Towards Cyber Operations

The New Role of Academic Cyber Security Research and Education

Jan Kallberg
CySREC, Erik Jonsson School of Engineering and
Computer Science
The University of Texas at Dallas
Richardson, TX 75083-0688
jkallberg@utdallas.edu

Bhavani Thuraisingham
CySREC, Erik Jonsson School of Engineering and
Computer Science
The University of Texas at Dallas
Richardson, TX 75083-0688
bhavani.thuraisingham@utdallas.edu

Abstract – The shift towards cyber operations represents a shift not only for the defense establishments worldwide but also cyber security research and education. Traditionally cyber security research and education has been founded on information assurance, expressed in underlying subfields such as forensics, network security, and penetration testing. Cyber security research and education is connected to the homeland security agencies and defense through funding, mutual interest in the outcome of the research, and the potential job market for graduates. The future of cyber security is both defensive information assurance measures and active defense driven information operations that jointly and coordinately are launched, in the pursuit of a cohesive and decisive execution of the national cyber defense strategy. The cohesive cyber defense requires universities to optimize their campus wide resources to fuse knowledge, intellectual capacity, and practical skills in an unprecedented way in cyber security. The future will require cyber defense research teams to address not only computer science, electrical engineering, software and hardware security, but also political theory, institutional theory, behavioral science, deterrence theory, ethics, international law, international relations, and additional social sciences. This paper is the result of an ocular survey of the U.S. 48 academic CAE-R research centers, evaluating the collective group of research centers' ability to adapt to the shift towards cyber operations, and the challenges therein.

Keywords - cyber operations; cyberdefense; information assurance; center of academic excellence; CAE-R; defense; cyberwar; cyber education; information operations.

I. INTRODUCTION

In November 2011, the CISO of the strategic investment firm In-Q-Tel, Dan Geer, was interviewed by the online security company Kaspersky Lab's on their website. Dan Geer said: "For cyber security, solving known problems is not research. Figuring out what the problems will be - that's research." [1]

Dan Geer's statement is mirrored in discussions within our research community how to perform better research and provide education that are aligned with a drive towards cyber operations. The U.S. recent declaration of cyber as a warfighting domain such as land, sea, and air also is a clear indicator where additional future research is necessary.

The shift towards cyber operation is a journey into the unknown. Cyber conflicts between state actors are still limited. A cyber security research center has to be able to search for the unknown – and successfully make it known. Cyber operations become a tangible way to contribute to the national security effort. For academia, it is also a changing environment when universities can play a role in enhancing the corporate and military abilities to respond quickly to threats compared to earlier research that years later led to improvements through product developments and defense procurement.

At the entrance to the militarized and contested cyberspace; academia and research universities need to find their new role. Universities have to a high degree continued to deliver only information assurance originating either from a computer science department or an engineering school. The posture has been all defensive. Traditional IT security has had a decade of significant funding as a response to the tragic events on 11 September 2001 and the society's increased reliance on the Internet and computerized systems. This posture has been built on hardening systems and created fail-safe processes that are strong enough to defend against intruders. This surge of resources to cyber security research centers, contractors, federal agencies, and private industry gave increased abilities to understand how to secure systems. Now, the evolution takes another step forward.

II. CENTERS OF ACADEMIC EXCELLENCE

If information assurance was a defensive posture, cyber operations have a flexible role that seamlessly adapts from defense to response. The drive towards cyber operations is reflected in many ways. The NSA (The U.S. National Security Agency) has set up criteria for the designation of academic departments as CAE (Centers of Academic Excellence) to ensure that the quality in education and research is upheld. A second purpose is to create a common body of knowledge, disseminate information and best practices for information security over the nation, and create a structured way to ensure high-quality education for the public and private sector IT workforce. NSA's latest addition is CAE Cyber Operations.

The NSA requirements for cyber operations are straight-forward but in a rigorous way, state the level of academic excellence sought [2].

978-1-4673-2104-4/12/$31.00 ©2012 IEEE

According to NSA;

"The CAE-Cyber Operations program is intended to be a deeply technical, inter-disciplinary, higher education program firmly grounded in the computer science (CS), computer engineering (CE), and/or electrical engineering (EE) disciplines, with extensive opportunities for hands-on applications via labs/exercises. The CAE-Cyber Operations program complements the existing Centers for Academic Excellence (CAE) in Information Assurance Education (CAE-IAE) and Research (CAE-R) programs, providing a particular emphasis on technologies and techniques related to specialized cyber operations (e.g., collection, exploitation, and response), to enhance the national security posture of our Nation. These technologies and techniques are critical to intelligence, military and law enforcement organizations authorized to perform these specialized operations."

The key statement is collection, exploitation, and response. The future will bring a broader scope for Centers of Academic Excellence (CAE) as centers moves toward becoming CAE Cyber Operations and beyond. The militarization of cyber space, with the potential for funding in the future, will require knowledge and understanding of the long-term impact of cyber beyond the near-time digital handling.

As a small experiment, we conducted a survey to get a snapshot where CAE-R academia stands today in relation to the broader systematic all-societal view on cyber operations. We are aware that all activities in a research center are not reflected online. This study is broad with no ambition to give a perfect picture of the actual state of the discipline, but it can serve as an indicator and raise awareness of areas that need to be addressed. We understand that this shift is a work in progress and we have credited schools that are moving in the direction towards cyber operations, even if the actual approach as of today is still *ad hoc*.

III. Survey of CAE-R institutions

The intention with the survey [3] was to investigate how many CAE-R academic research centers are already committed to cyber operations beyond traditional information assurance and could contribute to the cyber operations mission. Advanced cyber operations require linkages outside of the engineering schools and benefit from collaboration with other university-wide schools and departments. A broader knowledge base enables the research center to do research that can utilize active defense of systems that turnaround, respond, and exploit the attacker. The research can then be transferred through research-based education to the workforce.

A set of variables were created and then each academic CAE-R research center's web presence was visited and the materials presented on the website were evaluated against the variables. There were in February 2012 in the US a total of 48 academic research centers in non-military higher education. All schools that met the CAE-R criteria had an information assurance program in place as the foundation for the designation.

The variables used were;

A) if there is research on offensive and responding cyber defense, if the research conducted steers toward counter-attacks, including psychological and information operations,

B) if there is a legal component, especially international law, ethics, and privacy,

C) if the research has involved political scientists or other social scientists, especially in theories about national institutional stability and international relations,

D) does the university have a designed policy school, or similar entity,

E) if there is a clear linkage between the cyber security program and the policy school of the same university, if one exists,

F) if security studies scholars are involved in the cyber security research,

G) if there is an international relations component in the research, and

H) if the research covers the space domain,

These areas should cover the future of cyber operations and be a direction where the development of cyber operations research is heading. The results are presented in Table 1.

IV. Results

One intention with the survey was to get a broad sense of how well-suited the academic community is to support cyber operations and where the majority of the U.S. cyber security research centers are on the learning curve.

Only 5 CAE-R centers are actively researching cyber operations in a broader extent for information and psychological operations, and aligned with future military operations.

The high number of CAE-R that have legal components in their research reflects the privacy component, which is central in information assurance but of less significance in information operations. The linkages to privacy are in many cases shallow and not a major theme in research projects unless there are dedicated scholars.

Only 10 CAE-R involve social scientists in their research. A significant number of schools do not involve social scientists in projects that are focused on human behavior and institutional arrangements.

Of the 48 CAE-R, 10 have a full-sized policy school on campus, with numerous specialized scholars running research over a spectrum of policy-related inquiries and with understanding of core tenets of societal cyber operation components. Only 5 CAE-R out of these 10 collaborate to a visible degree with their own policy school and utilize the joint knowledge. In other terms, 50 % of the cyber security research centers with policy schools on campus underutilize the policy school's pool of competence when doing cyber defense and cyber operations research.

Cyber is also an arena for international cybercrime and transnational illicit activities, only 6 CAE-R involved international relations scholars in their projects. Cyber issues in space only draw interest from 5 CAE-R even if the U.S. military global information grid relies heavily on satellites and spaceborne assets.

The largest portion of the CAE-R is doing information assurance independently of other scholarly activity on their campuses. If these schools have a presence in security studies or privacy, it is often the result of a single or a few dedicated scholars that have extended their interest.

V. Conclusion

NSA clearly states that cyber operations should be interdisciplinary; focusing initially within the engineering schools, but in the continuum the militarization of cyber space will increase the width of collaboration. If our society is under cyberattack, we can defend the nation if we are technically advanced, but we will also be able with the help of other sciences to mitigate cyber vulnerabilities in societal behavior, economic structure, and institutional arrangements. Cyber operations require an ability to do collection, exploitation, and response. Academic institutions train the workforce that will staff the execution, management, and monitoring of cyber operations. All schools are capable of collections; the two other pivotal terms, exploit and response, will require university-wide collaboration. How do cyber security centers become successful in cyber operations?

We would like to propose five steps that could be beneficial:

1. Identify scholars at your own university that share the cyber security and cyber operations research interest even if they are located in other schools such as policy school, business school, school of liberal arts, or other departments, and collaborate, to get intellectual leverage;

2. Develop cyber relevant courses in a cohesive manner between as an example; cyber security research, business school's information and risk management, public policy courses, and other relevant course offerings and promote these courses to the students, and enrich their opportunities for a good education;

3. Seek funding with the business school, school of social science, engineering school, as equal partners, where the other school gets a fair share so they are dedicated to the project;

4. Find ways to avoid "issue ownership" conflicts between departments and schools, such as only business school can teach information security management because it is management, and the business school see itself as the sole base for all management education; and

5. Be prepared to handle a constructive critique of your research program by the newly-added collaborating peers from other schools. If a research team has operated as intellectual solitaires in our departments, surrounded by scientists of our own kind, the research team could have made assumptions other scholars from other science disciplines might see differently.

Finally, the future for cyber operations research and education requires an institutional and cultural challenge to academia. In our view, many of the resources needed to be successful are already accessible. The task is to identify, arrange, and structure the intellectual capacity in place for each university.

TABLE I. Survey results

	CAE-R institutions N=48 (DoD institutions not counted)		
	Variable	***Number of schools***	***% of total***
A	Active-defense / offensive cyber research	5	10.4
B	Legal considerations and privacy	18	37.5
C	Involving social scientists and/or behavrioal scientists	10	20.8
D	Policy school on campus	10	20.8
E	Of universities with policy schools, how many untilize this resource in cyber security research	5	10.4
F	The presence of security studies scholars or activity	14	29.2
G	International relations	6	12.5
H	Cyber in outer space	5	10.4

Acknowledgement

We acknowledge the limitation in the survey as it is conducted based on the research progress, knowledge production, and publication records presented online. The purpose of this paper is to promote intra-university collaboration, increase research efficiency in publically funded research, and support alignment to a doctrinal shift towards cyber operations. The manuscript represents the opinion of solely the authors.

[1] Geer, Dan. A New Cybersecurity Research Agenda (In Three Minutes or Less). https://threatpost.com/en_us/blogs/new-cybersecurity-research-agenda-three-minutes-or-less-110711

[2] NSA, Criteria for Measurement for CAE / Cyber Operations http://www.nsa.gov/academia/nat_cae_cyber_ops/nat_cae_co_criteria.shtml#4

[3] J. Kallberg, "The DoD Move From Information Assurance to Cyber Operations – Analysis of Competitiveness in the New Defense Posture", internal report, Cyber Security Research and Educational Center, Erik Jonsson School of Engineering and Computer Science, The University of Texas at Dallas. February 15, 2012.