The Army Cyber Institute

HISTORY REPORT
AY 2016 - 2017

THE ARMY CYBER INSTITUTE

In 2012, the Chief of Staff of the Army recognized the critical need for experienced Army cyber leaders, and an organization to provide a source of strategic insight and advice on cyber-related issues affecting the Nation. The Army created the Army Cyber Institute (ACI) at West Point and provided appropriated funding for its mission-essential requirements. Composed of multi-disciplinary civilian and military cyber experts and educators, the ACI is a national strategic initiatives group for cyber issues affecting the Army. It has a broad charter to conduct outreach with the Army, federal and state governments, academia, and the private sector at the tactical, operational, and strategic levels.

Reporting directly to the Superintendent of the United States Military Academy (USMA), the ACI develops intellectual capital with subject matter experts to expand the cyber knowledge base for Army cyber operations. This cyber focus will help the Army outmaneuver its adversaries in cyberspace and bridge gaps to promote information exchange across the military, government, academia, public and private sector.

The ACI's cyber enrichment activities provide West Point cadets, staff, and faculty with a wide range of opportunities to see how the material they cover in the classroom, and the leadership skills they develop at the Academy, map to the real world.

VISION AND MISSION

Vision
A premier institute that expands our knowledge of cyber conflict to prevent strategic surprise.

Mission
The ACI is a national resource for research, advice, and education in the cyber domain, engaging military, government, academic, and industrial cyber communities in impactful partnerships to build intellectual capital and expand the knowledge base for the purpose of enabling effective Army cyber defense and cyber operations.

YEAR IN REVIEW

The ACI History Report highlights many of the institute's accomplishments and efforts that took place during the academic year 2016-2017.

The ACI consisted of 53 military and civilian staff members. Many ACI members leverage over 500 faculty members from all disciplines across USMA. They have experience in Electrical Engineering, Computer Engineering, Cyber Ethics, Cyber Law, Behavioral Science, Mathematics, Cyber History, and Cyber Policy. The fellows and faculty are positioned in the Departments of Systems Engineering, Electrical Engineering and Computer Science, Social Sciences, Law, History, English and Philosophy, Mathematical Sciences, and Behavioral Sciences & Leadership.

The institute also welcomed the new Deputy Director, Mr. Christopher L. Hartley. Mr. Hartley has an extensive U.S. Army operational background with over 27 years of experience in strategic organization, cybersecurity implementation, and organizational level operations. He is a Certified Information Systems Security Professional (CISSP) and holds a Master's Degree in Network Security and Information Assurance.

FIRST SUMMER INTERNSHIP WITH ROTC CADETS

ACI hosted its very first summer internships for 4 ROTC Cadets in the summer of 2016. Zoe Schorr, a Mathematics major attending Worcester State University, Keenan Wresch, a Computer Science major attending Purdue University, Conrad Kress, a Mathematics major attending the University of Alaska, Anchorage, and Nick Celfo, a Computer Science major attending the Virginia Military Institute all helped to code and program brute force attack and defense algorithms associated with Big Data. Additionally, they co-authored an article entitled "Criminals Beware—The Future of FBI Cyber is Now" with LTC Ernest Wong and Assistant Special Agent in Charge, Richard Jacobs, of the NYC FBI Cyber Branch for *The Cyber Defense Review*.

The Big Data Lab was also the home for this summer's ROTC cadets under the direction of Mr. Erik Dean, ACI, Chief of IT and Security Operations, and the collaboration of Dr. Stephen Henderson, CMU SEI Researcher and former ACI Faculty and Researcher. These cadets leveraged a distributed computation and storage platform, and composed consumer-grade desktop computers.

They also optimized Apache Hadoop processing and discovered how to leverage the platform to generate thousands of fairly secure passwords and then break them in hours using normal distributed computing. This was the cadets' first exposure to non-Windows operating systems, distributed computing, programming, and password cracking.

CEMA SUPPORT TO CORPS AND BELOW (CSCB)

One of ACI’s priorities during AY 16-17 has been CEMA Support to Corps and Below (CSCB). During this time frame, CSCB conducted operations along four supporting efforts: Conventional Forces Support, Support to Leader Development, SOF Support, and Outreach. CSCB integrated CEMA into OPFOR operations at NTC, hosted Conventional and SOF CSCB Integration working groups, contributed cyber expertise to multiple working groups on warfare in Dense Urban Terrain (DuT), and authored and presented numerous articles and papers at academic outlets.

Additionally, CSCB integrated CEMA into CLDT at USMA, and provided multiple guest lectures and instructions to a myriad of cadet classes and clubs. Through these efforts, CSCB engaged with leaders and Soldiers from the military, academia, and public and private sectors to garner increased knowledge about CEMA operations, and their impact on the Army and the warfighter in the future. Through the last year CSCB has expanded familiarization of Electronic Warfare (EW) and cyber operations to educate USMA cadets and faculty during CLDT, which is intended to expose rising seniors to small unit tactics and assess them on their leadership ability.

This year, the ACI also partnered with the Department of Military Instruction (DMI) and Modern Warfare Institute (MWI) to continue demonstration of battlefield innovation with the cyber rifle in countering the enemy use of Unmanned Aerial Surveillance (UAS) / quad-copters. The MWI requested ACI build a virtual reality (VR) capability, and conduct a case study through the Department of Behavioral Sciences and Leadership (BS&L) to determine the level of confidence cadets would exhibit before the execution of physical leader's reconnaissance when exposed to this technology. The ACI developed a third capability with the integration of one operator to conduct cyber operational preparation of the environment (OPE). This cyber OPE accessed vulnerable Wi-Fi cameras to take manipulation of the full motion video feed.

The cadets used the video feed to provide the platoon leader's priority intelligence requirements (PIR) and identify enemy high valued targets on the objective.

Each cadet platoon per day received an attachment of either a cyber rifleman to neutralize the drone; or a cyber operator to access the cameras and incorporate into their planning process. All cadets familiarized with these new or emerging EW and cyber capabilities expressed that these enablers were value added to each platoon mission.

In addition to CLDT, members of team CSCB served as guest lecturers and subject matter expert panelists across several academic departments and clubs including Math, DMI, Social Sciences, Electrical Engineering and Computer Science Departments, and Irregular Warfare Group. In these engagements with cadets and faculty, team CSCB shared lessons learned and expertise from the operational force. Lastly, team CSCB supported the CLD Program as cadet mentors.

JACK VOLTAIC

Prepare | Prevent | Respond

Planning team from L to R: Chief Warrant Officer 3 Judy Esquibel (ACI), Scott Hagerty (CITI), Dr. Fernando Maymi (ACI), Anthony Vitello (CITI), John Cosgrove (CITI), Irina Garrido de Stanton (ACI), Stephen Ross (CITI), Arielle Budoff and Brian Wilson (CITI)

During the period of 29-31 August, 2016, the ACI in conjunction with Citigroup, executed a major city, multi-sector, public-private cyber exercise called Jack Voltaic (JV). It was the first step in building a framework to prepare, prevent, and respond to multi-sector cyber-attacks on major cities. A research experiment in the form of cyber exercise that involved players from first responders, emergency management, transportation, telecommunications, power, water, finance, and healthcare.

JV was designed to incorporate and correlate two parallel tracks consisting of 1) an on-range network defender versus attacker live-fire exercise (LFX), and 2) a facilitated table-top exercise (TTX) among senior sector leadership focused on events occurring in the virtual range play. The goal was to exercise and observe a city's ability, to collaborate in a coordinated response to any cyber-attacks.

Both components promoted exposure and opportunities to conduct collective cybersecurity training and enhance cross-sector information sharing practices. Developing the exercise in this manner helped ensure there was coordination both at the technical level and at the information sharing with the management level participating in the TTX. LFX participants were exposed to threat tactics, tools, and shared techniques.

[redacted]
citi
NYC Information Technology & Telecommunications
NYC Emergency Management
NYC Environmental Protection
NYU Langone Medical Center
AT&T
verizon
conEdison
MTA

Objective:

The primary objective was to identify an exercise framework and rehearse coordinated responses by any city to cyber events that affect multiple sectors.

Irina Garrido de Stanton and Chief Warrant Officer 3 Judy Esquibel, ACI members

First Responders during the Live-Fire Exercise

BIG DATA PLATFORM

Mr. Erik Dean, ACI Chief of IT and Security Operations in collaboration with Dr. Steve Henderson, CMU SEI Researcher and former ACI faculty member, deployed and tested a small-scale Defense Information Systems Agency (DISA) Rapid Deployment Kit (RDK) to determine the feasibility of deploying small data processing platforms at Army installations. DISA RDK is a core component of the Army Big Data platform and was tested with network simulation data captured from Jack Voltaic 1.0. The determination was that the small-scale deployment was unable to process large quantities of data in real-time while maintaining historical records without significant storage and processing requirements.

The ACI also began an initial investigation into Big Data-enabled Machine Learning to determine whether or not Machine Learning could leverage historical trends in network analytics to assess the likelihood of network-related cyber events. The ACI was able to leverage its strong partnership with one of the leading financial institutions to determine what work has already been done in this space and to make sure the existing work is relatively stable. This will give the ACI the ability to leverage partnerships with government and private sector to allow further research into Machine Learning (ML), Artificial Intelligence (AI), and Big Data.

THREATCASTING 2016

Participants from government, military, academia, and industry

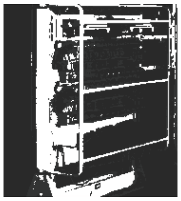
Participants during breakout group

In August 2016, twenty-five participants from government, military, academia, and industry gathered for two days to participate in a Threatcasting workshop to formulate possible future cyber threats. Threatcasting is a conceptual framework and process that enables multidisciplinary groups to envision threats ten years in the future, and then systematically plan what organizations and individuals can do to disrupt, mitigate, and recover from these threats.

The primary goal of the threatcasting and backcasting process was to model future cyber threats as dictated by curated technology, culture and business trends while exploring the implications on the ACI, Army, Department of Defense (DoD) and wider participants (public and private organizations, academic, general public). Our second goal was to come up with clear next steps that the Army could take as an organization to move towards the combined positive futures that we modeled while avoiding the negative futures.

Based upon the technological, cultural and economic shifts and advances in the next decade, we begin to see an evolving threat landscape emerging. This new reality of cyber and data security can be described as a widening attack plain. The attack surface in the future broadens out, including more people, increasing targets, and changing the very nature of security and threat.

CYBER TALKS – NEW YORK CITY



Cyber Talks was a semi-annual one-day event of high-impact, innovative ideas presented in a fast-paced and engaging format by thought leaders and rising stars from the defense, academic, industry, government, and non-profit communities.

Cyber Talks – New York City was held at the Alexander Hamilton Customs House in the Wall Street financial area in lower Manhattan on 8 September, 2016. The nine 20-minute presentations sought to inform, inspire, and sometimes even provoke while trying to foster creative solutions and intellectual capital for the cyber operations community.

The theme was “New Colossus”; a reference not only to the Statue of Liberty, a symbol of American values and a changing world order but also to the British government’s supercomputer Colossus that led to an Allied victory and change in cryptanalysis methods during World War II. We explored concepts that might emerge to lurch us from our cyber status-quo and to pursue domestic and international policies that advance technological and human innovation, which will fundamentally change cybersecurity.

Almost 300 people attended the event in person while others watched the limited live-stream. This was a successful opportunity to put diverse people and organizations together in one facility to exchange ideas and create future research relationships.

CYCON U.S. 2016

USMA Cadets with GEN (R) Keith Alexander, Mr. Ted Koppel and LTG Paul Nakasone during CyCon U.S. 2016

The inaugural U.S. based International Conference on Cyber Conflict took place 21-23 October, 2016 in Washington D.C. Focusing on a theme of *Protecting the Future*, CyCon U.S. sought to create more significant information exchange among industry, academia, and government entities at both the national and international levels.

Additionally, the conference brought together decision-makers and experts from diverse backgrounds to approach the conference theme of *Protecting the Future* from legal, technology, and strategy perspectives, often in an interdisciplinary manner. The issues included the future of international cooperation, rising technical challenges and requirements, impending conflicts in cyberspace, and the potential for new legal frameworks, standards, and regulations.

CyCon U.S. is a collaborative effort between the ACI and the NATO Cooperative Cyber Defence Centre of Excellence. CyCon U.S. complements the NATO CyCon Conference held every spring in Estonia.

ACI team with Distinguished Speakers

Panel: Educating to Protect the Future

Powerful Keynotes *Speakers and Panelist*

Sen Mark Warner *Commonwealth of Virginia*
Keith Alexander *IronNet Cybersecurity*
Steven M. Bellovin *Columbia University*
Teresa Carlson *Amazon*
Dmitri Alperovitch *CrowdStrike Inc.*
Matthew Green *Johns Hopkins*
Melissa Hathaway *Harvard Kennedy School*
Fred Kaplan *Journalist/Author*
Mark Anderson *Palo Alto Networks*
Herbert Lin *Stanford University*
Angela McKay *Microsoft*
Terrell McSweeny *FTC*
Milton Mueller *Georgia Tech*
Sven Sakkov *NATO CCD COE*
Adam Segal *Council on Foreign Relations*
Bernard Skoch *Air Force Association*
Katie Moussouris *Luta Security*
Heather West *Mozilla*
Catherine Lotrionte *Georgetown University*
Gary Corn *US Cyber Command*
Marcus Sachs *NERC*

Ted Koppel *Journalist/Author*
Diana Burley *George Washington University*
Laura DeNardis *American University*
David Wajsgras *Raytheon*
Robert Kahn *Corp for Ntl. Research Initiatives*
Dmitri Alperovitch *CrowdStrike*
Shawn Henry *CrowdStrike*
James Lewis *CSIS*
Kevin Mandia *FireEye*
Sarah McKune *Citizen Lab*
Uzi Moscovitch *formerly of J6/C4i, Israel Defense Forces*
Michael Schmitt *U.S. Naval War College*
Ambareen Siraj *Women in Cybersecurity*
Kim Zetter *Wired/Journalist/Author*
Andrea Matwyshyn *Northeastern University*
Gail Slater *The Internet Association*
Trey Herr *Harvard Kennedy School*
Ed Goetz *Exelon Corporation*
Joel Langill *AECOM*
Richard J. Harknett *NSA/CSS*
Dave Aitel *Immunity, Inc.*

General Information

- Over 400 registered attendees from 16 countries
- 40% Government (119 government)
- 19 Congressional staffers
- 30% Industry (62 companies)
- 30% Academia (33 universities plus 50 students including USMA cadets)
- 16 foreign countries

UPCOMING CYCON U.S. 2017

The **2017 International Conference on Cyber Conflict U.S. (CyCon U.S.)** is scheduled for on 7-8 Nov 2017 at the Ronald Reagan Building in Washington D.C.

CyCon U.S. facilitates knowledge generation, information exchange, and the building of relationships across the cyber community, including participation from military, government, academia, and industry from around the world. The conference promotes interdisciplinary security initiatives and furthers research and cooperation on cyber threats and opportunities.

CyCon U.S. will explore The Future of Cyber Conflict related to these areas:

Cyber diplomacy Cybersecurity strategies and policies
Military strategy and doctrine
Government, industry, and academic cooperation
Cyber workforce development and readiness
Best practices in cyber education
Intelligence fusion and situational awareness
Integration of Machine Learning and
Data Science into cyber operations

Network resilience
Innovative and disruptive cyber research
Law and ethics in cyberspace
Information sharing
Cyber deterrence/cyber power
Cybersecurity training and exercises
Emerging opportunities, risks, threats, and vulnerabilities
Security practices for government and industry
Threat countermeasures

For additional information please visit the conference website: http://aci.cvent.com

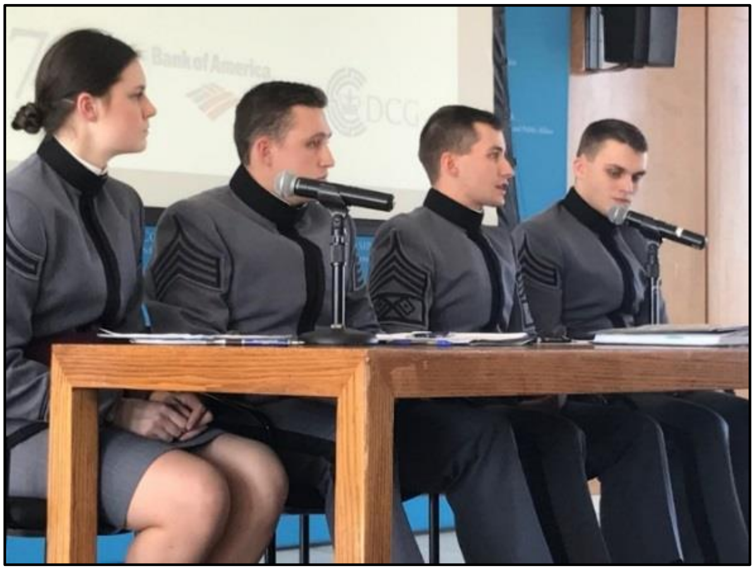
DEFENSE DIGITAL SERVICES

The joint Defense Digital Services (DDS)/ACI visit to the Southwest Asia Cyber Center (SWACC), located at Camp Arifjan, Kuwait, evolved out of Secretary Carter's desire to assist DOD agencies with technical problem solving. According to the tasking order signed by the secretary, "The Defense Digital Service (DDS) will partner with U.S. ARCENT, and the ACI to investigate, automate, and improve the network used in theater to support our forces in the CENTCOM region."

The 2-week visit provided temporary technical capability and capacity to assist the SWACC with a finite set of their intractable technical challenges. This effort was a combination of developing small-scale technical solutions, providing guidance on larger-scoped issues, and taking back a subset of problems to CONUS to work toward solutions. MAJ Natalie Vanatta and LTC Glen Robertson were the ACI component of the team joining with Mathew Weaver from DDS.

LTC Robertson and MAJ Vanatta were able to solve the theater's issue with the ArcSight infrastructure. They developed a custom solution of python, command line, and bash scripts to export the data from the old loggers, translate the events to the new logger schema format, and then import into the new logger infrastructure. During the visit, they were able to perform this action for all the BlueCoats and McAfee events on NIPR. The team left the custom scripts and explanations with the SWACC team as well as provided training on the system. The team also offered solutions to network monitoring issues across a diverse theater, ASI processing, and the troubleshooting of high-priority VTCs.

CADET CYBER POLICY TEAM



ACI members MAJ Shawn Lonergan and CPT Blake Rhoades formed and coached the USMA Cadet Competitive Cyber Policy Team in 2017. The USMA Cyber Policy team is an effort dedicated to the study and application of cyber policy. The team competes at the regional, national and international level in various cyber policy competitions, including the annual Cyber 9/12 Student Challenge. The team's purpose is to encourage competition and the honing of cyber policy skillsets within our Cadets.

The team competed in two national and one regional competition this academic year, winning the northeastern regional competition and advancing to the national semifinals.

The USMA Cyber Policy Team achieved excellence in November 2016 at the Atlantic Council's Regional Cyber 9/12 policy competition at Columbia University. Competing against 21 other teams (majority were graduate schools), the USMA team was the only undergraduate team to make it to the finals.

During the finals, the Cadets defeated three other teams to earn first place. They drew upon their knowledge of international affairs, cybersecurity, national security, and international law to demonstrate their mastery of policy concepts in the cyber domain.

The actions of these Cadets reflect well upon the Army and West Point's cyber policy initiatives; it shows the academic community and private sector that USMA is developing leaders that are prepared to face the challenges of the 21st century's complex operating environment. The Cadets spent countless hours preparing for this competition, and after the first day of the competition, they worked through the night to deliver a remarkable semi-final round brief. Their semi-final brief received accolades from the judges and their competitors. The other teams were impressed with the Cadets ability to handle pressure as well as their knowledge of cyber policy.

In April 2017, MAJ Shawn Lonergan and CPT Blake Rhoades, both ACI research scientists, took the West Point Cyber Policy Team to Geneva Switzerland to compete in the World Cyber 9/12 competition, were the West Point team were semi-finalists. The contest challenged participants to generate a whole-of-government approach to an evolving cyber-attack against public and private infrastructure. This contest challenged Cadets to generate responses that engaged the EU, NATO, and specific entities within affected European countries. CPT Rhoades commented that this was a "great way to finish the year and that it was thrilling to see several members of the team travel abroad for the first time in their lives."

In September 2017, the team will travel to Sydney, Australia to compete in the Indo-Pacific competition, against international undergraduate students. This is the first event of its kind in the region.

"The Indo-Pacific competition is hosted in partnership with the Atlantic Council and the University of Sydney's Centre for International Security Studies (CISS) and Sydney Cyber Security Network (SCSN). Student teams will confront a major cyber-attack of national and international importance. In response, teams will compose policy recommendations and justify their decision-making process, consider the roles and responsibilities of relevant civilian, military, law enforcement, and private sector organizations, and update their recommendations as the scenario evolves" (information by the atlanticcouncil.org).

Inaugural Team
Patrick Dancer
Hannah Fairfield
Chris Maixner
Margaret Goode

The Cyber Policy 9/12 multi-disciplinary team drew upon the strength of a variety of academic departments and programs:

AY 2017-2018:

- Hannah Fairfield - Human Geography, '18
- Lexi Johnson – International Relations, '18
- James Prunenski – Math, '19
- Robert Norwood – Computer Science, '20

Inaugural Team Members:

- Patrick Dancer - International Relations, '17
- Hannah Fairfield - Human Geography, '18
- Meg Goode – Psychology, '17
- Chris Maixner - Computer Science, '17
- Conner Wissman – Systems Engineering, '17

Coach - CPT Blake Rhoades, ACI Research Scientist
Coach – MAJ Shawn Lonergan, ACI Research Scientist
Assistant Coach - MAJ Brian Schultz, ACI Research Scientist

PANEL AT THE UNIVERSITY OF TEXAS LAW SCHOOL'S SYMPOSIUM

On 7 February 17, the ACI Cyber Law Fellow Robert Barnsby moderated a panel at the University of Texas Law School's Symposium for the Tallinn Manual 2.0 and the International Law Applicable to Cyber Operations. As an academic pre-launch of the second version of the Tallinn Manual, which is international law's preeminent cyber reference, the Symposium's four panels rigorously dissected chapters of the new Manual before its official release the following day at an Atlantic Council / NATO CCD CoE event in Washington, D.C. The Symposium and other associated events in Austin featured Mr. Barnsby as part of a select group of legal scholars including Professor Michael Schmitt, General Editor of the Tallinn Manual, Professor Jack Goldsmith, Harvard Law School, author of *The Terror Presidency*, Dean Bobby Chesney, Univ. of Texas Law School, co-creator of *Lawfare Blog*, Professor Bill Banks, National Security Law scholar and former Dean of Syracuse Univ. Law School, and Mrs. Dinah PoKempner, General Counsel, Human Rights Watch, among other distinguished legal scholars.

WOMEN IN CYBER SECURITY CONFERENCE (WiCyS) 2017

UNITED STATES MILITARY ACADEMY
WEST POINT
Army Cyber Institute
http://cyber.army.mil
Teaching Cybersecurity to Undergraduates:
The Benefits of Leveraging Multidisciplinary Project Teams to Develop Cybersecurity Solutions
Ernest Y. Wong
Chief of Staff, Army Cyber Institute
Assistant Professor, USMA Department of Systems Engineering
Katherine R. Hutton
Volunteer Research Scientist, Army Cyber Institute

ACI Researchers LTC Ernest Wong, Ms. Katherine Hutton, and CW3 Judy Esquibel attended the Women in Cyber Security Conference (WiCyS) 2017 from 30 March – 01 April 2017 in Tucson, AZ.

The Women in Cyber Security Conference (WiCyS) is not a women-only conference. It is a conference and community for women in cybersecurity, but the program is not limited to a specific gender. WiCyS was launched in 2013 with support from a National Science Foundation grant for a collaborative project between Tennessee Tech, University of Memphis, and Jackson State Community College. With support from various industry, government, and academic partners, WiCyS has become a continuing effort to recruit, retain and advance women in cybersecurity. The conference serves to empower women in this field where approximately 8-11% of the workforce is currently represented.

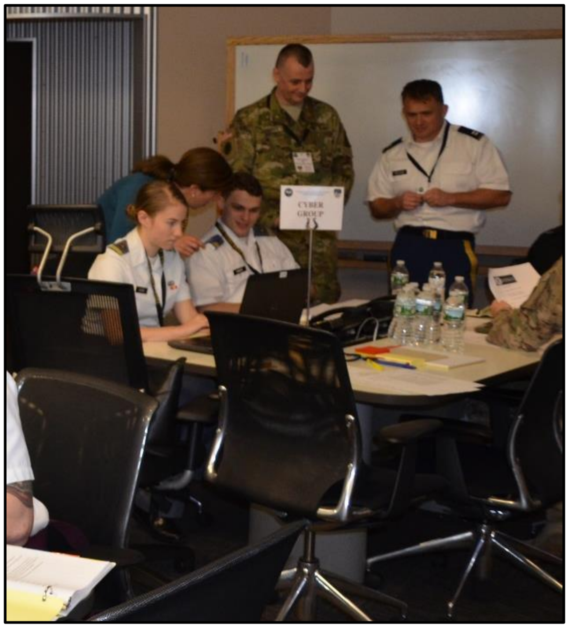
Ms. Hutton and LTC Wong presented research on "Teaching Cybersecurity to Undergraduates: The Benefits of Leveraging Multidisciplinary Project Teams to Develop Cybersecurity Solutions."

CYBER TERRORISM FUNCTIONAL EXERCISE: OPERATION "AMBASSADOR STRIKE"

On 9 November 2016, Chief Joseph W. Pfeifer of the Fire Department New York (FDNY) invited the ACI to participate and include Cyber Policy and Cyber Operations to this year's Functional Exercise for the first time during its eight years conducting it with the USMA's Combating Terrorism Center (CTC). ACI provided the Cyber Policy White Paper and Scenario for this exercise. ACI also provided links as the Cyber Lexicon Dictionary Options for the Homeland Security Class.

ACI participation in the planning and exercise included MAJ Shawn Lonergan, CPT Blake Rhoades, CPT Frederick Waage, Ms. Irina Garrido de Stanton, CW3 Judy Esquibel, and Ms. Katherine Hutton. Cadets from the ACI Cyber 9/12 Policy Team were Megan Goode '17 and Patrick Dancer '17. It also included representatives from the FDNY, members and cadets of the CTC and Homeland Security class, members of the NYS Division of Military and Naval Affairs, J-3 and JFHQ-NY, and The Maneuvering Center of Excellence at Ft. Benning, GA.

The team conducted several in-person and teleconference planning meetings before this year's exercise. The exercise took place at the FDNY building at 9 MetroTech, Brooklyn, NY, on 13 April 2017. The duration was 5+ hours to include a briefing to leadership.



FDNY leadership included Commissioner Daniel A. Nigro and FDNY Joseph W. Pfeifer Chief of Counterterrorism & Emergency Preparedness. The New York Air National Guard Major General Anthony P. German, Adjutant General NY.

Leadership expressed the importance of cyber in day-to-day security operations, and provided excellent feedback regarding the exercise.

"THE UNFITNESS OF TRADITIONAL MILITARY THINKING IN CYBER – FOUR CYBER TENETS THAT UNDERMINES CONVENTIONAL STRATEGIES"

Dr. Jan Kallberg, ACI Cyber Research Fellow, and Dr. Thomas S. Cook, former ACI Research Director, in May published in IEEE Access with the title: "The Unfitness of Traditional Military Thinking in Cyber - Four Cyber Tenets that Undermines Conventional Strategies" that highlighted the unique cyber environment with a lack of object permanence, which undermines the concept of maneuver; limited or absent measurement of effectiveness in offensive cyber, conflicts that are executed at computational speed, and anonymity.

TREATCASTING WEST

THREATCASTING WORKSHOP

1-2 May 2017
Tempe, Arizona

Exploring complex issues including the advancement of artificial intelligence, the diminishing ability to conduct covert intelligence gathering, the growing complexity of code, and the future division of work roles between humans and machines.

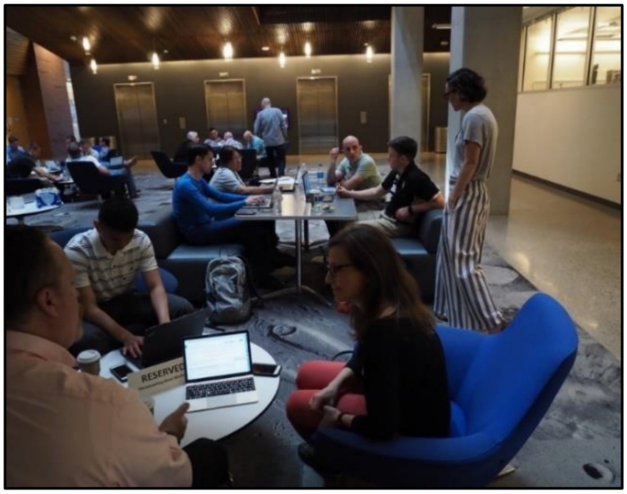
threatcasting.com

Contact threatcasting@usma.edu for more information.

In May of 2017, the Army Cyber Institute and the Threatcasting Lab at Arizona State University conducted Threatcasting West workshop.

With 47 participants from diverse organizations, we created 22 unique futures while exploring complex issues including the advancement of artificial intelligence, the diminishing ability to conduct covert intelligence gathering, the growing complexity of code, and future division of work roles between humans and machines. Attending Threatcasting West were a diverse group of government, academic, and private industry participants. Strategists and practitioners from the U.S. Secret Service, U.S. Army Network Enterprise Technology Command (NETCOM), Army Capabilities Integration Center (ARCIC), Assistant Secretary of the Army for Research and Technology (ASA R&T), U.S. Army Special Operations Center of Excellence (SOCoE), U.S. Army Cyber Command (ARCYBER), and the ACI represented government agencies.

They were joined by academics from Arizona State University, University of Arizona, and Northeastern University as well as cadets from West Point and the United States Air Force Academy. Industry provided futurists and technologists from Intel, Lockheed Martin, AECOM, Capital One, Illumnio, APICS, ISACA, Fractal Industries, Soar Technology, Strategic Foresight Partners, and BaldFuturist with expertise and a wide range of diverse perspectives. All attendees worked in small, collaborative, cross-industry groups to model futures taking place in the year 2027.



Work session Expert Interviews: Six curated inputs from cross-industry experts helped inform the futures we modeled. First was Dr. Genevieve Bell, discussing how we should think about interrogating AI. Sam Harris posed the question of how we might build AI without losing control over it. Dr. Dave Gioe outlined 14 cyber considerations for humans. Paul Thomas discussed how to approach Threatcasting from an economic perspective. Andre LeBlanc outlined the growth, impact, and future of applying AI to real-world industries. The sixth and final talk was MAJ Natalie Vanatta, Ph.D., with a wrap up of key ideas from various expert interviews regarding cyber growth and our relationship with machines. Transcripts of all talks will be made available in the final technical report**.**

CADET RESEARCH WITH THE DEPARTMENT OF MATHEMATICS

MAJ Natalie Vanatta enabled cadet research within the Department of Mathematics on relevant digital topics. Cadet Oliver DiNallo spent a year working on his honors research thesis where he investigated the effects of changing groups within El Gamal and RSA Encryption Schemes. Cadet DiNallo commissioned as a Cyber Officer and went immediately to the Naval Postgraduate School to complete his Masters' degree. Cadet David Weidman worked with MAJ Vanatta on neural networks as his math thesis. He used convolutional neural networks to train a basic artificial intelligence to play Go. He was in the midst of his research when an algorithm finally beat the world's master of Go.

MAJ Vanatta also worked with two cadets on their thesis research. Cadet Gabe Hake researched talent management analytics and their potential use in branching decisions for Army Cyber. Cadet Jake Schmitz applied network science principles to model the world's undersea communications cable network to determine if it could pose a national security risk in the future.

THE SECRETARY MICHAEL W. WYNNE CYBER LEADERSHIP AWARD

The Honorable Michael Wynne, the 21st U.S. Secretary of the Air Force, endowed the Secretary Michael Wynne Cyber Leadership Awards Program, in which the 2017 Convocation awarded the first cadet recipient for exceptional leadership in the cyber domain. The first awardee was CDT Christopher Maixner '17.

Cadet Maixner as a young cyber leader demonstrated excellence in both technical proficiency and a broader strategic knowledge of the domain. Cadet Maixner also demonstrated excellent leadership as a member of Cadet Policy Team, the West Point's elite hacking team, and the Competitive Cadet Cyber Team (C3T). He competed for the last two years on C3T, with his team placing first in the NSA's Cyber Defense Exercise (CDX) in 2016 and in the top three in 2017. He has been an active member of ACI/West Point's Cyber Policy Team, which won first place in the Regional Cyber 9/12 competition in November of 2016. The Cyber Policy Team has competed against over 40 schools (including Ivy League graduate programs and law schools) at both the national and international level. Cadet Maixner has been instrumental in the success of both teams and has shown academic prowess in the classroom. He is admired as one of the top Computer Science cadets at West Point, and was selected to commission as a Cyber Officer in May 2017. He served as the cadet officer in charge of the West Point chapter of the Special Interest Group on Security, Audit and Control (SIGSAC), an organization which espouses cybersecurity leadership and research.

CYBER HISTORY INTERVIEW

The West Point Center for Oral History published online, on 2 June 2017, the cyber oral history interview of ACI's Sergeant Major, MSG (P) Jeff Morris, which was conducted in studio by ACI History Fellow, Dr. David Gioe. The interview captures MSG (P) Morris' pioneering path from early enlistment to earning a Ph.D., branching cyber, and becoming an assistant professor at the US Military Academy. The interview can be viewed here: http://westpointcoh.org/interviews/a-pioneering-cyber-master-sergeant-earns-a-phd-and-becomes-a-west-point-professor

OPERATIONAL EXPERIENCE AT THE CYBER NATIONAL MISSION FORCE

COL Dan Bennett served a ten-month operational experience (22 Aug 16 - 15 Jun 17) as the Infrastructure and Special Projects Officer for the Commander of the Cyber National Mission Force, a joint 2-star command. COL Bennett led the execution of split-based operations being conducted for the first time, on networked infrastructure at three separate locations. This capability was directly referenced by the U.S. Cyber Command (USCYBERCOM) Commander, ADM Mike Rogers, on his 23 May testimony to the House Armed Services Committee. He led the final engineering, identification, and resourcing of space, equipment, and vendors as well as the accreditation of the interconnected network infrastructure to allow the national teams to execute operations worldwide from the CNMF's four key locations. In coordination with USCYBERCOM, COL Bennett also helped lead USCYBERCOM's first Defensive Cyberspace Operation's cloud solution with integrated analytic support to dispersed Cyber Protection Teams, and have it serve as a prototype to USCYBERCOM's Unified Platform.

THE CYBER DEFENSE REVIEW

VOLUME 1 • NUMBER 1
SPRING 2016
THE CYBER DEFENSE REVIEW
The Future of Army Maneuver-Dominance in the Land and Cyber Domains
Lieutenant General Edward C. Cardon
The U.S. Navy's Evolving Cyber/Cybersecurity Story
Rear Admiral Nancy Norton
Embedding Airmenship in the Cyberspace Domain
Major General Burke "Ed" Wilson
Protecting the Digitized Society: The Challenge of Balancing Surveillance and Privacy
Dr. Janne Hagen
Dr. Olav Lysne
Cyber Situational Awareness
Maj. Gen. Earl D. Matthews, USAF, Ret
Is There a Cybersecurity Dilemma?
Dr. Martin C. Libicki
INTRODUCTION
A Dynamic Multidisciplinary Dialogue
Colonel Thomas Cook
Dr. Corvin J. Connolly
BOOK REVIEW
Dr. Jan Kallberg
ARMY CYBER INSTITUTE • WEST POINT
VOLUME 1 • NUMBER 2
FALL 2016
THE CYBER DEFENSE REVIEW
Attacking Cyber: Increasing Resilience and Protecting Mission Essential Capabilities in Cyberspace
Lieutenant General Larry Wyche
Dr. Dawn Dunkerley Goss
Special Operations Forces Truths – Cyber Truths
Major General Stephen G. Fogarty
Major Jamie O. Nasi
Four Imperatives for Cybersecurity Success in the Digital Age: We Must Flip the Scales
Maj. Gen. John Davis, USA, Ret
Preparing for a Bad Day – The importance of public-private partnerships in keeping our institutions safe and secure
Mr. Thomas J. Harrington
Cyber Education via Mathematical Education
Professor Chris Arney
Major Natalie Vanatta
Major Thomas Nelson
Engaging Security and Intelligence Practitioners in the Emerging Cyber Regime Complex
Dr. Mark Raymond
INTRODUCTION
Discussions from the Front Lines of the Cyber Domain
Colonel Andrew O. Hall
BOOK REVIEW
Cyber War by Richard A. Clarke and Robert K. Knake
Professor Chris Arney
Second Lieutenant Joseph Kudrik
ARMY CYBER INSTITUTE • WEST POINT
WINTER 2017
THE CYBER DEFENSE REVIEW
Cyberspace in Multi-Domain Battle
Lieutenant General Paul Nakasone
Mr. Jamil N. Jaffer
Dr. Aaron Brantly
Mr. Andy Cohen
Colonel Andrew O. Hall
Dr. David Gioe
CYBER INSTITUTE • WEST POINT

The Cyber Defense Review (CDR) is a scholarly journal published by the ACI. The CDR publishes original, unpublished, relevant and engaging content from across the cyber community and is currently the only unclassified Department of Defense (DoD) sponsored journal that exclusively covers the cyber domain. Dr. Corvin Connolly, Editor-in-Chief, engineers a multidisciplinary dialogue through thought-provoking research articles and essays on the strategic, operational, and tactical aspects of the cyber domain. Oxford University Press listed CDR as one of the "top ten security journals to read as a crucial source for interdisciplinary perspective on cybersecurity."

The ACI signed an agreement with JSTOR to include the CDR in their open access digital library. JSTOR is the world's most prestigious digital library with a wide-range of scholarly content distributed through a technologically advanced platform. JSTOR will launch the CDR in early 2018 as part of a Security Studies collection. Through JSTOR, the CDR will reach 8,000 institutions and libraries in 176 countries.

Dr. Connolly forged a partnership with Fort Gordon's Joint Advanced Cyber Warfare Course (JACWCG) to screen/edit student papers for CDR publication. The CDR also partners with the USMA Department of Mathematical Sciences for online material dedicated to Network Science. The CDR has distributed 3,500 print copies to West Point and ACI distinguished guests and visitors, government and military leaders in the National Capital Region (NCR), and cyber stakeholders around the globe. The online CDR continues to post thoroughly researched articles and blogs designed to stir rapid discussion within the broader cyber community. The online CDR posted 35 articles, 18 blogs, and 4 book reviews. To read the most recent articles and blogs, visit http://cyberdefensereview.army.mil/

Sample of the prestigious CDR authors and articles:

Vol 1.
LTG Edward Cardon – "The Future of Army Maneuver Dominance in the Land and Cyber Domains"
RDML Nancy Norton – "The U.S. Navy's Evolving Cyber/Cybersecurity Story"
Maj Gen Ed Wilson – "Embedding Airmanship in the Cyberspace Doman"
Dr. Martin Libicki – "Is There a Cybersecurity Dilemma?"

Vol 2.
LTG Larry Wyche and Dr. Dawn Dunkerley Goss – "Attacking Cyber: Increasing Resilience and Protecting Mission Essential Capabilities in Cyberspace"
MG Stephen Fogarty – "Special Operations Forces Truths- Cyber Truths"
Mr. Thomas Harrington – "Preparing for a Bad Day - The importance of public-private partnerships in keeping our institutions safe and secure"
Dr. Paulo Shakarian – “Darknet Mining and Game Theory for Enhanced Cyber Threat Intelligence”

Vol 3.
LTG Paul Nakasone – "Cyberspace in Multi-Domain Battle'
GEN (R) Keith Alexander – "Clear Thinking about Protecting the Nation in the Cyber Domain"
Mr. Snehal Antani – "Cybernomics - Changing the Economics of Cyber Defense"
Mr. Eric Troup – “Growing Role of Platforms in Cybersecurity”

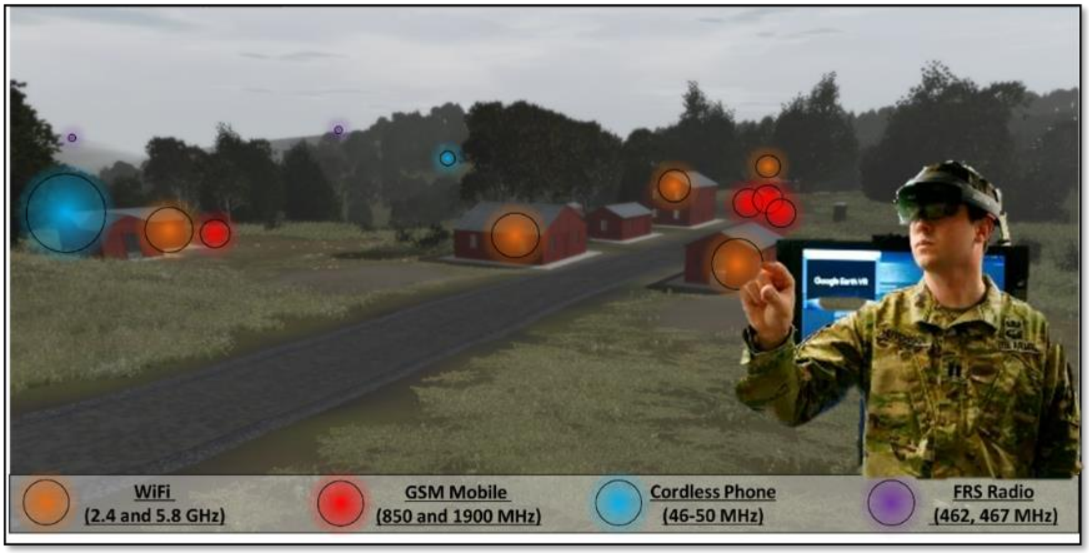
Vol 4.
MG John Baker and Dr. Steve Henderson – "The Cyber Data Science Process"
Mr. Rob Schrier – "Demonstrating Value and Use of Language-Normalizing Cyber as a Warfighting Domain"
Mr. Jim Routh – "The Emergence and Implications of Unconventional Security Controls"
COL Andy Hall and MAJ Brian Schultz – "Direct Commission for Cyberspace Specialties"

CADET CAPSTONE FINAL TECHNICAL REPORTS

LTC Ernest Wong met with members of the CENTCOM Joint Cyber Center at MacDill Air Force Base to brief them on the Cadet Capstone Final Technical Reports that addressed five of its research concerns: Benchmarking the Estonian Cyber Forces, Operationalizing Cyberspace, Assisting Partner Nation Cyber Defenses and Bolstering Trust, Educating the Force on Cyber, and Roles of the Officer in the US Cyber Branch. Furthermore, LTC Wong worked to finalize additional cyber-related research for Cadet Capstones for AY18.

LTC Wong briefed BG David Julazadeh, CENTCOM's Deputy Director of Operations, on the Cadet research; in turn, BG Julazadeh signed certificates of achievement for all 15 Cadets who spent last semester working on the CENTCOM JCC projects.

AUGMENTED REALITY RADIO FREQUENCY VISUALIZATION CAPABILITY (ARFVIS)

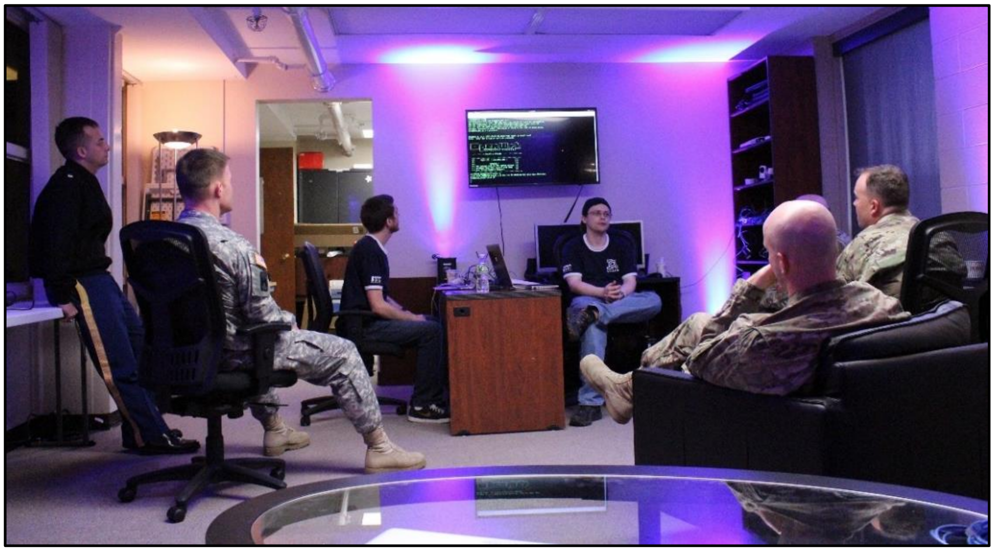


In conjunction with Dr. Steve Henderson’s (CMU SEI CERT CWD) Cyber Affordance Visualization In Augmented Reality, ACI SEG developed a project plan to create an Augmented Reality Radio Frequency Visualization capability (ARFVIS).Continued to research integration of topics of networked sensors, direction finding, and extended reality development.

Understanding the electromagnetic spectrum (EMS) and how its manipulation can affect military operations is difficult to both explain and to train. A major reason for this difficulty stems from the fact that the radio frequency (RF) spectrum is invisible to the eye and therefore difficult to visualize and place in a mental context. The ACI is researching tools that can help Signal, Cyber, and Electronic Warfare (EW) professionals visualize RF emissions emanating from a source radio, and provide multi-spectrum scanning and mapping, as well as geo-located source data in a see-through display, beyond the capabilities of common waterfall spectrum analyzers. Augmented Reality Radio Frequency

Visualization (ARFVIS) aims to help professionals who work with the electro-magnetic spectrum better understand the challenges and complexities of a contested spectrum, as well as providing kinetically-focused combat operators a tangible representation of the invisible environment around them, which can increasingly be both a tool and a threat.

INTERNET OF THINGS



Members of the ACI participating in the initial setup and training for the Internet of Things lab

One of ACI's main lines of effort this year has been to explore the Internet of Things (IoT) and how security can impact our everyday lives through home automation. The IoT refers to the ever-growing network of physical objects that feature an IP address for Internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems.

Members of the ACI used their experimental lab to develop a unique cyber-kinetic IoT demonstration that was shown to multiple visitors. This demonstration conveyed the impact connected devices will have in future operating environments including assisting military planners with conceptualizing the role cyber operations can have at the tactical level.

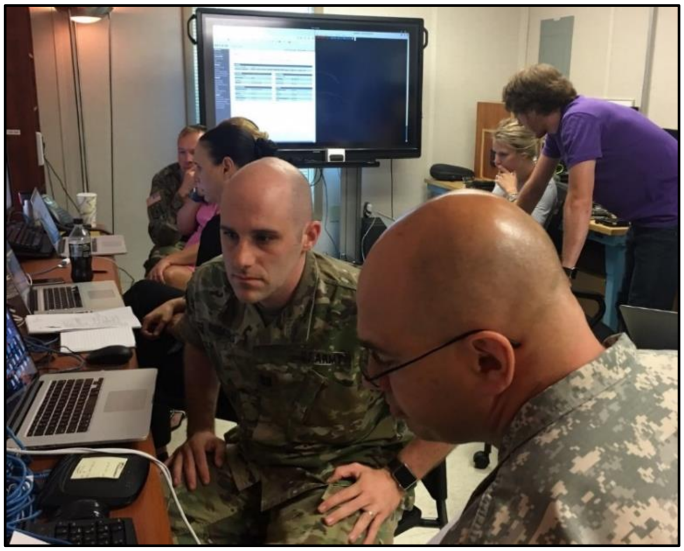
Over the last year, there have been focused efforts by NIST and DHS to provide security guidance to developers and users alike. Their efforts resulted in the release of these two sets complementary IoT security guidance in the below reports:

DHS and NIST release complementary IoT security guidance:
http://searchsecurity.techtarget.com/news/450403110/DHS-and-NIST-release-complementary-IoT-security-guidance

NIST's Network-of-Things Model Builds Foundation to Help Define the Internet of Things:
https://www.nist.gov/news-events/news/2016/07/nists-network-things-model-builds-foundation-help-define-internet-things

One ACI advisor often refers to the convergence of the physical and virtual domains. The IoT is part of the progression towards that eventual reality. Currently, the ACI, alongside other governmental and academic partners, is working to anticipate how IoT may be integrated into the future operating environment. In the future, IoT will be a necessary planning consideration for everything from strike forces to stability operations.

In 2017, the bipartisan Congressional IoT working group, which includes Senators Den Fischer (R-Nebraska), Cory Booker (D-New Jersey), Cory Gardner (R-Colorado), and Brian Schatz (D-Hawaii), introduced the Developing and Growing the Internet of Things (DIGIT) Act. The Bill seeks to encourage the growth of this globally interconnected network and identify barriers to its advancement.



Training on IoT device penetration testing

“The most important part of the Internet of Things aren’t things at all. They are people: the families, children, patients, and entrepreneurs whose lives could change through connected technology,” said Senator Fischer. “The DIGIT Act would open up the lines of communication between the private and public sector to help ensure our nation can seize the incredible benefits of this growing, global network.”

THE WEST POINT CYBER CHAIR

The West Point Cyber Chair, LTG (R) Rhett Hernandez, continues to provide invaluable advice to the ACI leadership and staff, the Cyber Research Center at the Department of Electrical Engineering and Computer Science (EE&CS), *The Cyber Defense Review* (CDR), and to the entire West Point team. The depth of his experience, combined with access to a vast network of senior leaders in government, academia, industry, and the private sector has improved cyber programs, and facilitated outreach, research, and education in the cyber domain.

LTG (R) Hernandez provides unparalleled mentorship and experience, which touched and impacted every member of the ACI organization. He has also leveraged the senior leadership of West Point and Army Cyber Command to advance the cyber mission.

LTG (R) Hernandez tirelessly logged over 64 external trips and meetings in his role as the West Point Cyber Chair. This number does not include numerous trips to West Point to mentor and advise cadets, faculty, staff, and leadership on cyber and military issues. LTG (R) Hernandez has engaged with numerous senior Army leaders in support of the ACI and National cyber mission: LTG Nakasone, Mr. Pontius, MG Morrison, and BG Rapp to name just a few. These engagements occurred during formal meetings, attendance at special events or through speaking engagements.

During a series of outreach engagements, the Cyber Chair led discussions to develop partnerships that included the meeting with Mr. Bob Butler from AECOM, which resulted in a partnership for the Jack Voltaic (JV) 2.0 exercise. JV is an exercise event, demonstrating the impact of a cyber-attack on a city, and its multiple critical infrastructure sectors. Additionally, an article for the CDR will result from this important dialogue. AECOM is a premier, fully integrated professional and technical services firm positioned to design, build, finance and operate infrastructure assets around the world for public and private sector clients.

LTG (R) Hernandez represented the ACI at several speaking engagements:
* AUSA Panel
* PANW IGNITE (ACI discussions)
* Army Cyber Institute at AFCEA (PANEL, Senior Leader Meetings)
* Army Cyber Institute (Veterans Day Panel)
* Modern War Institute at West Point (War Studies Conference)
* CNAS Keynote
* AFCEA San Antonio
* Cadet Class Discussion
* OFFSET Symposium
* Naples Founders Day

LTG (R) Hernandez will contribute his expertise and network of government and industry relationships to make CyCon U.S. 2017 the premier cyber conference in the United States.

PARTNERSHIPS

The ACI has partnered with Citigroup since 2013. This partnership has involved working on joint exercises and creating joint working groups on issues of mutual interest such as Big Data and critical infrastructure protection. An example of our partnership was the jointly hosted exercise called Jack Voltaic 1.0 (JV), a major city, multi-sector, public-private experimental cyber exercise.

AECOM

The ACI in conjunction with AECOM is in the planning stages for the execution of JV2.0. This robust public-private partnership between ACI and AECOM will provide expertise, resources, support, and new ideas necessary to enhance the cyber body of knowledge. The relationship between our organizations will inspire information sharing, the building of intellectual capability, and an enduring strategic partnership focused on the cyberspace domain.

CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

CyCon U.S. is a collaborative partnership between the ACI and the NATO Cooperative Cyber Defence Centre of Excellence. CyCon U.S. complements the NATO CyCon Conference held every spring in Tallinn, Estonia.

CyCon U.S. facilitates knowledge generation, information exchange, and the building of relationships across the cyber community, including participation from military, government, academia, and industry from around the world. The conference promotes interdisciplinary security initiatives and furthers research and cooperation on cyber threats and opportunities.

ASU

Arizona State
University

Threatcasting, ACI effort in partnership with Arizona State University (ASU), is a conceptual framework and process that enables multidisciplinary groups (public, private, and academic) to envision and plan systematically against threats ten years in the future.

Threatcasting not only describe tomorrow’s threats but also identify specific actions, indicators and concrete steps that can be taken today to disrupt, mitigate and recover from these future threats. The use of the Threatcasting process on cyber/digital problems is a joint effort over the next five years between Arizona State University’s School for the Future of Innovation in Society and the ACI.

The Threatcasting Lab was stood up at ASU to support this effort. More information about the process and the lab can be found at www.threatcasting.com as well as publications. One of the T-Lab’s stated goals is to conduct two workshops a year (alternating West and East Coasts) focused on creating relevant futures that partners, fellows, and students can then help solve. The pilot effort was held at West Point, NY in August 2016. The next workshop was held in Tempe, Arizona in May 2017.

PJM Interconnection (PJM) partnership was officially established on 27 February 2017 but was in development since December 2015 when Mr. Jonathon Monken, PJM's Senior Director, System Resiliency and Strategic Coordination conducted an initial visit to the ACI.

On 08 April 2016, the ACI partnered with PJM to host the Cyber Mutual Assistance Workshop (CMAW). During the CMAW practitioners and experts from the public and private sectors collaborated in a holistic approach to investigate energy sector issues. One of the objectives was to conduct a follow-on experiment to examine interdependencies among critical infrastructure sectors. During the event Mr. Tom O'Brien, PJM Vice President and Chief Information Officer, presented a brief "Use Cases for Cyber Incidents". The CMAW report will be available in the fall 2017.

PJM Interconnection is a regional transmission organization (RTO) and reliability coordinator (RC) that coordinates the movement of (bulk-energy) wholesale electricity in all or 13 states (Delaware, Illinois, Indiana, Kentucky, Maryland, Michigan, New Jersey, North Carolina, Ohio, Pennsylvania, Tennessee, Virginia, West Virginia and the District of Columbia.

ACI is currently conducting a collaborative study alongside PJM Interconnect leveraging the venue of an Energy Sector owned, cybersecurity exercise known as Grid Ex IV.

Grid Ex is a 2-year planning cycle, national-level, unclassified, public-private exercise designed to simulate a coordinated cyber/physical attack with operational impacts on electric and other critical infrastructures across North America to improve security, resiliency, and reliability. The exercise is led by the Electricity-Information Sharing and Analysis Center (E-ISAC) and North American Electric Reliability Corporation (NERC).

PJM-ACI intends is to conduct a collaborative study to develop a use case while leveraging the venue of GRID-Ex IV's Distributed Exercise Component. The study will evolve public-private partnerships, address gaps, and enable capability and capacity among the Energy Sector and the Army in defending the nation. The study will further examine the concept of "Cyber Mutual Assistance" to address crucial objectives to explore the governance around Cyber Defense Support to Civil Authorities (DSCA) for the National Guard supporting the energy sector and to gain insight into the critical technical skills likely needed in a cyber environment.

In the end, by leveraging partners, it enables opportunities and evolves the capability and capacity of our Cyber Force.

Army Cyber Institute (ACI)
Spellman Hall
2101 New South Post Road
West Point, NY 10996

To request additional copies or for inquiries, please email contact.cyber@usma.edu

ARMY CYBER
INSTITUTE
AT WEST POINT

**Army Cyber Institute (ACI)
Spellman Hall
2101 New South Post Road
West Point, NY 10996**