https://doi.org/10.48009/3_iis_2016_39-47

INFORMATION WARFARE: THE CHALLENGE OF RELATING INTENT WITH TECHNOLOGY IN CYBER INTELLIGENCE

Quinn E. Lanzendorfer, D.Sc., Robert Morris University, qelst1@mail.rmu.edu
Scott C. Spangler, D.Sc., Middle Georgia State University, scott.spangler@mga.edu
Gary J. DeLorenzo, California University of Pennsylvania, delorenzo@calu.edu

ABSTRACT

The challenges that cybersecurity organizations face are different than those of traditional warfare. Many of these challenges hinge on the difficulties in relating the intent of cyber attacks with the outcome. The concept of information warfare used in the 1990's accounted for both the psychological and technical factors in digital warfare long before the term cyber became so widely used. Using qualitative and quantitative data collected from cybersecurity experts, this exploratory study examines the unique nature of cyber warfare, intelligence and operations, and the demands on government and industry partners. This study also establishes a framework for future research in the areas of cybersecurity, intelligence, and information warfare.

Keywords: Cyber Warfare, Information Warfare, Cybersecurity, Cyber Intelligence

INTRODUCTION

Arguably, the first palpable example of information warfare appears to be that which was used in World War I. However, the use of information in warfare is as old as warfare itself. Information warfare describes the act of obtaining and using an enemy's information or communications. This exploratory study will consider the concept of information warfare and seek to re-establish its relevance in today's cybersecurity vernacular. This study seeks to understand how cyber warfare has changed, challenged, or presented new demands on intelligence operations. The research will seek to understand how cybersecurity organizations collaborate and foster innovations. Finally, this study will attempt to determine if U.S. Government (USG) cybersecurity organizations are equipped to counter foreign intrusions.

RESEARCH QUESTIONS

RQ1: Have the speed of information and unique demands of cyber warfare presented more challenges to intelligence and operations than other types of warfare?

RQ2: Has U.S. industry's expertise in cybersecurity operations and intelligence exceeded the expertise of USG cybersecurity organizations?

RQ3: Have current collaborations between USG cybersecurity and cyber research organizations to foster innovation been effective?

RQ4: Is the industry workforce that performs services for USG cybersecurity organizations is ill-equipped to counter intrusions from foreign intelligence entities?

LITERATURE REVIEW

Cyberspace

Cyberspace is the fifth and most recent domain of warfare (Lanzendorfer, 2015; Schreier, 2015). The established domains of warfare that precede cyberspace are land, sea, air, and space (Schreier, 2015). 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" (Schreier, 2015, p. 10). 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]" (Schreier, 2015, p. 7). Cyberspace lacks an identity when compared to the other domains of warfare. Thus, cyberspace lacks a definite or common definition. Cyberspace "is not a physical place–it defies measurement in any physical dimension or time space continuum" (Wingfield, 2000, p. 17). The cyberspace domain of warfare lacks both physicality and identity (Wingfield, 2000). 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" (Kuehl, 2009, p. 4).

Cyber Warfare and Information Warfare

The Defense Science Board (DSB) defines cyber as a 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" ("Defense Science Board" [DSB], 2013, p. 2). The DSB defines resiliency as "the ability to provide acceptable operations despite disruption: natural or man-made, inadvertent or deliberate" (DSB, 2013, p. 2).

Warfare is revolutionary. Warfare has again innovated, changed directions, and became deeper ingrained in purpose. The concepts of cyber warfare and information warfare are sometimes used interchangeably. Both cyber warfare and information warfare are typically at the beginning stages of full-scale war (Haig, 2009). Literature traces a broad scope and intermingles the two theoretical terms. Ohlin, Govern, and Finkelstein (2015) proclaim that cyber is "specific technology way station between the sling and the hydrogen bomb" (p. 16). Schreier's (2015) definition of information warfare covers five key areas: psychological elements, military deception, operations security, computer network operations, and electronic warfare. 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" (Marlatt, 2008, p. 1). Information warfare incorporates the psychological, social, and human factors, whereas cyber warfare is focused attacks and technologies (Haig, 2009). 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" (Marlatt, 2008, p. 1). Cyber warfare includes the following modes of cyber attack: cyber infiltration, cyber manipulation, cyber assault, and cyber raid (Marlatt, 2008).

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 (Lowenthal, 2009; McNeil, 2010). 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" (Lieberman, Collins, and Carper, 2001, p. 1). 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 (Knappenberger, 2012). 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 (Lowenthal, 2009). 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" (Eom, 2014, p. 138). 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" (Eom, 2014, p. 137). Collecting intelligence from cyberspace is "any valuable information that we can collect from cyber operations environment" (Eom, 2014, p. 139). 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 (Schreier, 2015).

For the sake of this research, it should be known that intelligence and operations in cyber and information warfare are a work in progress (Marlatt, 2008). 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" (Lowenthal, 2009, p. 194).

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 (Sternberg, 1997). The population then describes the degree of difference or acceptability through the salient features of the process (Sternberg, 1997).

The U.S. Department of Defense (DoD) embraced the information age in the 1990s with the Net Centric Warfare (NCW) concept (Pattee, 2008). This concept was more than just an architectural and organizational concept, as NCW focus on cultural dimensions as a success factor. It treated the formation of an information culture as key ingredient for success (Pattee, 2008). Four domains of conflict comprised NCW, which are: physical, information, cognitive, and social (Pattee, 2008). The NCW theory paved the way for future initiatives by addressing cyber warfare as a domain of war and information as a culture (Pattee, 2008).

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 – 5.88% 15 – 17.65% 20 – 5.88% **25 – 35.29%** 30 – 23.53% 35+ - 11.76%
Highest degree obtained	Bachelors – 11.76% **Masters – 52.94%** Doctorate – 35.29%
Specialization of highest degree	Business/ Management – 5.88% **Computer Science/ Information Systems – 52.94%** Engineering – 23.53% Humanities – 5.88% Law – 5.88% Other – 5.88% (Math)
Current Employment	Government Civilian – 35.29% **Industry Research, Not for Profit and/ or Federally Funded Research & Development Center (FFRDC) – 64.71%**
Current Position	Policy – 5.88% Program Manager – 23.53% Professor – 11.76% **Systems Engineer – 35.29%** Other – 23.53% (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 Challenges

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 if the speed of information and unique demands of cyber warfare present more challenges to intelligence and operations than other types of warfare. Figure 1 illustrates the summary distribution of responses. Table 2 analyzes the variance between Government and Industry Research participants.

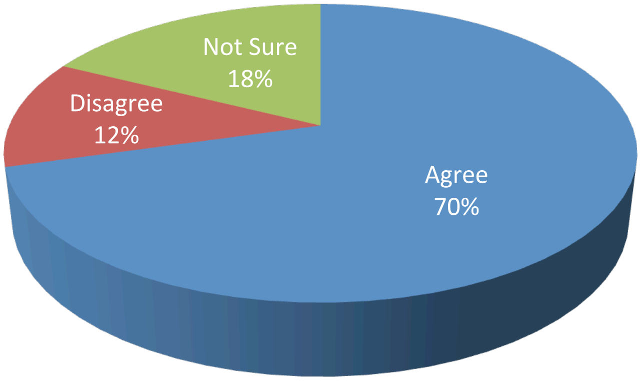

Figure 1. Pie Chart of Inherently-Unique Demands Responses

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

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. This analyses concludes 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".

Government and Industry Expertise

Research Question 2 asks the participants if U.S. industry's expertise in cybersecurity operations and intelligence exceeds the expertise of USG cybersecurity organizations. Figure 2 illustrates the summary distribution of responses. Table 3 analyzes the response by professional group.

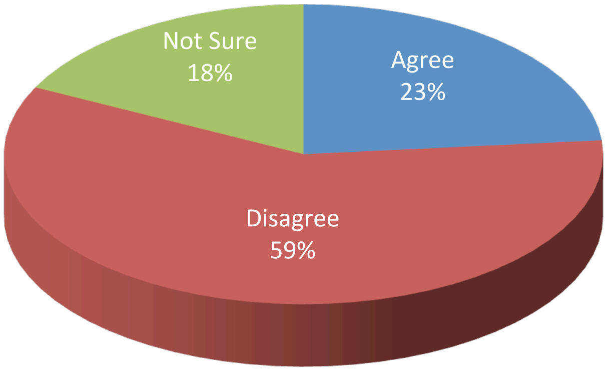

Figure 2. Pie Chart of Government and Industry Intelligence Experience Responses

Table 3. Analysis of Government and Industry Intelligence Experience by Professional Groups

	Agree	**Disagree**	**Not Sure**	**Total**
Government	1	4	1	6
Industry Research	3	6	2	11
Total	4	10	3	17

While the majority disagrees with this statement, there does appear to be notable agreement and uncertainty. One participant responded "Yes, in aggregate. However, the density is uneven in industry as well as government. Both have exceptional expertise, but neither have a monopoly". Another participant added "I work directly with industry, specifically Fortune 500 companies. They have established cybersecurity operations and intelligence that exceed those of the USG. They engage the USG as an additional information source. At times, we have joined industry in identifying a cyber incident and have jointly deployed measures to monitor and mitigate future activities. This is not the case when engaging small or mid-sized businesses.".

Cybersecurity and Research Collaborations

Research Question 3 asks the participants if current collaborations between USG cybersecurity and cyber research organizations to foster innovation have been effective. While the majority of the participants agreed, there does appear to be notable disagreement and uncertainty. Figure 3 illustrates the summary distribution of responses. Table 4 analyzes the response by professional group. One participant responded "Access to data for research is the real challenge. Classification restrictions are a bigger challenge."

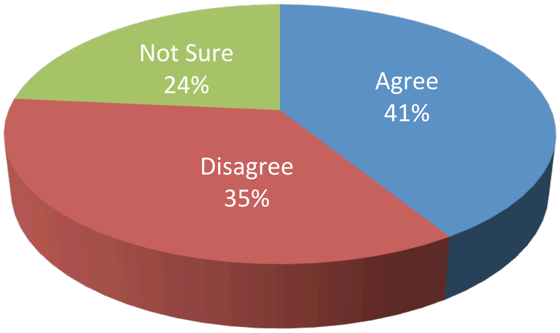

Figure 3. Pie Chart of Cybersecurity Collaboration and Innovation Responses

Table 4. Analysis of Cybersecurity Collaboration and Innovation by Professional Groups

	Agree	Disagree	Not Sure	Total
Government	4	2	0	6
Industry Research	3	4	4	11
Total	7	6	4	17

Domestic and International Expertise

Research Question 4 asked the participants if the current industry workforce that performs services for USG cybersecurity organizations is ill-equipped to counter intrusions from foreign intelligence entities. The majority of the participants were uncertain of this. Figure 1 illustrates the summary distribution of responses. Table 5 analyzes the response by professional group. One participant responded, "On the whole, yes. There are a few defense industrial base players that are fully capable of defending themselves."

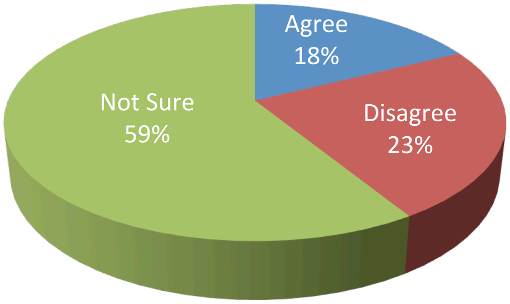

Figure 4. Pie Chart of Cybersecurity Workforce Knowledge of Foreign Intelligence Entities

Table 5. Analysis of the Cybersecurity Workforce Knowledge of Foreign Intelligence Entities

	Agree	**Disagree**	**Not Sure**	**Total**
Government	1	1	4	6
Industry Research	2	3	6	11
Total	3	4	10	17

CONCLUSIONS

Intelligence appears to be used tenuously in cyber warfare. A stronger linkage between information warfare and cyber warfare would likely benefit cybersecurity organizations more so than traditional warfare. The term information warfare seems to be old and out of style to those who work in cybersecurity. However, using the term cyber warfare doesn't account for all of what Schreier defines as information warfare, nor does it account for the cognitive and social dimensions proposed in Net Centric Warfare. Any focus on psychological, cognitive, social elements seems to be missing or perhaps an afterthought in today's cyber warfare. This lack of focus or importance on the psychological elements of information warfare serves a weak link. The importance of the intent behind cyber attacks appears to be an afterthought in many examples.

The participants provide evidence that cyber warfare does indeed offer new and unique challenges due to the speed of information and types of attack. The expertise of cyber operations and intelligence in U.S. industry does not exceed that possessed by U.S. Government cybersecurity organizations. For the most part, the participants disagreed that current collaborations to foster innovation have been effective. Finally, the majority of the participants were uncertain if U.S. industry are ill-equipped to counter attacks from foreign intelligence entities. This may very well be an indicator that intelligence is of low interest when compared to traditional warfare and other types of intelligence gathering, or that we are simply in the very early stages of this domain of war.

RECCOMENDATIONS FOR FUTURE WORK

The researchers' aim in conducting this study was to build a framework for future research in the areas of intelligence, information warfare, and cybersecurity. The recent nature of cybersecurity serves as a potential barrier for studying it accurately. Perhaps time will open these areas for analysis as cyber resiliency matures. The methodology used in this study is repeatable, and the findings serve as a basis for future research.

Perhaps a future study with a mixed methods approach to comparing the differences between domestic and foreign cyber attacks and how USG and industry could improve the knowledge bases and readiness of cleared cyber professionals. Also, a focus group study with USG cybersecurity professionals to discuss the difference between information warfare and cyber warfare, as well as the state of innovation in cybersecurity is would certainly add value.

REFERENCES

Defense Science Board (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.

Eom, J. (2014). Roles and responsibilities of cyber intelligence for cyber operations in cyberspace. *International Journal of Software Engineering and Its Applications, 8*(9), pp.137-146.

Haig, Z. (2009). Connections between cyber warfare and information operations. AARMS Security, Vol. 8, No. 2 (2009) 329–337. Retrieved from http://www.zmka.hu/docs/Volume8/Issue2/pdf/13haig.pdf

Knappenberger, B. (Director). (2012). We are legion [Documentary]. U.S.: Luminant Media.

Kuehl, D. (2009). From cyberspace to cyberpower: Defining the problem. Cyberpower and National Security, Washington D.C., National Defense University Press, Potomac Books,

Lanzendorfer, Q.E. (2015). Enabling knowledge in the paradigm of international cyber intelligence. Order Number 3708703. 2015 Ann Arbor, MI: ProQuest UMI.

Lieberman, Collins, and Carper (2001). Avoiding a digital Pearl Harbor. *The Washington Post, 1*, 1-2.

Lowenthal, M. (2009). Intelligence: From secrets to policy (4.th ed.). Washington, DC: CQ Press.

Marlatt, G. E. (2008, January 30). Information warfare and information operations (IW/ IO): A bibliography. Naval Postgraduate School. Retrieved from http://www.nps.edu/Library/Research/Bibliographies/index.html

McNeil, J. J. (2010). Maturing international cooperation to address the cyberspace attack attribution problem. Ann Arbor, MI: ProQuest UMI.

Ohlin, D., Govern, K., & Finkelstein, C. (2015). Cyber War: Law and Ethics for Virtual Conflicts (1st edition). Oxford, United Kingdom: Oxford University Press.

Pattee, P.G. (2008). Network-centric operations: A need for adaptation and efficiency. *The Air Force Research Institute.* Retrieved from http://www.au.af.mil/au/afri/aspj/airchronicles/apj/apj08/spr08/pattee.html

Schreier, F (2015). On cyberwarfare. Geneva Center for the Democratic Control of Armed Forces Horizon 2015 Working Paper No. 7. Retrieved from http://www.slideshare.net/KennethHardyCMIIB/on-cyberwarfarefred-schreierdcaf-2015-working-paper-no-7

Sternberg, R. (1997). Successful Intelligence: How Practical and Creative Intelligence Determine Success in Life. New York: Plume.

Wingfield (2000). The law of information conflict: National security law in cyberspace. Aegis Research Corp.