AFRL-RI-RS-TR-2019-102

THE ADVANCED COURSE IN ENGINEERING 2018: LEADING CYBER-WARRIOR DEVELOPMENT

MAY 2019

FINAL TECHNICAL REPORT

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

AFRL-RI-RS-TR-2019-102 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE CHIEF ENGINEER:

/ S /
DAVID BLAIR
Work Unit Manager

/ S /
JAMES S. PERRETTA
Deputy Chief, Information
Exploitation & Operations Division
Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* MAY 2019	**2. REPORT TYPE** FINAL TECHNICAL REPORT	**3. DATES COVERED** *(From - To)* APR 2016 – SEP 2018

4. TITLE AND SUBTITLE

THE ADVANCED COURSE IN ENGINEERING 2018:
LEADING CYBER-WARRIOR DEVELOPMENT

5a. CONTRACT NUMBER
IN-HOUSE

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
62788F

6. AUTHOR(S)

David Blair and Erich Devendorf

5d. PROJECT NUMBER
G1AC

5e. TASK NUMBER
IH

5f. WORK UNIT NUMBER
01

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/Information Directorate
Rome Research Site/RIGA
525 Brooks Road
Rome NY 13441-4505

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/Information Directorate
Rome Research Site/RIGA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/RI

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TR-2019-102

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. PA# 88ABW-2019-2044
Date Cleared: 26 Apr 2019

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The 2018 ACE continued a 15-year tradition of excellence with immersion in the cybersecurity discipline over a 10-week time span through a combination of intense coursework and internship experiences. This graduate level curriculum covered leadership during crises, the science of mission assurance, the art of cyber warfare and written/oral communication skills. This year ACE interns put every lesson into practice through open-ended challenge problems that covered the full range of cyber operations. Their capstone combined these lessons through a two-day exercise in a contested cyber-kinetic battlespace at the Air Force Research Laboratory (AFRL) Stockbridge Test Range.

15. SUBJECT TERMS

Advanced Course in Engineering, cyber, security, information assurance, training, education, development

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** **DAVID BLAIR**
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	21	**19b. TELEPHONE NUMBER (*Include area code)*** **N/A**

TABLE OF CONTENTS

Section **Page**

1.0 SUMMARY

The Advanced Course in Engineering (ACE) develops the next generation of cyber warriors, with emphasis on educating future leaders. In 2018, the ACE graduated a class of 32 cyber warriors composed of 10 Reserve Officer Training Corps (ROTC) cadets, 13 civilians, 3 United States Air Force (USAF) lieutenants and 6 Ministry of Defense (MoD) exchange interns. The 2018 class had a 3.9 average GPA.

The 2018 ACE continued a 15-year tradition of excellence with immersion in the cybersecurity discipline over a 10-week time span through a combination of intense coursework and internship experiences. This graduate level curriculum covered leadership during crises, the science of mission assurance, the art of cyber warfare and written/oral communication skills. This year ACE interns put every lesson into practice through open-ended challenge problems that covered the full range of cyber operations. Their capstone combined these lessons through a two-day exercise in a contested cyber-kinetic battlespace at the Air Force Research Laboratory (AFRL) Stockbridge Test Range.

The ACE research internships had an impact on AFRL research programs, the National Security Agency (NSA) red team and MoD Defense Science and Technology Laboratory (DSTL). The projects included contributions to the ACT3 autonomy, machine learning for vulnerability mitigation, red team visualization, Internet of Things vulnerability assessment and cyber training effects. The Air Force benefited from ACE R&D during RED FLAG 19-1 where the 57th IAS applied ACE cyber effects to the operationally degraded, contested battlespace in the CAOC.

The ACE remains the only pre-commissioning cyber program and the premier undergraduate cyber warrior development program in the nation. Since 2003 the 423 ACE graduates have a 65% retention rate in the Air Force. Over 25% of eligible graduates attend the NSA's prestigious Cyber Network Operations Development Program (CNODP). The Air Force CNODP class has been composed of over 25% ACE graduates even though they represent only 0.7% of the Air Force's cyber forces. The asymmetric impact of ACE graduates reflects the asymmetric impact of cyber power itself.

2.0 INTRODUCTION

The ACE develops the next generation of cybersecurity warriors, with a particular emphasis on educating future military leaders. The ACE follows the model for the General Electric ACE to transform the top ROTC cadets, civilian undergraduates, and USAF junior officers into original thinkers, problem solvers and technical leaders.

The underlying ACE philosophy is to completely immerse interns in the cyber security discipline through a combination of intense coursework and internship experiences. These experiences fall into 4 categories: academics, leadership, research, and BLUE EDGE.

Learning objectives for the ACE are formulated according to Bloom's taxonomy. Bloom's taxonomy is an education framework, stating education goals in terms of how the material strengthens participants' abilities to remember, understand, apply, analyze, evaluate, or create (Armstrong, 2018). Learning objectives are listed for below for the complete program, and included with each program component's description:

1. **Application** Articulate the foundational elements of the science of mission assurance
2. **Synthesis** Adapt principles on the art of cyber warfare to achieve mission objectives
3. **Evaluation** Select between courses of action during crisis decision making
4. **Synthesis** Formulate a plan to achieve open-ended mission objectives
5. **Analysis** Prioritize tasks to fulfill mission objectives based on an evaluation of solution quality
6. **Knowledge** Appreciate the importance of physical fitness for cyber warriors

2.1 ACADEMICS OVERVIEW

The ACE provides education and training to the next generation of cyber-leaders, as such academics are a core component of the ACE. Each week, interns attend a daylong lecture, given by a domain expert from the military, academia or industry. Lectures are at a graduate level, and focus on educating ACE interns in the fundamental science of the cyber domain. Interns work as teams to solve open ended, Air Force relevant challenge problems associated with every lecture. Every lecture is paired with a "tradecraft" lesson. Tradecraft lessons are similar to the hands on "labs" in a university setting. Lessons train interns in the application of concepts in that week's lecture. The learning objective for the academics component – including both lecture and tradecraft – are listed below:

1. **Evaluation** Judge the appropriate level of completeness for open-ended problems
2. **Synthesis** Write a comprehensive, technical solution to an open-ended problem
3. **Evaluation** Grade the completeness, professionalism, and originality of written reports
4. **Synthesis** Express technical concepts in a time constrained oral presentation

5. **Comprehension** Describe the capabilities and limitations of defensive cyber tools and techniques
6. **Application** Use tools to establish a foothold, persist and move laterally through a network
7. **Knowledge** Recognize common exploitation avenues at all levels of the OSI model
8. **Application** Develop exploits, agents and tools to gain access, escalate privileges and communicate covertly

2.2 RESEARCH OVERVIEW

ACE interns perform USAF relevant research under the mentorship of subject matter experts (SME). ACE staff sends out calls for a research topics, and SMEs from various agencies respond with concrete proposals. Research proposals are selected for USAF relevance and program fit. Topics from all levels of theory and abstraction have been chosen. Interns work closely with mentors, communicate regular status reports, and provide final deliverables for possible transitions to SMEs and agency customers. Learning objectives for this component are listed below:

1. **Comprehension** Describe the state of the art for a specific, deep dive research topic
2. **Analysis** Experiment with new concepts and techniques to advance research plan
3. **Synthesis** Develop fundamental mathematics and engineering artifacts to support research objectives
4. **Analysis** Survey the state of an unfamiliar field to identify fundamental research challenges

2.3 LEADERSHIP OVERVIEW

The ACE program maintains that technical excellence is a necessary, but not sufficient condition to develop the next generation of cyber leaders. The program possesses a significant leadership component. Each week interns attend leadership seminars and case studies provided by a senior retired USAF officer. Interns and staff attend a joint leadership retreat at the Battle of Gettysburg historic site. ACE interns also engage in shared physical training in the form of a weekly 8-mile run. The run encourages comradery, and imbues an appreciation for physical fitness in the next generation of cyber leaders. Learning objectives for this unique focus are listed below:

1. **Knowledge** Appreciate the need to lead upward through demonstrated professional competence and personal relationships.
2. **Evaluation** Evaluate basic leadership principles and the imperatives of command applicable to future cyber warriors
3. **Application** Apply the important models and theories dealing with critical decision making and leadership in analyzing case studies and conducting cyber related exercises
4. **Evaluation** Assess individual, group and organizational planning and decision making flaws and determine how to prevent them.

5. **Comprehension** Identify attributes and conduct critiques of good and bad planning and decision making processes

2.4 BLUE EDGE OVERVIEW

BLUE EDGE is a cohesive collection of cyber-exercise technologies and infrastructure developed at AFRL/RI. Participants execute missions in a contested, multi-domain battlespace to fulfill mission objectives, modeling conflict in a richer manner than a capture the flag scenario. ACE interns configure a wide variety of service configuration and deployment as well as in simulated kinetic training operations to prepare for the BLUE EDGE capstone. BLUE EDGE culminates in a two-day training exercise, simulating full-scale cyber and cross-domain warfare at AFRL/RI's Stockbridge test site.

1. **Comprehension** Express the relationships between the cyber and physical domains
2. **Application** Demonstrate leadership skills in a multi-domain environment
3. **Synthesis** Develop a strategy to translate an operational end state into tactical objectives
4. **Synthesis** Plan an integrated cyber-physical operation to achieve tactical objectives
5. **Comprehension** Identify the challenges to execute a distributed multi domain operation

3.0 METHODS, ASSUMPTIONS, AND PROCEDURES

The ACE program underwent gradual change and maturation in 2018 while being under the direction of new senior leadership. The goal was to maintain everything good in the evolution of the ACE and to simultaneously refine and formalize them.

The ACE historically graded interns on their weekly challenge problem report and corresponding presentation. This grading was expand to include all aspects of the program: academics (including the previously mentioned report and participation in tradecraft), research, leadership evaluation, run times, and BLUE EDGE operational performance. Interns were then stratified on the basic of their performance, as standard in military education programs. The program's distinguished graduates were then selected as the three interns with the highest standing.

The ACE culminated with a cyber-security competition since the early days of the program. This competition was similar to a traditional CTF. BLUE EDGE gradually developed, initially being the addition of a few actually and simulated physical assets. BLUE EDGE expanded to scores of physical assets seamlessly integrated into the cyber-domain and shifted to an entirely objective based conflict. Past participants of the exercise noted that, while they thoroughly enjoyed and learned from the experience they felt ill prepared. The ACE curriculum contained several lessons and activities on military planning. ACE staff instituted a wide variety of preparatory and training operations for the interns in response. ACE interns received significant training on mission planning and experience in mission execution in the BLUE EDGE battlespace prior to the ACE capstone.

3.1 CLASS RECRUITMENT, SELECTION, AND COMPOSITION

The ACE staff executed a variety of recruitment strategies. The diversity of recruitment strategies is reflective of the final ACE class composition. The ACE director provided materials for national ROTC arms message and met with the body of ROTC commanders. ACE staff visited select ROTC detachments. The ACE program conducted civilian undergraduate recruitment by conducting university career fair visits, as well as visiting the 2018 Scholarship for Service (SFS) virtual and live career fairs. In continuation of a long and productive relationship, the United Kingdom's Ministry of Defense reached out with civilian professional, commissioned officer, and officer cadet candidates. The Air Force Operational Test and Evaluation Center also provided junior commissioned officers. The ACE staff recruited an AFRL Lieutenant in a program first.

Candidates submitted resumes, university transcripts, and references. The ACE program seeks ROTC and civilian rising junior and senior undergraduates as well as junior commissioned officers. An education in STEM very strongly preferred, with particular preference to those in Computer Science and Computer Engineering. The vast majority of candidates must have a GPA of 3.0 or higher, with preference given to those with at least 3.5. Those meeting the programs criteria were given phone interviews. The phone interviews would provide candidates with program information. Candidates were asked technical and leadership questions throughout the interview to determine program fit.

The final 2018 ACE class consisted of 29 first year interns, with 3 returning interns serving as program teaching assistants. US participants had an average GPA of 3.9. An exact breakdown of the class can be found in the following table:

Table 1. ACE 2018 Class Composition

	Civilian Undergraduates	ROTC Cadets (or UK equivalent)	Commissioned Officers	Civilian Professionals	Total
1st year ACE interns	9	12	0	0	29
- 1st year US students	9	11	0	0	20
- 1st year USAF	0	0	3 (2 AFOTEC, 1 AFRL)	0	3
- 1st year MoD	0	1	4	1	6
ACE teaching assistants	2	1	0	0	3
ACE 2018 class	11	13	7	1	32

3.2 ACADEMIC EXECUTION

The ACE staff of 2018 were fortunate to inherit a history of academic breadth. Most chosen topics were continuation of years previous. The topic selection is indicative of how information assurance should be interwoven into all layer of the technological stack. A substantive addition was adding operationally focused materials, this introduced interns to the fundamentals of tactical and operational training. These additions helped educate the next generation of leader in the nature of operations in the cyber domain and helped prepare them for the ACE capstone. The focus on cyber operations and planning is a unique contribution.

Many instructors had a history of working with ACE. This previous working relationship helped vet both the material, instructor performance, and the intern experience. The ACE instructors came from a wide variety of government organizations: AFRL/RI, AFRL/RY, the 90th COS, NSA, and the Air Force Cyber Weapons School. Government efforts were supplemented by SMEs employed by Parsons and Syracuse University.

3.2.1 Lecture Topics

All lecture topics for the ACE 2018 are listed below:

- *Cyber-Tactical Planning*
  This fundamentals lecture provides an introduction to planning cyber missions at the tactical level, with emphasis on continuous improvement through training regimen and PBED cycle. Interns will learn the necessity of planning and its various levels: strategic, operational and tactical. A rigorous methodology will be provided for planning cyber missions at the tactical level. Interns will then perform a hands on exercise to hone their tactical planning skills.

- *Cryptography Fundamentals*
  A first introduction to central concepts and algorithms of cryptography, with strong emphasis on what each algorithm or method provides in terms of the C-I-A triad. Start with the underlying mathematics of functions, boolean logic, number theory, and finite fields. Proceed to cryptographic hashing, symmetric key cryptography, public key cryptography, and certificates. End with synthesizing the previous topics and a discussion of advanced protocols such as STS and TLS.

- *Networking Fundamentals*
  An introduction to networking concepts and protocols. Begins with discussion of TCP vs UDP, IP addresses (IPv4, and IPv6), MAC addresses, and ports. The OSI model is explained as well as the taxonomy of hubs, switches, and routers. Lecture ends with discussion of routing protocols such as OSPF and an interactive learning activity.

- *Security Systems Engineering*
  The Security Systems Engineering topic intertwines traditional lecture with student activities to provide an overview of systems engineering with an emphasis on initial system specification. Students study the stages of the systems development lifecycle and learn the purpose, format, and content of a system requirements specification (SyRS). Students explore how to express security within a SyRS, differentiate between functional and non-functional requirements, and recognize well-written requirements. During the lecture, students generate Unified Modeling Language (UML) use case and activity diagrams, conduct a brief use case analysis, and create a high-level architecture model. As a final project, students generate a SyRS for either their summer research project or their capstone enclaves.

- *Certified Security by Design*
  The lecture provides the requisite background in Access Control Logic and Certified Security by Design for the cadets to execute a novel challenge problem: to devise and verify the authentication and authorization CONOPS for a UAV payload controller. The payload controller is a system to release a weapon within a kill box within mission timing, by means of transmitting, receiving, and executing a valid release command, in order to contribute to accomplishing an air interdiction mission. Cadets will use an access-control logic to describe and verify the authentication and authorization CONOPS.

- *Secure Enclave Design*
  Secure Enclave Design will provide students with the knowledge required to build and operate a mission network in a contested environment. The class will address mission network topologies, enterprise network security issues, and on time network deployment. Additionally, it will provide the students a look through the eyes of an adversary for the development and execution of an offensive attack on an adversarial mission network. The students will complete a project that will require them design a secure mission enclave.

- *Network Reconnaissance*
  This lecture is intended to provide instruction on network reconnaissance and pivoting. The topics covered are network fundamentals, reconnaissance, network enumeration, wireless networks, network attack, credential mining, privilege escalation, and pivoting. The course focuses on the fundamentals with interactive examples, and provides a challenge problem that covers many of the topic areas addressed during the lecture.

- *Bypassing IDS, Firewalls, and Antivirus*
  Lecture will start with an introduction of network designs utilizing a defense in depth strategy leveraging antivirus, IDS/IPS, and firewalls to protect hosts. Cadets will be introduced to the history, theory, and technology behind these tools, and how they are leveraged in home and enterprise networks. The corresponding challenge problem will consist of cadets circumnavigating four (4) example networks and defense systems of increasing security posture.

- *Code-Level Attacks*
  The lecture will cover code-level attacks primarily involving memory corruption through buffer overflows and memory information leaks. The lecture will guide the students through a set of hands-on exercises that introduce exploitation concepts and modern protections. All material used in this course is derived from publically available sources.

- *Reverse Engineering & Forensics*
  The two part lecture is a crash course in reverse engineering, cyber-forensics, and actionable threat intelligence principles. Interns will be introduced to x86 machine language, executable file formats, and obfuscation methods such as “packing”, "obfuscation," and “anti-debugging/anti-disassembly”. Interns will learn to utilize reverse engineering software such as IDApro and Ollydbg along with additional analysis tools to bypass these techniques. Lastly, interns will learn the principles of analysis – both static and dynamic – of malware analysis. The corresponding challenge problem will be analysis of a captured malware and investigation to compromise of the computer system.

- *Wireless Fundamentals*
  This lecture will provide students with a basic understanding of wireless technologies and their application in computer networking. Although physical layer aspects will be covered, particular focus will be placed on the wireless protocols and standards that form the basis of popular wireless technologies. The security and vulnerability of these will be studied in detail, including issues related to protocol security, encryption, and authentication. There will be several in-class exercises, and students will be assigned a challenging wireless security homework problem.

3.2.2 Tradecraft Activities

All tradecraft activities for the ACE 2018 are listed below:

- *Social Engineering*
  The Social Engineering Exercise introduces students to the topic of social engineering in the context of information systems (IS). It focuses on an academic methodology to educate students on how social engineering works; namely, it highlights how social engineering in the IS context relies on flaws in systems. The exercise accomplishes this in the framework of a short lecture, followed by an interactive exercise that steps students through use of open-source, industry standard tools for social engineering. Throughout, the exercise emphasizes methods to mitigate social engineering attempts through proper IS engineering.

- *Concord Dawn*
  Concord Dawn meets its education and training objective through a strongly integrated multi-domain operation executed in air, space and cyberspace. Participants support an air strike on a High Value Target through gathering and interpreting intelligence, developing a plan to achieve mission objectives, and executing that plan as part of a time phased mission.

- *SCADA*
  The SCADA lecture covers the fundamentals of SCADA systems, using physical hardware as examples to understand security and vulnerabilities of these devices. The students will learn about specific network protocols used to talk to these devices, the software architectures that sit on top of these devices, discover vulnerabilities within the devices, and exploit these vulnerabilities to understand the impact to these SCADA systems.

- *Code Hardening*
  Code-level hardening consists of activities undertaken by software developers, code reviewers, or testers to produce secure source code. In the Code-Level Hardening exercise, students explore code-level hardening by mitigating Perl and PHP vulnerabilities of a web application to prevent input-based attacks such as Cross-site Scripting and SQL injection.

- *Adversary Tactics*
  This intense course immerses students in a simulated enterprise environment, with multiple domains, up-to-date and patched operating systems, modern defenses, and active network defenders responding to Red Team activities. We will cover several phases of a Red Team engagement in depth: user profiling and phishing, host enumeration and “safety checks”, advanced lateral movement, sophisticated Active Directory domain enumeration and escalation, persistence (userland, elevated, and domain flavors), advanced Kerberos attacks, data mining, and exfiltration. Come learn to use some of the most well-known offensive tools from the authors themselves, including co-creators and developers of PowerView, PowerShell Empire, PowerSploit, PowerUp, and BloodHound.[1]

- *Code-Level Attacks*
  The tradecraft consists of a scenario in which the student must apply the knowledge from the lecture to successfully attack a system. All material used in this course is derived from publically available sources.

- *Privilege Escalation*
  The privilege escalation lecture covers one to two specific privilege escalation techniques focused on chroot jail breakouts and hypervisor escalation. The tradecraft has students perform hands on debugging and exploitation of the Venom vulnerability using the gdb Linux debugger. Students are required to compose shell code and inject it into heap memory to take advantage of the Venom bug.

- *Meltdown*
  This tradecraft will provide interns a conceptual and hands on appreciation for the meltdown attack in specific and hardware attacks in general. A review of germane computer architecture details such as caching, branch prediction, and out of order execution will be conducted. Interns will then learn and implement cache reading as a side channel, exploit out of order execution to read protected memory, and optimize the attack through memory conditioning and shell code.

3.3 RESEARCH EXECUTION

Research continued to be an essential part of the ACE experience. The ACE staff issued a call for topics and received several responses. The proposals were evaluated on feasibility of reaching a desirable end state and organizational fit. Staff accepted 6 proposals from three agencies: AFRL, DSTL, and NSA. Interns were divided between efforts and contributed 24 hours of research time a week.

[1] This Description was provided by Specter Ops, Inc

3.3.1 Research Topics

All research topics for the 2018 ACE are listed below:

- *Red Team Visualization*
  This effort develops a graphical management tool for Red Teams that visualizes targets and their exfiltration paths plus possible lateral movement candidates. This network security tool will allow for more effective red team collaboration allowing for shared sessions, data, and communication through a single Agent. This gives operators and leaders better situational awareness for planning, coordination and de-confliction.

- *Internet of Things Security*
  This effort is looking at the natural behavior of wearable Internet of Things (IoT) devices. By doing experiments and performing data analysis on devices and their interactions with open public networks. IoT is a rapidly growing space in the cyberspace domain. Unlike the air, space, land and sea domains, the cyber domain is created by humans and evolves with society. This proposed research intends to focus on the interaction between the IoT devices, specifically understanding the data collection between devices through the development of algorithms and data analysis.

- *Multi-Level Security Devops*
  The purpose of this research effort is to demonstrate a proof-of-concept for multi-level security DevOps. DevOps is both a philosophy and set of tools and techniques that enable technology developers to deploy new technology quickly and securely to operational networks. A critical aspect of this research is demonstrating the security mechanisms that need to be in place that mitigate the risks associated with shortened development timelines. Students will get hands-on experience learning about server hardware, container based micro-services, agile software development, cross-domain solutions (including Secure View and ISSE Guard), and how risk is managed on operational Air Force networks. This proof of concept will be a critical component to moving the project towards actual deployment.

- *Machine Learning Enabled Static Code Analysis*
  The red team automation effort brings the power of state-of-the-art machine learning to software vulnerability research, to create a tool that can identify vulnerabilities with better sensitivity than the best of breed static analyzers. This research will involve use of machine learning techniques, code parsing and analysis, graph databases, cybersecurity and vulnerability research.

- *Red team Automation*
  The proposed R&D effort would develop a software framework to automate Vulnerability Assessment and Penetration Testing (VAPT) and the Phases of the Cyber Intrusion Kill Chain through the Installation Phase. This effort would leverage and augment existing software, Application Programming Interfaces (APIs) and Interface

Control Descriptions (ICDs) to automate the end-to-end software as well as tactics, techniques and procedures (TTPs). [2]

- *Cyber Mission Effect Chain*
  This ACE R&D effort will have the participant(s) exploring the communications security of the multi-agent autonomy platform, performing research into options for implementing the communications security mechanism, the development/implementation of alternatives, and the measurement/characterization of alternatives under different assumptions and environmental conditions. This will culminate in a set of recommendations, supported by data, for implementation within the Cyber Mission Effect Chain (MEC) development, and for consideration by the platform system engineer for broader adoption. [3]

- *Nuisance-Ware Training Effects*
  This effort must develop a series of effects deployable on an existing implant. The effects shall disrupt and degrade productivity of the target by means attributable to causes such as a slow computer, user errors, or commonly occurring computer malfunctions. The purpose of the effect is to degrade war fighting ability of users on deployed systems and provided training targets for defensive cyber operation teams.

3.4 Leadership Execution

The ACE program's sharp focus on leadership is rare among internship programs. This focus has been with the ACE program since the beginning, and interns have often remarked that it is their favorite component. The primary way the program instills leadership principles into interns is by a weekly leadership seminar. These seminars are led by Colonel Frederick "Fred" Wieners, USAF (Ret). Interns are put into smaller groups for the seminar and there they engage in leadership case studies. The height of these seminars is a joint intern and staff retreat at the battle of Gettysburg historic site. Colonel Wieners is an accredited field guide and takes participants throughout the battlefield, imparting valuable leadership lessons in the historical setting.

Also unique is the ACE's focus on physical fitness and group physical training. Every Wednesday morning at 7:30 AM interns and staff are expected to 8 miles in less than 90 minutes. If needed, interns may start earlier at 7:00 AM and complete the 8 miles in 2 hours. These requirements work out to an average pace of Exemptions are granted for medical issues. Interns are graded based off their run performance, and are required to pass the run component to graduate. While some interns initially struggled with the run requirements, they improved and were able to graduate from the program.

[2] Description(s) provided by Chad Heitzenrater, PhD.

[3] Description(s) provided by Chad Heitzenrater, PhD.

3.4.1 Leadership Topics

The topics covered in leadership seminars are listed below:[4]

- *Introductory Lectures / Seminar*
  The opening lecture "Why Cyber Is Important" sets the stage by providing an appreciation of the growing importance of cyberspace over time, highlighting the lack of understanding relating to the opportunities and threats in this new domain. This session will also demonstrate why cyber leaders are important! A second lecture also takes a historical look at "Revolutions in Military Affairs" analyzing some patterns and conditions in past successful transformations in warfighting as well as demonstrating the causes of military failures and the impact of surprise.

- *Warfighting: Leadership and Critical Decisions*
  "Warfighting" will introduce the key concepts common in all warfare and will focus on the 'essence of military leadership' as well as the 'imperatives of command.' The lecture will use the American Civil War 'Battle of Gettysburg' to provide the context for our discussions.

- *Warfighting: Leadership and Critical Decisions*
  Our leadership development 'staff ride' to Gettysburg National Military Park will bring the vital 'essence of leadership' components to life and will demonstrate many of the vital concepts and strategies relating to warfare. The interns will analyze the critical decisions as well as the leadership and command styles of many of the key participants in order to determine what lessons are relevant for future cyber warriors and leaders.

- *Logic and Lexicon of Operational Design and Art*
  The purpose of these lectures and exercises is to foster an awareness of the 'logic and lexicon' of cyber operational planning. Interns will determine how to achieve cyber effects to compel an enemy to bend to our will by designing a cyber-operations plan enabling our national command authorities to deter and defeat adversaries.

[4] The majority of the following descriptions are credited to Colonel Frederick "Fred" Wieners, USAF (Ret)

- *Space Shuttle Disasters . . . Flawed Culture*
  In this seminar we will analyze the Challenger and Columbia space shuttle disasters to determine how flawed organizational cultures and structures can lead to decision failures. In addition, we will focus on the importance of individual courage and the need to promote a sense of mindfulness which can facilitate critical thinking and promote conversations necessary to avoid disaster.

- *Black Hawk Shoot-Down . . . 'Friendly Fire'*
  We will identify and analyze the flawed decisions at the individual, group and organizational levels in this tragic 1994 shoot-down of two U.S. Army Black Hawk helicopters by two U.S. Air Force fighters. We will also discuss and apply some contemporary thoughts on 'systems theory accident models' to understand how those tenets can be used in designing cyber related systems.

- *Cuban Missile Crisis . . . 'Thirteen Days'*
  Using the movie "Thirteen Days," we will explore how President Kennedy kept the two cold war nuclear powers from annihilating each other. Interns will apply several models in analyzing this compelling conflict, as well as appreciate the importance of 'deciding how to decide.'

- *9-11 . . . 'Failure of Imagination'*
  The terrorist attacks against the U.S. on 11 September 2001 were a tragic surprise representing a 'failure of imagination' and an 'inability to connect the dots.' Lessons learned in this case study may enable our interns to prevent future disasters in the cyber domain.

3.5 BLUE EDGE Execution

BLUE EDGE is a cyber-focused yet multi-domain exercise, and supporting infrastructure. BLUE EDGE seamlessly interweaves operations in cyber, air, ground, and space domains. The goal is fundamentally different than that of a capture the flag (CTF) event. Participants in a CTF utilize their skills in the cyber-domain to acquire points for the competition. Participants in BLUE EDGE must navigate the cyber and physical domains, using infrastructure they constructed, in a high stress environment modeling the fog and friction of war. The goal of a CTF is to increase technical knowledge, while the goal of BLUE EDGE is cyber warrior development. BLUE EDGE execution is broken down into 2 phases: preparation for war, and war proper.

The preparation phase takes the bulk of the summer. Interns are grouped into an east and west team upon arrival. These teams are fixed for the duration of the program. Interns perform a variety of system administration tasks: setting up web servers and chat channels, configuring routers and e-email, etc. Interns learn basic networking and service concept from this activity. The created and configured infrastructure also becomes the substrate over which interns perform their operations on. Interns engage in a variety of preparatory training missions. The training missions help prepare participants for the richness of the battle space. Team leaders and deputy are selected by staff, and lead team planning in the run up to the capstone. Team leaders receive operational orders and fabricated "intelligence" documents in the final phases of preparation.

The war proper phase takes place during the last week of the program. This event is known as the ACE capstone. The ACE capstone takes place offsite at AFRL/RI's Stockbridge test site. Interns are physically separated into command pods holding four interns each. Interns must communicate to their team mates using the communications services they set up in preparation for the event as cellphones are prohibited. This is a stressor that trains interns to operate under the fog and friction of war Interns operate over a textured battle space where they execute cross-domain fires in support of tactical and strategic objectives. A kinetic strike on a datacenter will greatly diminish the opposing teams computing resources. A cyber-attack against an air defense site will leave it disabled and the region subject to air raids. The following figure is an illustrative example of the tasks interns must complete during the capstone.

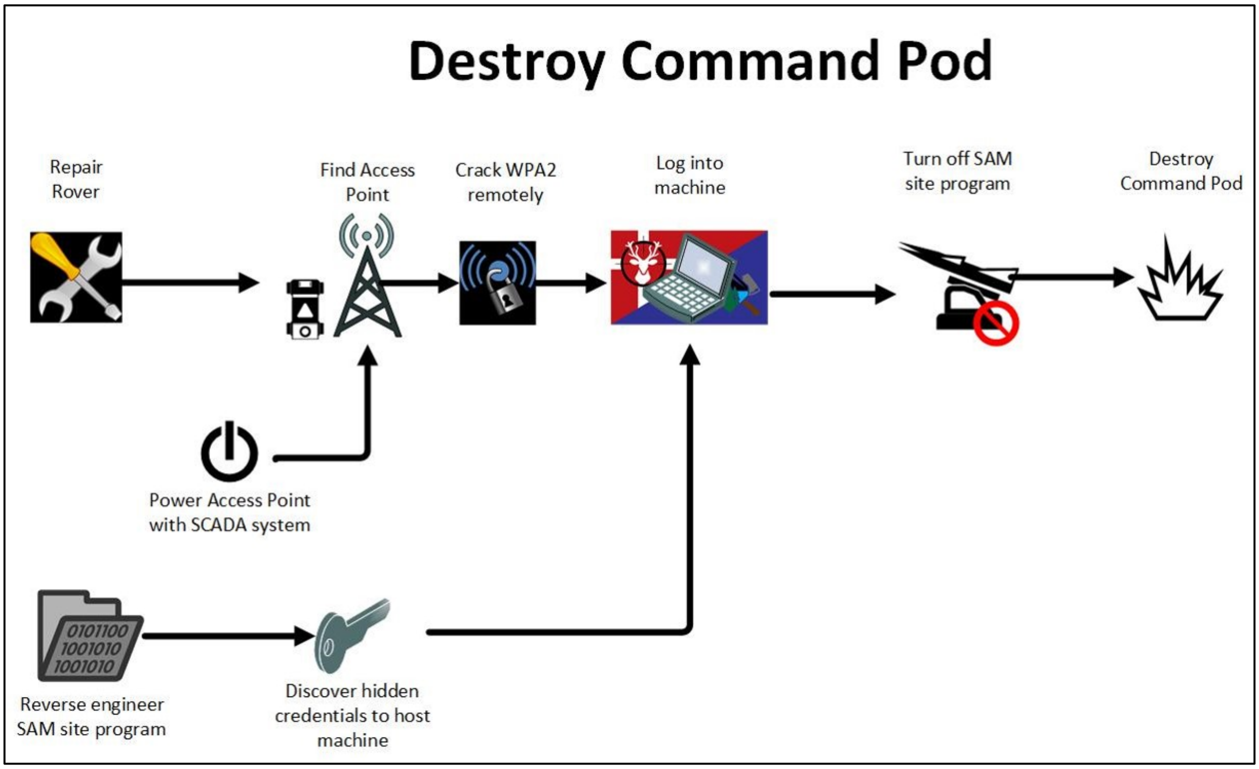
Destroy Command Pod
Repair Rover
Find Access Point
Crack WPA2 remotely
Log into machine
Turn off SAM site program
Destroy Command Pod
Power Access Point with SCADA system
0101100
1001010
1001010
Reverse engineer SAM site program
Discover hidden credentials to host machine

Figure 1. Example Capstone Killchain

4.0 RESULTS AND DISCUSSIONS

The ACE 2018 class graduated 29 first year interns and 3 teaching assistants. Interns left the program with a better understanding of the science of mission assurance, leadership, and warfighting the cyber domain. Interns from the UK went back to their positions in the MoD and strengthened their country's cyber capability, and strengthened the bond between AFRL, the USAF and UK counterparts. Active duty USAF officers returned to their assignments to contribute with their newly deepened knowledge of mission assurance. ROTC cadets received extensive preparation for their coming roles and officers and leaders. Civilian undergraduates left the program well prepared to serve their country as civil servants or economic contributors and thought leaders. The research performed by ACE interns successfully transitioned to the requesting agencies.

5.0 CONCLUSIONS

The ACE program matured significantly in 2018. The program's structure became more sharply defined and rigorous. All changes preserved the core of the ACE: technical excellence in the science of mission assurance synthesized with leadership principles to train the next generation of leaders and develop cyber-warriors. As the cyber environment continues to evolve the cyber warfare will become an increasingly important pillar of national military power. The structure of the ACE provides the rigorous pedagogical foundation required to mature the DoD workforce from industrial to information age warriors. In the next section, we provide recommendations for how the techniques, concepts and paradigms developed during the ACE can be used to create enduring value for cyber workforce and leadership development.

6.0 RECOMMENDATIONS

The 2018 ACE program formalized principles for the development of cyber warriors. In particular, the 2018 ACE advanced the state of the art in the conceptualization, design and execution cyber exercises. These principles have the potential to transform war gaming, exercises and competitions in the DoD to influence cyber warriors and operators.

We recommend the following future work to augment and increase the impact of the ACE across the DoD:

1. Exercises and competitions hosted by the DoD must focus on the synthesis of fundamental cyber skills in support of mission objectives
2. Break out operations from network building components into a formal operational chain the gradually builds capability to plan, execute and debrief
3. Cyber warrior development programs must educate for the future and train on the current state in order to guarantee effective current operators and relevant future operators
4. Lectures and tradecraft planning should be refined to better mutually support the others learning objectives
5. Greater outreach of the ACE program and AFRL/RI into the local community, top national universities and military training pipelines

7.0 REFERENCES

Armstrong, P. (2018, August 13). Bloom's Taxonomy. Retrieved March 21, 2019, from https://wp0.vanderbilt.edu/cft/guides-sub-pages/blooms-taxonomy/

LIST OF SYMBOLS, ABBREVIATIONS, AND ACRONYMS

90th COS – 90th Cyber Operations Squadron
57th IAS – 57th Information Aggressors Squadron
ACE – The Advanced Course in Engineering
ACT3 – AFRL Autonomy Capability Team
AFOTEC – Air Force Operational Test and Evaluation Center
AFRL – Air Force Research Laboratory
CAOC – Combined Air Operations Center
CONOP – Concept of Operations
CTF – Capture the Flag
DoD – Department of Defense
DSTL – Defense Science and Technology
GPA – Grade Point Average
MoD – Ministry of Defense
PBED – Plan Brief Execute Debrief cycle of mission planning
R&D – Research and Development
RI – Air Force Research Laboratory’s Information Directorate
ROTC – Reserve Officer Training Corps
RY – Air Force Research Laboratory Sensors Directorate
SFS – Scholarship for Service
SME – Subject Matter Expert
UAV – Unmanned Ariel Vehicle