Training of Interdisciplinary Cyber Warriors

Prof. Dr. Srisakdi Charmonman
Asian Computer Man, Father of Thai Internet, and Fellow of the Royal Institution of Great Britain
Charmonman@gmail.com, www.charm.SiamTechU.net

Chatpawee Trichachawanwong
IT Princess of Thailand, Vice President of the Computer Association of Thailand and Vice President of Thailand Internet Association
Chatpacee@gmail.com, www.ceemeagain.com

Abstract - Cyber Warfare is interdisciplinary in the sense that it involves several disciplines. All countries in the world including ASEAN are concerned with Cyber Warfare which is becoming more and more popular. Conventional Warfare are being replaced by Cyber Warfare. In Conventional Warfare, armed forces are employed using tanks, gunboats, combat aircrafts, and etc. and the weapons are canons, rockets, missiles, bombs, and etc. Another name of Cyber Warfare is Electronic Warfare. The North Atlantic Treaty Organization has recognized the importance of Electronic Warfare by establishing "NATO Electronic Warfare Advisory Committee". Cyber Warfare Organizations and cyber warriors are employed using weapons which are computer software. At least twelve countries have established cyber warfare organizations. They are Argentina, Brazil, Canada, China, the Democratic People’s Republic of Korea, Denmark, Germany, India, Iran, the Republic of Korea, Switzerland and the United States. One of the most important aspects of Cyber Warfare is training of Cyber Warriors. This paper will discuss cyber warrior training concepts, cyber warrior training by US armed Forces, cyber warrior training by non-government and private organizations, and cyber warrior training by universities and colleges.

Keywords - Cyber Warriors, Cyber Warrior Training Concepts, Cyber Warrior Training Programs

1. INTRODUCTION

From "Wikipedia" [1], CyberWarfare is politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare. Cyber Warfare may also be referred to as "Information Warfare" or "Internet Warfare" or "Electronic Warfare". The North Atlantic Treaty Organization has recognized the importance of Electronic Warfare by establishing "NATO Electronic Warfare Advisory Committee" [2].

Cyber Warfare is interdisciplinary in the sense that it involves more than one discipline. All countries in the world including NATO countries and ASEAN countries are concerned with Cyber Warfare. Conventional Warfare are being replaced by Cyber Warfare. In Conventional Warfare, armed forces are employed using tanks, gunboats, combat aircrafts, and etc. and the weapons are canons, rockets, missiles, bombs, and etc. In Cyber Warfare, cyber warriors are employed using weapons which are computer software. At least twelve countries have established cyber warfare organizations. They are Argentina, Brazil, Canada, China, the Democratic People’s Republic of Korea, Denmark, Germany, India, Iran, the Republic of Korea,
Switzerland, and the United States [3]. In the case of the US, the Cyber Warfare organization is called "the Cyber Command" which is separated from the conventional armed forces. The US Cyber Command is planning to have 6,000 cyber warriors comparing to over 300,000 cyber warriors in China. The US, China, and all other countries need to train Cyber Warriors. Therefore, one of the most important aspects of Cyber Warfare is Training of Cyber Warriors. This paper will discuss cyber warrior training concepts, cyber warrior training by US armed Forces, cyber warrior training by non-government and private organizations, and cyber warrior training by universities and colleges.

II. CYBER WARRIORS TRAINING CONCEPTS

The Director of Training at US Cyber Command said that training of Cyber Warriors is very complicated [4]. In the US, Cyber Warriors trainings are done by Military Services, Contractors, Military Academies, and National Defense University’s “iCollege”. Cyber Warriors need a wide range of technical skills, namely, IT skills, Engineering skills, Management skills, and Advanced Cybersecurity skills which include Information Assurance, Information Security, and Network Defense. For Network Defense, Cyber Warriors have to be well versed in auditing, incident response, and infrastructure support. The US Cyber Command and the US military services have developed joint cyberspace training standards for both existing approaches and new approaches to cyber warfare and security.

The US Department of Defense has developed “Four-Phases Training for Cyber Warriors”. Phase 1 is “Feeder Courses” to help military personnel obtain military occupation specialties for their respective services. Phase 2 is “Foundation Training” for specific CMF work categories. Phase 3 is “Collective Training” for mission-oriented team. Phase 4 is “Sustainment Training” to keep Cyber Warriors abreast of changing needs and requirements.

In summary, Cyber Warriors have to continue to learn all the time because Cyber Technology is developing and changing very fast. The US Cyber Command makes frequent discussions with subject matter experts to identify improvements needed for the training and conduct “Regular Exercises” such as “Cyber Flag” which is “annual joint, interagency exercises”.

III. CYBER WARRIORS TRAINING BY US ARMED FORCES

The US Armed Forces need more and more Cyber Warriors in addition to the 6,000 at the Cyber Command. The US has established schools for cyber warfare, such as:

1) The Army Cyber Center of Excellence at Ft. Gordon, Georgia.
2) The Navy Center for Information Dominance in Pensacola, Florida.
3) The Air Force established the 24th Air Force as its operational cyber organization at Joint Base San Antonio-Lackland, Texas.
4) The 24th Air Force has the 688th Information Operations Wing for recruitment and training of Cyber Warriors.

Air Force Cyber Warriors get initial training at Keesler Air Force Base, Mississippi. Cyber Warriors may be enrolled in Undergraduate Cyber Training. Enlisted personnel for Cyber Operation may attend a Cyber Defense Operation course Air Force Cyber Warriors may attend advanced training at Hurlburt Field, Florida. Cyber Warriors get their training on particular weapons systems, including, at their mission locations and from professional civilian certifications such as Information Assurance, Computer Security, Network Security, Hardware and Software Platforms, and Incident Handling.

The Air Force also offer recurrent training to ensure its Cyber Warriors are well-versed in the most recent tactics, techniques, and procedures. Cyber Warriors also receive
education and training in information operation, cryptography, and intelligence to enable them to attack, defend, and exploit intelligence information.

Other US Armed Forces also carry out training, for example, Navy offers Cryptologic Information System Training, Intelligence Specialists Training, Information Warfare, and Cyber Warfare Engineering. The US National Defense University (NDU) offers Technology Aspects of Cyber Security, Technology Aspects of Cyber Warfare, and situations not covered by training manuals or textbooks.

The US Army in December 2013 consolidated its cyber command operations from a half dozen government buildings in Washington, D.C. to Fort Gordon. The US Army also moved its cyber and network operations from Georgia to be under the control of a single commander with 21,000 soldiers and civilians.

The US Navy has a cyber workforce of 5,000 uniformed and civilian employees at Fort Meade, Maryland. US Fleet Cyber Command at US Tenth Fleet operational facilities and task forces around the world with expertise in Cyber Networks, Information Operations, Electronic Warfare, and Signals Intelligence. The Naval Reserve Officer Training Corps got 85% of its scholarship midshipmen for 2013 and 2014 to enroll in technical academic majors. 11% of the 85% are majoring in Cyber Security and Cyber Warfare. It is expected that the first group of graduates with cyber operations major will be in the year 2016.

NDU’s iCollege also offer training in Cyber Security and Cyber Warfare to one-star general or equivalent. NDU’s iCollege is educating future cyber leaders by using Case Studies, Modeling and Simulations, and etc.

From <scienceblog.com/70496/darpa…> [5], DARPA (Defense Advanced Research Projects Agency) in January 2014 offered cyber security training to Cadets and Midshipmen. The training program was called “Service Academy Cyber Stakes”. The trainees are from the US Military Academy in West Point, N.Y., the US Naval Academy in Annapolis, Md, and the US Air Force Academy in Colorado Springs, Colorado. DARPA must train 4,000 Cyber Warriors by the year 2017. Two world-class experts who helped in the training were David Brumley, Technical Director of CyLab Carnegie Mellon University and Dan Guido, CEO at Trail of Bits and Hacker-in-Residence, New York University and Polytechnic School of Engineering.

IV. CYBER WARRIORS TRAINING BY NON-GOVERNMENT AND PRIVATE ORGANIZATIONS

There are Non-Government and private organizations offering training for Cyber Warriors and a few examples will be given. They are W2CW, SecureNinja, and Cypherpath.

The first example, W2CW is an abbreviation for “Warrior to Cyber Warrior.” W2CW is a non-government organization (NGO). W2CW has been offering training course for Cyber Warriors between 28 Jan - 17 Jun 2012, 8 Apr - 27 Aug 2013, 1 Jul - 11 Nov 2013, and 10 Dec 2013 - 31 Apr 2014. W2CW Program does not discriminate on the basis of race, color, national and ethnic origin, or on administration of its educational policies, admissions policies, other school-administered program, and learn anytime anywhere. W2CW features Echo360’s blended learning system that provides a combination of online and classroom training tailored to individual learning objectives. The cost may be negotiated between W2CW and the student or the organization sending student.

W2CW Program includes certified cyber security training, professional certification, security clearance for government initiatives, internship in the cyber security field, and job placement upon completion of the program.

The second example is SecureNinja which provides, “Cyber Warrior Expert Team
Training”. It is an effective solution that develops, builds and maintains an expert team of practical, real world skilled expert Cybersecurity warriors for any organization. SecureNinja provides strategic training to ensure identified personnel have the knowledge, skills and commitment to meet the requirements of maintaining an elite force of Cyber Warriors; providing a framework for training on Cybersecurity within each team. The focus is such that all team members can develop their specific skills, needed to perform their role at the highest level by clarifying the need for training and identifying those who should receive particular levels of training; providing a strategic basis for training across the organization including a delivery plan and methodology; and detailing how the strategy will be evaluated. SecureNinja provides three levels of training. The first level is Foundation knowledge and core security skills. This is important as the facts, the knowledge and information about procedures and processes is very critical to the ability to continuous growth and learning. Your Cyber Warrior’s will have this required “core” set of training. The second level is Process Centric Training what individuals need to be able to do to implement the process and methodology is to follow a systematic method that emulates the threat mind set. It includes technical skills and tactical skills in identifying vectors of attacks and hence having the capability to secure against those threats regardless of the technology used. Once your personnel are trained on the above then they will receive specialty training to allow them to perform the requirements of their job function. The third level is Continuous Learning and Growth which is the medium to long term development of skills, especially at an advanced level, which will ensure the Cyber Warrior maintain their elite skillset. This will require the staff to maintain currency on the latest topic and more importantly be engaged in the latest threat discussions. SecureNinja uses the following training methods, including, in-house training, OJ (On the job) training, core security training, advanced security training, research training, and recurring training via Scorm compliant portal. SecureNinja provides the following resources are budget core security skills training, advanced specialized training, conferences, certifications/qualification, research opportunity, and test environment.

The third example is Cypherpath which is a private organization providing Cyber Warfare training thru Distance Learning or eLearning. Cypherpath provides several topics of training, for example, Vulnerability Analysis Modeling, Wikileaks Case Study Assignment, Cleared Insider Case Study, Al-Qaeda's Case Study Assignment, Counter Cyber Intelligence Case Study, Cyber Weapons Classification Study, and SCADA. SCADA includes Introduction and Overview, Setting the Cyber Security Stage, Cyber Hacktivism, Cyber Espionage, Cyber Terrorism, Cyber Intelligence, Cyber Weapons, eBombs, and other devices, Cyber Attack Process, Cyber Warfare Doctrine & Strategy, International Issues (Investigations), and the Problems of the Near Future.

V. CYBER WARRIORS TRAINING BY UNIVERSITIES AND COLLEGES

Several universities and colleges are offering degree programs specialized in Cyber Warfare and a few examples to be offered in this Section are Bachelor’s Program in Korea, Master’s Program in USA, Master’s Program in France, and a Ph.D. Program.

The first example is Bachelor’s Program in Korea [6]. In July 2011, Korea University cooperated with the South Korean Army offers an undergraduate program for Cyber Warfare specialists. Thirty students were admitted for the 4-year course. The subjects in the curriculum are information technology, cryptography, psychology, cyber warfare tactics, and etc. The students will receive a full scholarship for four years and upon graduating, will join the armed forces to serve as commissioned officers, specializing in information, and communications for seven years.
The second example is from the University of Maryland at Baltimore County (UMBC) in the US offering a Master’s degree with specialization in Cyber Security [7]. UMBC is conveniently located off of I-95 near the BWI Airport, approximately ten miles from Fort Meade (home of DISA, NSA, and the U.S. Cyber Command). UMBC is convenient to a host of federal agencies and government contractors that need cyber-related research, education, and training.

The third example is a Master’s Program in France [8]. ESIEA University in France offers “International Master in Computer Security and Cyberwarfare.” The purpose of the program is for the graduate to gain practical technical skills and prepare for an exciting career in Network and Information Security or in Cyberwarfare Techniques. The graduate can expect a variety of exciting careers in security information ranging from computer network administrator, IT security expert or cyberwarfare expert for the Department of Defense to security officer in charge of the IT security in an international firm.

The fourth example is from the University of South Wales [9] which offers Ph.D. in Cyberwarfare Operations Planning and Impact Assessment and provides financial grant to fund Ph.D. project for European and UK Students Only. The project aims to examine the feasibility of constructing and validating a planning model/tool/method that can be used to plan a computer network operation and assess the impact of the operation. The applicants of this project will adopt the following objectives which are definition of emerging policy and practical capabilities in the sphere of Cyberwarfare to develop a framework Concept of Operations; investigation and development of modeling and simulation technologies capable of providing an analysis of the effect of Computer Network Operations methods on defined target systems; and specific development of innovative toolsets enabling scientific planning of Computer Network Operations events and provision of a level of confidence assessment of preferred course of action. The Ph.D. program is three years full time. Also, the funding will be available to provide a student stipend (currently £13,390pa) and fees for EU/UK applicants.

VI. CONCLUDING REMARKS

Conventional warfare is being replaced by cyber warfare. Cyber attacks are carried out by more and more countries such as China and the US. China has about 300,000 Cyber Warriors. The US is speeding up training of Cyber Warriors. Every country is vulnerable to cyber attacks. Therefore, every country should establish action plan about cyber warfare. Included in the plan should be training of cyber warriors, either locally or abroad or both. Scholarships should be given to study Cyber War. If a country does not have a cyber warrior training program locally, one should be established. Military exercises jointly with advanced countries similar to Cobra Gold should be carried out for Cyber War.

REFERENCES

(Arranged in the order of citation in the same fashion as the case of Footnotes.)


