), U.S. Cyber Command (USCYBERCOM), the National Defense University (NDU), and the Defense Acquisition University (DAU). The industry research cybersecurity organizations that participated in this study are the Carnegie Mellon University (CMU) Software Engineering Institute (SEI) Computer Emergency Response Team (CERT), the Johns Hopkins University (JHU) Applied Physics Lab (APL) Asymmetrical Operations Sector (AOS), and the Riverside Research Cyber Center of Excellence. Convenience sampling was used to recruit these participants, as these organizations presented representatives to whom they felt were best suited to participate in the study. Once the survey was complete, the participants were given to chance to view the results and respond with optional feedback.

DATA ANALYSIS

Demographics

The participants sampled in this study were purposefully chosen for their knowledge in cybersecurity. The unique blend of USG and industry research cybersecurity participants offered an extra dimension credibility, validity, and reliability to this study. The participants were asked demographic questions that dealt with their levels of experience, highest degree, degree specialization, current employment, current position, and if they had domestic or international experience. The average participant in this study had 25 years of experience, a Masters degree in a Computer Science or Information Systems field, works for an industry research firm, is a systems engineer, and has experience in both domestic and international cybersecurity operations. Table 1 lists the demographic questions asked and their results. The results in bold indicate the majority group of the responses.

Table 1. Demographic Analysis

Question	Results
Years of relevant experience (cumulative of military, civilian, and industry experience)	5 – 5.56% 10 – 0% 15 – 16.67% 20 – 5.56% **25 – 33.33%** 30 – 22.22% 35+ - 11.11%
Highest degree obtained	Bachelors – 11.11% **Masters – 50.00%** Doctorate – 33.33%
Specialization of highest degree	Business/ Management – 5.56% **Computer Science/ Information Systems – 50.00%** Engineering – 22.22% Humanities – 5.56% Law – 5.56% Policy – 0% Other – 5.56% (Math)

Current Employment	Government Civilian – 27.78% Government Military – 5.56% **Industry Research, Not for Profit and/ or Federally Funded Research & Development Center (FFRDC) – 61.11%**
Current Position	Policy – 5.56% Program Manager – 22.22% Professor – 11.11% Software Engineer – 0% **Systems Engineer – 33.33%** Other – 22.22% (Senior Advisor, Historian, Scientist, Systems Engineer/ Policy, Strategy/ Policy)
Your cybersecurity experience is:	Domestic: 35.29% International: 5.88% **Both: 52.94%** Neither: 5.88% (Historian)

Inherently-Unique Demands

Before the data collection commenced, the researchers' assumed that cyber warfare was a domain of warfare with inherently-unique demands. Research Question 1 asked the participants "Does the speed of information and unique demands of cyber warfare present more challenges to intelligence and operations than other types of warfare?". Table 2 analyzes the variance between Government and Industry Research participants. Despite having three Government participants respond with Not Sure responses and having two Industry Research participants Disagree, the results conclude that cybersecurity professionals face inherently-unique demands when conducting cyber operations and intelligence. Table 3 analyzes the same question with the variance between cybersecurity professionals with more than 25 years of experience and less than 25 years of experience. The Table 3 analysis reflects a very similar consensus, yet it also shows that the Disagree and Not Sure responses appear to be evenly distributed between the experience groups.

Table 2. Analysis of Inherently-Unique Demands by Professional Groups

	Agree	**Disagree**	**Not Sure**	***Total***
Government	3	0	3	6
Industry Research	9	2	0	11
Total	12	2	3	17

Table 3. Analysis of Inherently-Unique Demands by Experience Groups

	Agree	**Disagree**	**Not Sure**	***Total***
Less Than 25 Years	3	1	1	5
More Than 25 Years	9	1	2	12
Total	12	2	3	17

The analyses from these two tables conclude that cyber warfare does indeed have inherently-unique challenges. However, it would seem as if there are not *more* challenges. One participant remarked "Does cyber warfare present MORE challenges? No. Different, but similar". Another participant expanded the response with "cyber warfare's greatest challenge to intelligence and operations comes from relating intent, objective and means just like in traditional warfare." A final participant response concludes "New challenges, but not necessarily more. I&O (intelligence and operations) have addressed/solved many challenges in other domains, but that doesn't mean cyber has more. Cyber does have more capability/need gaps than other areas".

Knowledge Management

In general, the application of knowledge management in government organizations is weak. Typically, the unification of people, processes, and technology is even more challenging than what corporate organizations face. Research Question 2 asked the participants "Is knowledge management in USG cybersecurity organizations a practice that is well-understood and consistently used?" Table 4 analyzes the variance between Government and Industry Research participants. Overall, the results reflected 15 Disagree responses and only 2 Not Sure responses. No Agree responses were submitted. Both the Government and Industry Research participants are in strong consensus that knowledge management is not well-understood or consistently used. Table 5 analyzes the same question with the variance between cybersecurity professionals with more than 25 years of experience and less than 25 years of experience. The same consensus exists between the Government and Industry Research participants, with a very similar distribution.

Table 4. Analysis of Knowledge Management Usage by Professional Groups

	Disagree	**Not Sure**	***Total***
Government	5	1	6
Industry Research	10	1	11
Total	15	2	17

Table 5. Analysis of Knowledge Management Usage by Experience Groups

	Disagree	**Not Sure**	***Total***
Less Than 25 Years	4	1	5
More Than 25 Years	11	1	12
Total	15	2	17

Research Question 3 asked the participants "Does U.S. industry's expertise and practice of knowledge management in cybersecurity services exceed the expertise and practice of knowledge management in USG cybersecurity organizations?" While the consensus concluded with a commanding amount of Agree responses over Disagree responses, the participants did reflect a notable amount of Not Sure responses. Table 6 analyzes the variance between Government and Industry Research participants. More Government participants chose Not Sure by a narrow margin, while the Industry Research participants overwhelmingly responded with Agree. The results from Table 7 reflected a strong consensus from both those who had Less Than 25 Years of Experience and those who had More Than 25 Years of experience. The only two Disagree responses came from the More Than 25 Years demographic.

Table 6. Analysis of Knowledge Management Expertise by Professional Groups

	Agree	**Disagree**	**Not Sure**	***Total***
Government	2	1	3	6
Industry Research	8	1	2	11
Total	10	2	5	17

Table 7. Analysis of Knowledge Management Expertise by Experience Groups

	Agree	**Disagree**	**Not Sure**	***Total***
Less Than 25 Years	3	0	2	5
More Than 25 Years	7	2	3	12
Total	10	2	5	17

The analyses from these two research questions and four tables conclude that the participants from Government and Industry Research strongly disagree that knowledge management is well understood and consistently used in Government cybersecurity organizations. In fact, no one agreed. Also, there is a notable consensus that responded with Agree responses that industry exceeds the USG in knowledge management in cybersecurity. One participant responded "Corporate knowledge is a serious issue for the Government in cybersecurity. Industry steals anyone who becomes competent in cyber. Contractors, labs, and development centers become the corporate knowledge". Another participant responded "USG organizations often fail to assess who they support, where their product lines are, or how they will fit within the greater whole". A final participant concludes "Knowledge management is hard and it often delivers limited value, as typically implemented in many organizations… Incentives are lacking".

Innovation

Nonaka's explanation of innovation is that it is achieved when organizations restructure according to visions and ideals [19]. Research Question 4 asks "Is the innovation of cybersecurity products and services more difficult for industry partners than other types of products and services procured by the USG?" Overall, the participant consensus chose the Disagree response. Table 8 analyzes these responses by Government and Industry Research. All Government responses were Disagree, while the Industry Research participants were more diverse. The narrow consensus for the Industry Research participants was Not Sure. Table 9 analyzes these responses between the categories of cybersecurity professionals with Less Than 25 Years and cybersecurity professionals with More Than 25 Years. Both demographics responded with similar Disagree responses. Notably, no one from the Less Than 25 Years demographic chose Agree or Disagree, while the More Than 25 Years demographic responded with 5 responses each for Disagree and Not Sure. The only 2 Agree responses came from the More Than 25 Years demographic.

Table 8. Analysis of Innovation by Professional Groups

	Agree	**Disagree**	**Not Sure**	***Total***
Government	0	6	0	6
Industry Research	2	4	5	11
Total	2	10	5	17

Table 9. Analysis of Innovation by Experience Groups

	Agree	**Disagree**	**Not Sure**	***Total***
Less Than 25 Years	0	5	0	5
More Than 25 Years	2	5	5	12
Total	2	10	5	17

The analysis from these two tables concludes that innovation truly is a new concept for U.S. cybersecurity organizations. One participant responded, "Innovation is hard… Not more so for cybersecurity." Another participant responded "The fact that operational data and information matters for demonstrating effectiveness and innovation makes this harder." The participant responses and the analysis from Table 8 and Table 9 conclude that innovation is difficult across the board. Nothing is uniquely different about innovation in cybersecurity.

CONCLUSIONS

Knowledge management systems in U.S. cybersecurity organizations are poorly implemented. These processes lack incentives for those who may benefit from them and the value of the knowledge gained has limited value to its users. Those who are responsible for knowledge management implementation and governance face challenges due to the amorphous structures and an overall lack of consistent usage resulting from the organizations' inconsistent visions. Government and Industry Research cybersecurity expert participants agree about the importance of having and utilizing knowledge management systems. The participants also agreed that the unique nature of the cyber warfare industry formulates a different set of issues that are not faced by regular communities of practice. These unique circumstances cause problems inside creating and sharing a knowledge management system. However, when asked if industry knowledge management practices superseded the USG, the Industry Research participants agreed that it did. Conversely, Government participants wavered on their answers and sided with an air of negativity and possibly caution.

In general, innovation is a vague term. Innovation seems to be a desirable state of being in most markets these days. The USG is no different. As the results of this study have uncovered, innovation truly is difficult. The innovation of cybersecurity products and services was not distinguished as a more difficult situation for industry partners than other types of products and services procured by the USG. The participants in this study agreed that innovations for industry stakeholders had no significant difference from that of the Government's. Interestingly, the industry participants demonstrated fewer concerns in utilizing and sharing knowledge within its ranks. Additionally, knowledge management practices were considered to be not well-understood and not consistently used, including situations where speed was necessary.

The inconsistency of knowledge management processes and the shortcomings of innovation in USG cybersecurity organizations seem to have a direct correlation with a lack of policy. Cybersecurity organizations in the U.S. have a unique problem with policy development. Executive Order (E.O.) 13636 *Improving Critical Infrastructure Cybersecurity* was signed by President Obama in February of 2013, which serves as the first relevant piece of legislation for cybersecurity in the U.S. As E.O. 13636 evolves, policy makers will have more opportunity to base knowledge management policies and procedures.

Further research in the field is needed to determine factors that cause conflict and degeneration of innovations. One possible conflict could be information hoarding. This long-time government and industry practice has repeatedly been observed throughout history. Further research is needed to understand how information hoarding conflicts with knowledge management constructions in the government sector.

REFERENCES

1. Lanzendorfer, Q.E. (2014). The Zachman framework: Enabling knowledge in the government information factory. *Issues in Information Systems*, Vol. 15, Issue 1, pp. 292-297 (2014). International Association of Computer and Information Systems. Retrieved from: http://iacis.org/iis/2014/56_iis_2014_292-297.pdf
2. Lanzendorfer, Q.E. (2015). *Enabling knowledge in the paradigm of international cyber intelligence*. Order Number 3708703. 2015 Ann Arbor, MI: ProQuest UMI.
3. Schreier, F (2015). On cyberwarfare. *Geneva Center for the Democratic Control of Armed Forces Horizon 2015 Working Paper No. 7*. Retrieved March 25, 2015 at: http://www.slideshare.net/KennethHardyCMIIB/on-cyberwarfarefred-schreierdcaf-2015-working-paper-no-7
4. Wingfield (2000) The law of information conflict: National security law in cyberspace. *Aegis Research Corp.*
5. Kuehl, D. (2009). From cyberspace to cyberpower: Defining the problem. *Cyberpower and National Security*, Washington D.C., National Defense University Press, Potomac Books,2009
6. DBS (2013). *Task force report: Resilient military systems and the advanced cyber threat.* Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.
7. Haig, Z. (2009). Connections between cyber warfare and information operations. *AARMS Security*, Vol. 8, No. 2 (2009) 329–337. Retrieved March 24, 2015 from: http://www.zmka.hu/docs/Volume8/Issue2/pdf/13haig.pdf
8. Marlatt, G. E. (2008, January 30). Information warfare and information operations (IW/ IO): A bibliography. *Naval Postgraduate School*. Retrieved December 18, 2013, from http://www.nps.edu/Library/Research/Bibliographies/index.html
9. Lowenthal, M. (2009). *Intelligence: From secrets to policy* (4.th ed.). Washington, DC: CQ Press.
10. McNeil, J. J. (2010). *Maturing international cooperation to address the cyberspace attack attribution problem*. Ann Arbor, MI: ProQuest UMI.
11. Lieberman, Collins, and Carper (2011). Avoiding a digital Pearl Harbor. *The Washington Post*, *1*, 1-2.
12. Knappenberger, B. (Director). (2012). *We are legion* [Documentary]. U.S.: Luminant Media.
13. Eom, J. (2014). Roles and responsibilities of cyber intelligence for cyber operations in cyberspace. *International Journal of Software Engineering and Its Applications*, Vol.8, No.9 (2014), pp.137-146.
14. Sternberg, R. (1997). *Successful Intelligence: How Practical and Creative Intelligence Determine Success in Life*. New York: Plume.
15. Davenport, T. H., & Prusak. (2000). *Working knowledge: how organizations manage what they know*. Boston, Mass.: Harvard Business School Press.
16. Polanyi, M., & Sen, A. (2009). *The tacit dimension*. Chicago; London: University of Chicago Press.
17. Perry, W.L., Moffat, J. (2004). Information sharing among military headquarters: The effects on decisionmaking. *RAND Corporation National Security Research Division*. Retrieved from http://www.rand.org/content/dam/rand/pubs/monographs/2004/RAND_MG226.pdf
18. Logan, D., King, J. & Fischer, H (2008). *Tribal leadership: Leveraging natural groups to build a thriving organization.* New York, NY: Harper Collins.
19. Nonaka (1998) The knowledge-creating company. *Harvard Business Review on Knowledge Management.* pp. 21-48
20. Rowe, A. & Mason, R. (1987). *Managing with Style: A guide to understanding assessing, and improving decision making.* London: Jossey-Bass Publisher.
21. Quinn, Anderson, and Finkelstein (1998). Managing professional intellect: making the most of the best. *Harvard Business Review on Knowledge Management.* pp. 181-205