

Working Group 9 – Cyber Analysis

Co-Chair: Mr. David Silvernail
Space and Missile Defense Command (SMDC), Huntsville, AL.
david.l.silvernail.civ@mail.mil

Co-Chair: Mr. Paul Works
TRADOC Analysis Center (TRAC), Ft. Leavenworth, KS.
paul.w.works.civ@mail.mil

Warrant Officer Inventory Flow Model

[27 Oct 15, 1400-1430, Rm 14]

Allan Cain

United States Army Cyber Center of Excellence

allan.cain.civ@mail.mil

Keywords: 170A, 255-Series Warrant Officer

ABSTRACT: The United States Army Cyber Center of Excellence (CCoE) has developed an inventory flow model to forecast personnel requirements for a given Military Occupational Specialty (MOS). The 255 Series and the newly created 170A are examined using this model and the results are described in this work. Promotion, attrition, and MOS reclassification rates were represented by multiple independent Beta distributions. The number of iterations are determined by the user and the output of the simulation provides lower-bound, mean, and upper-bound values for each year of a five-year projection. Microsoft Excel was chosen as the medium to performing the simulations to allow for portability and ease of use.

This tool provides career managers with timely insights regarding the expected effects of accessions over time. With respect to 170A, the model indicated that the inventory plan under consideration would have negatively impacted the careers of the upcoming Warrant Officers. Our analysis efforts corrected the issue and improved management of the MOS.

Cyberspace Operations Analysis Task Force (COATF)

[27 Oct 15, 1430-1500, Rm 14]

Paul Page

U.S. Army Space and Missile Defense Command/Army Forces Strategic Command
Paul.a.Page6.civ@mail.mil

David L. Silvernail

U.S. Army Space and Missile Defense Command/Army Forces Strategic Command
david.l.silvernail.civ@mail.mil

Keywords: Cyberspace Operations, Cyberspace Studies

ABSTRACT: Cyberspace Operations has emerged as a key analytical focus area for the DoD analytic community, both technical and operational. At this time, multiple Army, Joint, and other service Cyberspace studies and related working groups are assessing cyber impacts on strategic, operational, and tactical operations. In the Fall of 2013, the U.S. Army Space and Missile Defense Command (USASMDC) and TRADOC Analysis Center (TRAC) analysis subject matter experts (SMEs) were tasked to meet and identify potential lanes of collaboration for Cyberspace analysis. Beginning in October, 2014, TRAC and USAMDC hosted a series of meetings of the Cyberspace Operations Analysis Task Force (COATF) to determine a baseline for Army cyber analysis methodologies and develop an Army analytic strategy focused on utilization of credible analysis techniques for cyberspace analysis. The briefing will review the COATF composition, objectives, process, and progress to date – to include the emerging results of the COATF Use Case Study on Defensive Cyberspace Operations Response Actions (DCO-RA) at Corps and below.

Concept for a Tactical Cyber Warfare Training Prototype for Current Live Virtual and Constructive (LVC) Simulations

[27 Oct 15, 1515-1545, Rm 14]

Christopher J. Metevier
US Army RDECOM ARL HRED STTC
Christopher.J.Metevier.civ@mail.mil

Henry Marshall
Army Research Laboratory (ARL)
henry.a.marshall.civ@mail.mil

Joseph McDonnell
Dynamic Animation Systems
Joe.McDonnell@d-a-s.com

Lana McGlynn
McGlynn Consulting Group
Lana.McGlynn@gmail.com

Keywords: Cyber Analysis, Live, Virtual, Constructive, and Gaming, Systems Engineering, Cyber Operations Battlefield Web Services, Modeling and Simulation

ABSTRACT: Current major simulations among the Live, Virtual, Constructive, and Gaming (LVC&G) domains lack a cyber implementation with the exception of a low fidelity cyber warfare effects simulation in the One Semi-Automated Forces (OneSAF) program. This shortfall was identified as a major technology gap in the simulation community.

To move towards a multi-domain cyber training solution, we conducted analysis of the problem space and developed an initial prototype to refine the user requirements as well as develop implementation architecture. The domain of cyber is very broad covering the whole range of mission command, weapon control, and information systems forcing us to pick the best focus to meet a likely Army use case.

After conducting a gap analysis among stakeholders, a clear missing capability was a cyber warfare mission command service that would work in a LVC&G training environment. The goal of this research is to develop a loosely coupled software service, called Cyber Operations Battlefield Web Services (COBWebS), that provides the capability to stimulate the effects of various cyber-attacks on command and control communication between the synthetic entities and the Blue mission command systems.

Our prototype leverages the Mission Command Adapter Web Service and adds cyber warfare effects modeling. Incorporating COBWebS in a LVC&G training event allows the trainee to recognize and make decisions that will minimize the attacks effects on overall mission. This presentation provides an overview of our front end analysis and conceptual prototype design to solicit feedback from the Army OR community.

Incorporation of Decision Making and Deconfliction in an Integrated Air and Missile Defense (IAMD) Scenario Using EADSIM

[28 Oct 15, 0945-1015, Rm 14]

Mr. Paul Chang
Mr. John Lumpkins
Center for Army Analysis
Paul.m.chang.civ@mail.mil

Keywords: Missile defense, integrated air and missile defense, IFF, Link-16, IBCS, cyber attack, sensor fusion, deconfliction, decision making, data functional descriptor, Ballistic and Cruise missiles, and Extended Air Defense Simulation (EADSIM)

ABSTRACT: Deconfliction of multiple sensors in an Integrated Air and Missile Defense (IAMD) environment has become increasingly important to effectively engage a diverse set of inbound threats. As the spoofing and jamming capabilities of airborne and missile threat systems become more complex and robust, the perception from different IAMD systems looking at the same threat can be different. This problem is complicated by the short time span from detection to impact for most threat systems. New IAMD systems use sensor fusion to present all sensor data to an IAMD commander for his/her engagement decision. In these scenarios, the IAMD commander must decide which sensor data is most reliable based on his/her knowledge of the threat. In this analysis, the data functional descriptor (DFD) within the Extended Air Defense Simulation (EADSIM) was used to code a decision-making and deconfliction hierarchy amongst different sensors. The DFD allows the user to rank the information provided by different sensors relative to each other in order to prioritize some sensors over others. Three different scenarios were modeled involving multiple external sensor inputs into a central decision making hub trying to engage a threat system with conflicting Identification Friend or Foe (IFF). All three scenarios involved the use of cyber attack to confuse the IAMD systems, thus resulting in conflicting IFF. One scenario involved incursion of new threat in a very time-sensitive situation with conflicting IFF. The scenarios were modeled using the current military tactical data exchange network, Link-16, as well as IAMD Battle Control System (IBCS).

Cyberspace Analysis: An Overview of the Cyberspace Domain and the Cyberspace Analysis Focus Areas of the Space and Missile Defense Command

[28 Oct 15, 1015-1045, Rm 14]

David L. Silvernail

U.S. Army Space and Missile Defense Command/Army Forces Strategic Command

david.l.silvernail.civ@mail.mil

Mike Thorne

U.S. Army Space and Missile Defense Command/Army Forces Strategic Command

gary.m.thorne.ctr@mail.mil

Keywords: Cyberspace, Cyber Studies

ABSTRACT: Cyberspace is a Domain -- man made, virtual, constantly expanding, and unique. It is not geographically constrained and can impact anyone anywhere within seconds. Land was once the dominant domain in ancient warfare and ancient armies fought for years to determine the outcomes. Today the Cyberspace Domain is causing a Revolution in Military Affairs (RMA). Military forces dependent on efficiencies gained by unprecedented C4I and smart weapons are at great risk. Those very efficiencies can be nullified very quickly and the Calculus of Warfare will change. Cyberspace will change warfare and the unprecedented rate of technological advance will make this domain more challenging to grasp than all the other domains and changes throughout the history of warfare.

The ground Warfighter is becoming increasingly reliant on the Cyberspace domain to win at the Strategic, Operational and Tactical levels of War. The analysis examines Cyberspace operational components and quantifies the operational impacts to the current and future Warfighter during Unified Land Operations. This analysis further seeks to determine the aspects of the cyberspace domain that impact the current and future ground Warfighter; to understand the impacts and effects of cyber operations; and to identify Cyberspace key terrain that require protection against Cyber Attacks.

The Army Space and Missile Defense Command (SMDC) Future Warfare Center (FWC) has completed seven studies in support of the Army Study Program (ASP) and Army Cyber Command (ARCC). These studies stem from the initial study proposal submitted in 2010. The focus areas include: (1) Brigade Combat Team (BCT) level Cyberspace Situational Awareness (SA) and key terrain identification; (2) Dynamic Cyber Defense (DyCD) in support of tactical operations; and (3) the integrating capabilities of the Cyber Electro-Magnetic Activities (CEMA) element across Cyberspace Mission Areas as identified and developed by the ARCC; (4) Defensive Cyberspace Operations-Response Actions (DCO-RA) in support of tactical operations; (5) The Landcyber 2 Study based on the Landcyber White Paper; (6) Extended Capabilities Study in support of the Tactical Commander; (7) the Army Equities in Cyberspace Study examining the Phase 0 and Phase 1 implications. The methodology has been to identify the first, second, and third order of cyberspace effects as determined by the ability to deceive, deny, degrade, disrupt, and destroy capabilities through the conduct of cyberspace operations in support of tactical operations. The specific focus was in the area of the overall impacts to combat operations through the utilization of constructive analysis capabilities to explicitly and implicitly modeling of cyberspace operations.

The overview of the SMDC FWC analysis of the cyberspace domain concludes by identifying some of the challenges inherent in the analysis of cyberspace operations and presents a way ahead to set the conditions for future analysis.

Cyberspace Key Terrain [28 Oct 15, 1300-1330, Rm 14]

Mr. John L. Cole
U.S. Army Research Laboratory
john.l.cole44.civ@mail.mil

Keywords: cyber, terrain, maneuver, targeting, fires

ABSTRACT: In the two-domain (land and cyber) warfare focus of the Army, Cyberspace Key Terrain (CKT) is a composite of terrain features from cyber and land domains, and these features include information and infrastructure elements.

Terrain features in the cyber and land domains intersect and overlap in a number of ways according to the variety and number of media and platforms, both fixed and mobile, used in the cyber infrastructure that exists in the battlefield; and from the reliance on information technology in the battlefield, including use of cyber-physical systems.

Land domain features such as “high ground” are analogous to the value and use of timely information, suggesting other analogs that cross domains.

CKT is dynamic, changing with time, circumstances, cyber topology, and physical location, although some attack pathways in that terrain may have longer persistence because of investment in their development.

Viewed in the context of cross-domain operations, and defined by the circumstances of the moment, CKT is still only one part of cyber operations, whether defensive or offensive, in which sets of interdependent maneuvers, agility techniques, terrain considerations, and complex targeting methods are employed.

Even so, understanding CKT enables commanders to categorize and prioritize assets according to mission criticality, both to protect them and to use them in cyber maneuvers directly affecting land operations.

Defining CKT for each circumstance is a significant burden, but the granularity is needed for appropriate selection and execution of maneuvers, for accurate battle damage assessment, for assessment of munitions effectiveness, for adherence to rules of engagement, and to achieve minimal collateral damage.

And a defined cyber terrain means that cyber fires may be used with targeting concepts analogous to “danger close” and collateral damage control in the land domain.

The footing CKT has in two domains, along with cyber domain contributions in terms of information and infrastructure elements presents a challenge to any who need a practical definition on the fly in circumstances that are unique from one moment to another.

But with awareness of the potential components of CKT and experience in evaluating this composite terrain, the challenge can be met.

Metrics for Tracking and Evaluating Cybersecurity Posture

[28 Oct 15, 1445-1515, Rm 14]

Ms. Jasmin Farahani and Dr. Natalie Scala
Towson University
nscala@towson.edu

LTC Paul L. Goethals
Army Cyber Institute
paul.goethals@usma.edu

Keywords: Cybersecurity, Decision Analysis, Value-Focused Modeling

ABSTRACT: In the context of security, businesses and agencies are frequently reminded of the vulnerabilities that exist in today's cyber environment. Data breaches continue to affect millions of computer users, while consuming valuable time, money, and other resources within the Department of Homeland Security, Federal Bureau of Investigation, and the Department of Defense. Privacy issues, the failure to find a standard in protection, and a constantly evolving cyber landscape all contribute to the complexity of the cybersecurity problem. In order to establish a benchmark for operational capability and facilitate decision making in this environment, analytical models are needed that provide a greater level of situational awareness with respect to the protection of information. Given the ability to assess an organization's degree of cybersecurity, the likelihood of predicting the location of a data breach may also increase.

To address this problem, our research objective is to identify a measure that evaluates the posture of an organization in defending against a cyberattack. Several examples of metrics in the decision analysis literature are presented that do or potentially might align with the measurement of cybersecurity posture. Then, an application of utility theory using techniques in optimization is explored in the design of an effective model. Extensions to future work in this area are also presented. The research is motivated by a Science of Security initiative that selected improved measurement capabilities as an area of emphasis that would benefit cybersecurity and defense programs.

Toward a Cyberspace Situational Awareness Capability

[28 Oct 15, 1545-1615, Rm 14]

Mr. William Jay Martin, CTR
U.S. Army Cyber Center of Excellence
d031785@iricp.osis.gov

Keywords: Cyber, Situational Awareness, SA

ABSTRACT: Nearly all U.S. Army capabilities ride on some kind of network, yet, there is currently no means to provide real-time situational awareness of the cyberspace domain for Army tactical combat units. This leaves tactical commanders blind to potential cyberspace threats and opportunities, lessens their ability to defend their own networks, and places the Army's network enabled capabilities at risk.

The Army considers cyberspace situational awareness a top priority, and several Cyber SA related platforms already exist, but the Army lacks the ability to aggregate, analyze, and synthesize the information, and then integrate a visual representation of that information into the common operational picture.

This paper establishes the necessity of Cyber SA, describes what is needed to achieve it, and then suggests how it can be integrated into the common operational picture at Army tactical echelons. It then provides a vignette to illustrate how Cyber SA might be used in the planning, preparation, execution, and assessment of future Army operations.

Virtual Radio Frequency (RF) Device Interactive Simulation Environment (ViRDISE)

[29 Oct 15, 0945-1015, Rm 3]

Kevin D. Sobczak
USArmy RDECOM CERDEC

ABSTRACT: Virtual Radio Frequency (RF) Device Interactive Simulation Environment (ViRDISE) is an entity-level 3D simulation program designed to model and simulate the effects of RF energy propagation in a realistic, operationally relevant environment. The main features of ViRDISE include a C# simulation server, 3D interactive environments powered by Epic Games' Unreal Engine 3 (UE3R), and various tools and methodologies to show RF propagation. RF systems are modeled using either the intuitive block diagram structure of MathWorks Simulink or by using the hardware-in-the-loop option provided by ViRDISE. ViRDISE calculates the propagation losses between all RF systems; this information is used in real time for either the Simulink model or the optional hardware-in-the-loop integration. The end-user can create custom vignettes by selecting an environment, adding assets, and assigning behaviors. ViRDISE can either run in a single-user, stand-alone mode or it can support multiple human-controlled nodes connected via TCP/IP. ViRDISE uses shared memory for interprocess communication between the C# simulation server, the game engine's host, and Simulink. Communication between the multiple simulation nodes is handled primarily through UE3's built-in data replication. In addition, transmitted RF propagation effects from terrain and antenna configuration can be visually displayed around RF systems. ViRDISE can be used as either a training aid or a modeling tool to assess operational effects of various RF systems. ViRDISE forms a framework in which integrating a popular, commercially available game engine and proven mathematical modeling tools can contribute to the modeling and simulation community.

Analysis of the Use of Intelligent Agents in Cyber Operations Testing

[29 Oct 15, 1015-1045, Rm 4]

Ethan Trewhitt, Stephen Lee-Urban, Ph.D., Joel Odom, Matthew Guinn, Trevor Lewis, Michael, Riley, Kevin Dickerson, Elizabeth T. Whitaker, Ph.D.

Georgia Tech Research Institute

Betty.whitaker@gtri.gatech.edu

George Thurmond, Ph.D., Emanuel Tornquist
PEO STRI/Threat Systems Management Office (TSMO)

george.e.thurmond2.civ@mail.mil

emanuel.m.tornquist.civ@mail.mil

Keywords: Intelligent Agents, Cyber Operations Testing, Threat Analysis

ABSTRACT: The goal of this study is to provide knowledge and understanding that will allow the Army to design, build or harden systems so that they are more resistant to cyber exploitation and to enhance the ability of Army systems to prevent, detect, react and recover from attacks.

A set of intelligent agents can be designed to collaborate to solve a complex problem, each agent having its own set of knowledge and expertise and being able to respond to requests from other agents for help in solving the problem. Agents can also act competitively working against each other using game theoretic approaches. An intelligent agent can contain or have access to knowledge about context or problem solving and can use any of the artificial intelligence reasoning techniques that are available to larger more comprehensive software modules. Some agents are mobile, that is they can move across a network to operate on multiple network nodes. Any of the intelligent agent paradigms could be used by cyber threat actors. Intelligent agents as individual intelligent software entities or as a collaborating set or as a swarm with emergent intelligence could be designed to manifest cyber offensive tactics, techniques or procedures (TTPs). We have provided an analysis of intelligent agent architectures and modeling and simulation approaches to evaluate their feasibility in cyber operations testing. This study includes an analysis of the design parameters of intelligent agent architectures and the implications of these parameter choices for agent behaviors in a cyber operations test. In order to motivate and support this analysis we provide several scenario use cases which envision the use of advanced intelligent agent teams in a cyber operations test. We have done a preliminary analysis of the feasibility of including these approaches in current Army cyber operations testing tools.