2019-06

Proceedings of the 20th Monterey Workshop

Luqi; Boger, Dan; Paduan, Jeffrey; Dell, Robert; Dinolt, George; Fouts, Douglas; Buettner, Raymond; Piombo, Jessica; Miller, Scot; Newman, James...

Monterey, CA; Naval Postgraduate School

https://hdl.handle.net/10945/62653

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun
NAVAL
POSTGRADUATE
SCHOOL
MONTEREY, CALIFORNIA

PROCEEDINGS OF THE 20TH MONTEREY WORKSHOP


June 2019

DISTRIBUTION A. Approved for public release: distribution unlimited.

Prepared for: Naval Postgraduate School Research Sponsored Programs Office.
# Proceedings of the 20th Monterey Workshop on Cyber

### Authors

### Date
30-06-2019

### Type
Final Report

### Dates Covered
10/2018 - 09/2019

### Security Classification
UNCLASS

### Abstract
This report is the proceedings of the 20th Monterey Workshop on Cyber held at US Naval Postgraduate School in Nov. 27-29, 2018.

### Subject Terms
Cyber, Security, Unmanned Systems, Architectures, Hardware, Software, Machine Learning, Insider Threats, Cyber Education, Command, Control, Communication, Computer, Intelligence

### Distribution
DISTRIBUTION A. Approved for public release: distribution unlimited.

### Notes
The views presented in this report are those of the authors and do not necessarily represent the views of DoD or its components.

### Contact
Luqi

---

### Table of Contents

<table>
<thead>
<tr>
<th>4. TITLE AND SUBTITLE</th>
<th>Proceedings of the 20th Monterey Workshop on Cyber</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</td>
<td>Naval Postgraduate School</td>
</tr>
<tr>
<td></td>
<td>1411 Cunningham Road Bldg 305</td>
</tr>
<tr>
<td></td>
<td>Monterey, CA 94943</td>
</tr>
<tr>
<td>9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)</td>
<td></td>
</tr>
<tr>
<td>10. SPONSOR/MONITOR'S ACRONYM(S)</td>
<td></td>
</tr>
<tr>
<td>11. SPONSOR/MONITOR'S REPORT NUMBER(S)</td>
<td></td>
</tr>
<tr>
<td>12. DISTRIBUTION / AVAILABILITY STATEMENT</td>
<td>DISTRIBUTION A. Approved for public release: distribution unlimited.</td>
</tr>
<tr>
<td>13. SUPPLEMENTARY NOTES</td>
<td>The views presented in this report are those of the authors and do not necessarily represent the views of DoD or its components.</td>
</tr>
<tr>
<td>14. ABSTRACT</td>
<td>This report is the proceedings of the 20th Monterey Workshop on Cyber held at US Naval Postgraduate School in Nov. 27-29, 2018.</td>
</tr>
<tr>
<td>15. SUBJECT TERMS</td>
<td>Cyber, Security, Unmanned Systems, Architectures, Hardware, Software, Machine Learning, Insider Threats, Cyber Education, Command, Control, Communication, Computer, Intelligence</td>
</tr>
<tr>
<td>16. SECURITY CLASSIFICATION OF:</td>
<td>a. REPORT UNCLASS</td>
</tr>
<tr>
<td>19b. TELEPHONE NUMBER (include area code)</td>
<td>831-656-2735</td>
</tr>
</tbody>
</table>
The report entitled “Proceedings of the 20th Monterey Workshop” was prepared for and supported by the Naval Postgraduate School Research Sponsored Programs Office.

Further distribution of all or part of this report is authorized.

This report was prepared by:

________________________
Luqi, Professor
Computer Science & Cyber Systems and Operations

Reviewed by:

________________________  __________________________
Peter Denning, Chairman  Dan Boger, Chairman
Department of Computer Science  Cyber Academic Group

Released by:

________________________
Jeffrey D. Paduan
Dean of Research
EXECUTIVE SUMMARY

The 20th Monterey Workshop on Cyber was held at the Naval Postgraduate School on Nov. 27-29, 2018. The NPS Provost, Cyber Academic Group Chair and Dean of Research chaired the workshop and led the workshop program committee with members from the Departments of Computer Science, Electrical and Computer Engineering, Information Sciences, Operations Research, and National Security Affairs. The workshop program consisted of five unclassified sessions, two panels, and one classified session. The presentation sessions addressed Cyber issues associated with unmanned/autonomous vehicles, Cyber challenges of Naval Operations, Cyber fundamentals and machine learning, and insider threats.

The first of two workshop panels discussed establishment of the Monterey Cyber Institute. In the second panel on Cyber Education, panelists and attendees exchanged curriculum related concepts and shared teaching experiences from Cyber education programs at the Naval Postgraduate School, the United States Naval Academy, and the University of Texas at San Antonio. These are among some of the largest Cyber education programs in the country, with more than 4,500 students.

One of the workshop conclusions was that Cyber education needs standardization. Different institutions have different views on what kind of preparation Cyber professionals need. These differences have to be reconciled, aligned with the needs of the Cyber community, and implemented at many educational institutions. There are accreditation bodies currently addressing these issues, and it is likely to take time for this process to converge on a community consensus. Related ideas that had support from the participants were that Cyber professionals need both theoretical understanding and hands-on experience with Cyber operations and related tools, and that simulated Cyber environments had a role to play in Cyber education and training.

It was recognized that machine learning could contribute to Cyber operations, and examples of such cases were presented. Cyber test facilities were described, including some that already have massive and growing datasets available, particularly with respect to autonomous vehicles. These datasets should be able to support new applications of machine learning in this area. There was great interest in how to check whether resulting
decision aids and autonomous subsystems are safe and secure, and multiple approaches to this were presented. It was pointed out that due to low cost of entry, the Cyber threats related to autonomous vehicles are rapidly evolving and that counter-measures must evolve rapidly to keep up. This puts a premium on balancing risks – delay in deploying solutions may have risk exposure comparable to or exceeding that of deploying imperfect solutions rapidly.

Another theme that emerged was how to mitigate risk posed by insider threats without alienating the loyal and conscientious majority of the Cyber workforce. The President of the United States issued an Executive Order on America’s Cyber Workforce On May 2, 2019, and an Executive Order on Securing the Information and Communications Technology and Services Supply Chain on May 15, 2019, see Appendices A and B.
# TABLE OF CONTENTS

## I. INTRODUCTION

A. MONTEREY WORKSHOP ON CYBER ................................................................. 1

B. GENERAL CHAIRS’ WELCOME REMARKS ..................................................... 2

C. WORKSHOP PROGRAM .................................................................................... 3

D. HISTORY ............................................................................................................ 5

## II. UNMANNED/AUTONOMOUS VEHICLES ..................................................... 7

A. M CITY AUTONOMOUS VEHICLE TESTBED ................................................ 7

1. Summary ............................................................................................................ 7

2. Facilities ............................................................................................................ 8

3. Research .......................................................................................................... 9

4. Consortium Structure ...................................................................................... 13

5. Findings .......................................................................................................... 14

B. RISKS OF INTEGRATING UAS INTO THE NATIONAL AIRSPACE SYSTEM ... 15

1. Summary .......................................................................................................... 15

2. Background ..................................................................................................... 16

3. Findings and Recommendations ..................................................................... 19

C. ENGINEERING LIGHTWEIGHT AUTONOMY ........................................... 20

1. Summary .......................................................................................................... 20

2. Background & Requirements ......................................................................... 21

3. Development ................................................................................................... 21

4. Conclusions and Implications ......................................................................... 23

D. UAV WITH MUNITION ................................................................................... 24

1. Summary .......................................................................................................... 24

2. Introduction ..................................................................................................... 25

3. Brief Discussion of Reliability Analysis .......................................................... 25

4. Bounding Method (Drone Case Study) ............................................................. 29

5. Conclusions ..................................................................................................... 32

E. TRACKING PROVENANCE OF AUTONOMOUS DECISIONS .................... 33

1. Summary .......................................................................................................... 33

2. Introduction ..................................................................................................... 33

3. Background and Motivation .......................................................................... 34

4. Intelligent Multi-UxV Planner with Adaptive Collaborative/Control Technologies (IMPACT) ................................................................................................. 34

5. Conclusions and Further Work ...................................................................... 40

F. AUTONOMOUS AERIAL SWARM ROBOTICS CYBER CHALLENGES ... 41

1. Summary .......................................................................................................... 41

2. Introduction ..................................................................................................... 41

3. Cyber Issues Studied ...................................................................................... 43

4. Conclusions & Recommendations .................................................................. 50

## III. CHALLENGES OF NAVAL OPERATIONS TO CYBERSECURITY ...... 51
# Table of Contents

## A. LVC SIMULATION SUPPORT FOR THE MARINE CORPS’ CEMOES 51
1. Introduction ........................................................................................................ 51
2. Summary ........................................................................................................... 52
3. Background ................................................................. ............................... 54
4. Proposed Solution ................................................................. .......................... 55
5. CEMOES ................................................................................................. 60
6. Role of MOVES .......................................................................................... 63
7. Integration of LVC ....................................................................................... 64
8. Future Work .................................................................................................... 65

## B. ZERO-DAYS, ONE OBLIGATION .......................................................... 65
1. Summary ........................................................................................................... 65

## IV. CYBERSECURITY ARCHITECTURES & HARDWARE .................. 67

## A. CONTINUOUS MONITORING, FRAGILITY, AND TRUST ............. 67
1. Summary ........................................................................................................... 67
2. Objectives and Background ................................................................. .......................... 67
3. Proposed Approach ....................................................................................... 70
4. Assessing Existing Supply Chain Risk .............................................................. 71
5. Conclusions ..................................................................................................... 75

## B. CYBERSECURITY ENGINEERING PLAN FOR NASA AIRSPACE

## OPERATIONS AND SAFETY PROGRAM (ASOP) ......................... 76
1. Summary ........................................................................................................... 76
2. Introduction ...................................................................................................... 77
3. Approach and Data ............................................................................................ 78

## V. PANEL ON MONTEREY CYBER INSTITUTE .......................... 89
1. Introduction ...................................................................................................... 89
2. Why Monterey? ................................................................................................. 89
3. How Can the Monterey Cyber Institute (MCI) be successful? ....................... 90
4. Questions for Consideration ............................................................................ 91

## VI. CYBER FUNDAMENTALS & MACHINE LEARNING ............... 93

## A. FUNDAMENTALS OF CYBERSECURITY .................................. 93
1. Summary ........................................................................................................... 93
2. Background ....................................................................................................... 94
3. Proposed Criteria ............................................................................................ 96

## B. NETBRANE: DETECTING AND PROTECTING FROM DDOS

## ATTACKS .................................................................................................... 102
1. Summary ........................................................................................................... 102
2. Problem Description and Approach ................................................................. 103
3. Status and Future Work .................................................................................... 116

## C. TIMING SIDE CHANNELS DUE TO HUMAN-COMPUTER

## INTERACTION ............................................................................................... 116
1. Summary ........................................................................................................... 117
2. Background ....................................................................................................... 117
3. Mitigation Strategies ......................................................................................... 121

## D. AI AND SAFETY/SECURITY THREATS ....................................... 123
1. Summary ........................................................................................................... 123
**LIST OF FIGURES**

Figure 1 – 20th Monterey Workshop Poster ................................................................. 2
Figure 2 - Key Trends in Personal Mobility ................................................................. 8
Figure 3 - The Mcity Consortium ................................................................................. 8
Figure 4 - Mcity Test Facilities ................................................................................... 9
Figure 5 - Mcity Driverless Shuttles ......................................................................... 9
Figure 6 - How V2V Helps Automated Vehicles ...................................................... 10
Figure 7 - Understanding User Behavior and Trust .................................................. 11
Figure 8 - The OpenCAV Platform ........................................................................... 11
Figure 9 - Mcity Datasets & Tools ............................................................................. 12
Figure 10 - Mcity Leadership Circle .......................................................................... 13
Figure 11 - Mcity Affiliate Program .......................................................................... 14
Figure 12 - Structural Issues .................................................................................... 14
Figure 13 - Technical Issues ..................................................................................... 15
Figure 14 - Myriad AI Security Challenges ............................................................... 17
Figure 15 - Four Domains ....................................................................................... 20
Figure 16 - Commercial Racing Drones .................................................................... 21
Figure 17 - Kestrel Control Board ........................................................................... 22
Figure 18 - Drone Carrier System ............................................................................ 24
Figure 19 - FTA vs. FMEA ....................................................................................... 26
Figure 20 - Scoring in FMEA ................................................................................... 27
Figure 21 - FMEA Example ...................................................................................... 28
Figure 22 - FTA Example ........................................................................................ 29
Figure 23 - Parrot Ar.Drone 2.0 ............................................................................... 29
Figure 24 - Severity and Probability Matrices ............................................................ 30
Figure 25 - Mishap Categories .................................................................................. 30
Figure 26 - Fault Tree for Communication Loss ....................................................... 31
Figure 27 – Results of FTA for the Parrot Drone ...................................................... 31
Figure 28 - Provenance Model Key .......................................................................... 34
Figure 29 – IMPACT Interface Mockup .................................................................... 35
Figure 30 - MAPLE FLAG IMPACT System ............................................................. 36
Figure 31 - Detailed IMPACT Diagram .................................................................... 37
Figure 32 - Dependency Change ............................................................................. 38
Figure 33 - Example RST Diagram .......................................................................... 39
Figure 34 – Anomaly (Policy Violation) .................................................................. 40
Figure 35 - ARSENL Platforms .............................................................................. 42
Figure 36 - Leveraging Open-source and COTS ....................................................... 42
Figure 37 - ARSENL Multi-UAV System Architecture ........................................... 43
Figure 38 - Typical air-to-air broadcast communications reliability ....................... 44
Figure 39 - Example GCS Interface .......................................................................... 45
Figure 40 - Typical On-UAV Architecture ............................................................... 47
Figure 41 - Typical Flight Control Architecture ....................................................... 49
Figure 42 - Initial CEMOES Concept developed in 2014 ....................................... 53
Figure 43 - Modeling a Noisy Environment .............................................................. 56
<table>
<thead>
<tr>
<th>Figure</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>88</td>
<td>NTP Attack Map</td>
<td>109</td>
</tr>
<tr>
<td>89</td>
<td>Packets/Bytes over Time</td>
<td>109</td>
</tr>
<tr>
<td>90</td>
<td>FPAC Two Passes</td>
<td>111</td>
</tr>
<tr>
<td>91</td>
<td>NTP (October 20, 2014) Scanners</td>
<td>112</td>
</tr>
<tr>
<td>92</td>
<td>Circle Diagram</td>
<td>113</td>
</tr>
<tr>
<td>93</td>
<td>Outlier Types</td>
<td>113</td>
</tr>
<tr>
<td>94</td>
<td>Pre-Attack Period</td>
<td>114</td>
</tr>
<tr>
<td>95</td>
<td>Attack Period</td>
<td>115</td>
</tr>
<tr>
<td>96</td>
<td>NTP Attack Packets over Time</td>
<td>115</td>
</tr>
<tr>
<td>97</td>
<td>– Assessment of Competing Approaches</td>
<td>116</td>
</tr>
<tr>
<td>98</td>
<td>Timestamps Exposed</td>
<td>117</td>
</tr>
<tr>
<td>99</td>
<td>Looking Back</td>
<td>118</td>
</tr>
<tr>
<td>100</td>
<td>Sender’s Fist in the 21st Century</td>
<td>118</td>
</tr>
<tr>
<td>101</td>
<td>Clock Tick Reveals OS Family</td>
<td>119</td>
</tr>
<tr>
<td>102</td>
<td>System Timer Effects</td>
<td>120</td>
</tr>
<tr>
<td>103</td>
<td>Determining Timer Resolution</td>
<td>120</td>
</tr>
<tr>
<td>104</td>
<td>Time Delay Embedding</td>
<td>120</td>
</tr>
<tr>
<td>105</td>
<td>Host Differences Revealed in Phase Space</td>
<td>121</td>
</tr>
<tr>
<td>106</td>
<td>Time Interval Obfuscation</td>
<td>121</td>
</tr>
<tr>
<td>107</td>
<td>Security/Usability Tradeoff</td>
<td>122</td>
</tr>
<tr>
<td>108</td>
<td>Keystroke-Level Anonymization Kernel</td>
<td>122</td>
</tr>
<tr>
<td>109</td>
<td>Homogeneity as an Indicator</td>
<td>123</td>
</tr>
<tr>
<td>110</td>
<td>Symbolic Analysis with Z3</td>
<td>125</td>
</tr>
<tr>
<td>111</td>
<td>Symbolic Analysis Engines</td>
<td>126</td>
</tr>
<tr>
<td>112</td>
<td>Microsoft’s Global Network</td>
<td>127</td>
</tr>
<tr>
<td>113</td>
<td>Network Verification</td>
<td>127</td>
</tr>
<tr>
<td>114</td>
<td>Network Powered Verification</td>
<td>127</td>
</tr>
<tr>
<td>115</td>
<td>Intent = Reality?</td>
<td>128</td>
</tr>
<tr>
<td>116</td>
<td>Scaling ACL &amp; Reachability Checks with Local Contracts</td>
<td>128</td>
</tr>
<tr>
<td>117</td>
<td>Scaling SAT/SMT with Lookaheads</td>
<td>129</td>
</tr>
<tr>
<td>118</td>
<td>– Requirements for Data Sharing</td>
<td>133</td>
</tr>
<tr>
<td>119</td>
<td>Facebook</td>
<td>136</td>
</tr>
<tr>
<td>120</td>
<td>Instagram</td>
<td>137</td>
</tr>
<tr>
<td>121</td>
<td>Tumblr</td>
<td>137</td>
</tr>
<tr>
<td>122</td>
<td>Reddit</td>
<td>138</td>
</tr>
<tr>
<td>123</td>
<td>Ancestry.com</td>
<td>138</td>
</tr>
<tr>
<td>124</td>
<td>PERSINT Puzzle Pieces</td>
<td>139</td>
</tr>
<tr>
<td>125</td>
<td>Theories to Combat Information Overload</td>
<td>140</td>
</tr>
<tr>
<td>126</td>
<td>Test Scenario 2</td>
<td>141</td>
</tr>
<tr>
<td>127</td>
<td>Experiment Design</td>
<td>142</td>
</tr>
<tr>
<td>128</td>
<td>– Findings</td>
<td>143</td>
</tr>
<tr>
<td>129</td>
<td>Types of Errors</td>
<td>144</td>
</tr>
</tbody>
</table>
THIS PAGE INTENTIONALLY LEFT BLANK
I. INTRODUCTION

From November 27-29, 2018, the Naval Postgraduate School hosted a workshop with attendees from academia, industry, and government to study the topic “Cyber” in Monterey. This workshop was the 20th in the Monterey Workshop series. Each of the previous workshops were focused on a specific, then-relevant topic. Details on past workshops can be found in Section I.D.

A. MONTEREY WORKSHOP ON CYBER

The Monterey Workshop on Cyber recognized that there was an urgent national need to provide assured and dependable software-intensive systems that can operate reliably in today’s contested network and computing environments. These systems and the personnel that develop, maintain, and use them are “a strategic asset that protects the American people, the homeland, and the American way of life”, as stated in the Presidential Executive Order 13870 reproduced in Appendix A.

The workshop explored current capabilities and gaps related to this national need. Potential participants were asked to present unclassified DoD concerns to industry and academic minds. The best papers were selected for presentation in order to familiarize researchers and practitioners with stakeholders’ issues, and to help them understand the feasibility and limitations of current and near-future technologies.

We emphasized interest in unmanned autonomous vehicles, managing the “internet of things”, future wireless communications using light (i.e., LIFI), and auto-tagging XML data based on user behavior and heuristics. Other areas of interest included Cybersecurity for military operations and baseline software/hardware, unmanned/autonomous systems, networked industrial control systems, and the relation between big data analysis and decision-making. How could machine learning, big data analysis, secure software/hardware architectures, AI, and other science methods enable the Cyber workforce to counter insider threats, integrate physical security, and conduct offensive Cyber operations? Is industry ready for the challenges and does it have solutions and tools to overcome the obstacles to secure Cyber operations? We worked together to find answers to questions like these in the 20th Monterey Workshop. The workshop poster is
shown in Figure 1.

Figure 1 – 20th Monterey Workshop Poster

General Chairs:                  Steve Lerman, Provost
                                 Dan Boger, Cyber, IS & C4I Chair

Program Committee Chair:        Jeff Paduan, Dean of Research

Committee Members:              Douglas Fouts, Electrical & Computer Engineering
                                 George Dinolt, Computer Science
                                 Robert Dell, Operations Research
                                 Jessica Piombo, National Security Affairs

Local Arrangement Chair:        Sharon Runde, Associate Cyber Chair

Committee Members:              LCDR Dave Couchman, US Navy
                                 Andre Xie & Karen Darken, Interns

Monterey Workshop Series Chair: Luqi, Computer Science & Cyber Group

B. GENERAL CHAIRS’ WELCOME REMARKS

The General Chairs, Dr. Steve Lerman, Provost of the Naval Postgraduate School and Prof. Dan Boger, Chair of the Cyber Academic Group, welcome you to Monterey, California for the 20th Monterey Workshop on Cyber.

There is an urgent national need to provide assured and dependable software-intensive systems that can operate dependably in today’s contested network and
computing environments. This workshop provides a forum for discussion and communication to align academic efforts with this need, and it solicits innovative solutions to Cyber problems that offer an achievable path to Cybersecurity assurance at all levels of the system. As in previous Monterey Workshops, the leading computer scientists, software and system engineers in government, academia, and industry are invited as well as Cyber agencies from around the nation. There will be both classified and unclassified sessions at the workshop.

For a quarter-century, the Monterey Workshops have served as an influential forum for exchange of ideas and experience in software-intensive systems. Given the current state of industry, there are obvious challenges to fully secure functioning Cyber systems. This workshop provides a fantastic opportunity for all of us to work together on innovations for Cyber problem solving.

C. WORKSHOP PROGRAM

Day 1, Tuesday 11/27/2018

08:00-08:30 Registration & Check In

08:30-08:45 Workshop Chairs’ Remarks

08:45-10:15 Unmanned/Autonomous Vehicles in Cyber

- Autonomous Aerial Swam Robotics Cyber Challenges, Duane Davis, NPS
- Mcity Autonomous Vehicle Testbed, Brian Noble, University of Michigan
- Risks of Integrating UAS into the National Airspace System, Brian Smith, NASA Ames

10:15-10:30 Break

10:30-12:00 Unmanned/Autonomous Vehicles in Cyber - continued

- Engineering Lightweight Autonomy, Nicholas Weaver, UC Berkeley and the International Computer Science Institute
- UAV with Munition, Valdis Berzins, NPS
- Tracking Provenance of Autonomous Decisions, Doug Lange, Space and Naval Warfare Systems Center

12:00-13:00 Lunch

13:00-14:00 Challenges of Naval Operations to Cybersecurity

- LVC Simulation Support for the Marine Corps’ CEMOES, Chris Fitzpatrick, NPS
14:00-15:00 Cybersecurity Architectures & Hardware
- Continuous Monitoring, Fragility and Trust, Ron Durbin, AFIT
- Cybersecurity Architectures and Hardware Issues, Brian Smith, NASA Ames

15:00-15:15 Break

15:15-16:30 Panel on Monterey Cyber Institute, Jeff Paduan (Chair), Jim Newman, Dan Boger, & John Drummond

Day 2, Wednesday 11/28/18

08:45-10:00 Cyber Fundamentals and Machine Learning
- Fundamentals of Cybersecurity, Dave Dampier, University of Texas, San Antonio
- NetBrane: Detecting and Protecting from DDoS Attacks, Stephen Hayne, Colorado State University

10:00-10:15 Break

10:15-12:00 Cyber Fundamentals and Machine Learning
- Timing Side Channels Due to Human-Computer Interaction, Vinnie Monaco, NPS
- AI and Safety/Security Threats, Brian Smith, NASA Ames
- Securing & Breaking Cyber Using SMT, Nikolaj Bjørner, Microsoft

12:00-13:00 Lunch

13:00-14:30 Insider Threats
- Personal Intelligence (PERSINT), William Roof, WHR
- Self-equity - A Trustworthiness Construct, Ryan Kelly, US Army
- Information Systems and Insider Threats, Sharon Runde, NPS

14:30-15:00 Break

15:00-16:30 Panel on Cyber Education and Cyber Physical Systems, Paul Tortora (Chair), Tracy Emmersen, Duane Davis, & Sharon Runde

Day 3, Thursday 11/29/18

08:30-10:00 Classified Cyber Issues in Military & Civilian Conflict

10:00-10:15 Break

10:15-12:00 Roundtable Discussion, Workshop Summary & 21st Workshop Plan
D. HISTORY

The objective of the Monterey Workshop series since its inception has been to increase the practical impact of scientific methods in computer science and engineering. Many of the world’s leading researchers have participated, and topics have included computer science, software and system engineering requirements and tools, innovation on systems, big data and cyber, and many other technical disciplines. The Workshop seeks to improve software practice via the application of engineering theory and to encourage foundational scientific results using formal methods and sound system models.

The Monterey Workshops have been an influential forum for aligning scientific research and innovations among academia, industry, and government agencies since 1992. The Workshops have developed productive research directions that have been adopted by various sponsors, and advanced the capabilities of various researchers. The titles of the past Monterey Workshops are:

1st 1993 Software Slicing, Merging and Integration [2]
2nd 1994 Software Evolution [3]
7th 2000 Modeling Software System Structures in a Fastly Moving Scenario [8]
8th 2001 Engineering Automation for Software Intensive Systems Integration [9]
11th 2004 Software Engineering Tools: Compatibility and Integration [12]
13th 2006 Composition of Embedded Systems: Scientific and Industrial Issues [14]
17th 2012 Development, Operation and Management of Large-Scale Complex IT Systems [18]
18th 2016/Feb. Integrity of Industrial Control System & Future Command & Control [19]
20th 2018 20th Monterey Workshop on Cyber
The Monterey Workshops have always focused on areas at the edge of the state of the art with potential for improvements that will shift the entire paradigm. Suggestions regarding the most important next step forward are always welcome. For further information on the workshop series, see the Monterey Workshop websites [21].
II. UNMANNED/AUTONOMOUS VEHICLES

Many of the workshop participants were concerned with Cyber aspects of unmanned and autonomous vehicles [22] [23] [24] [25] [26] [27]. The first presentation by Brian Noble explained the work of the Mcity Autonomous Vehicle Testbed at the University of Michigan. Brian Smith’s presentation laid out the potential risks posed by the integration of machine learning and AI into the aviation industry. The third presentation by Nicholas Weaver explained his work on developing a cheap and effective anti-drone drone. The fourth presentation by Valdis Berzins examined how risk-based testing could be applied to autonomous vehicles that operate in contested Cyber environments. The fifth presentation by Doug Lange studied the necessity of tracking the provenance of autonomous decisions. The sixth presentation by Duane Davis studied the challenges inherent to operating swarms of UAVs. This session was chaired first by Bryan O’Halloran and then by Brian Bingham.

A. M CITY AUTONOMOUS VEHICLE TESTBED

Presenter: Brian Noble, University of Michigan

1. Summary

The Mcity Autonomous Vehicle Testbed is a public-private partnership for vehicle testing and pre-competitive research. This facility has conducted 3,500+ hours of testing in a virtual environment using simulation tools. It operates the largest Dedicated Short-Range Communication (DSRC) fleet in the United States. The project has found that an augmented reality environment speeds testing and deployment. This allowed the project to deploy a Level-4 Connected and Automated Vehicle (CAV) on the campus of the University of Michigan. The project developed V2V support for autonomy using the OpenCAV platform with Hybrid Lincoln MKZs (NAVYA, open source, Lincoln & Kia), and identified four key trends in personal mobility, as shown in Figure 28.

The project recommends that vendors participate in pre-competitive research, explore user behavior and trust, share in datasets and tools, leverage significant existing partnerships, and give early access to facilities and data.
2. Facilities

The Mcity consortium provides a unique combination of research, laboratories, and education as shown in Figure 39.

Features of the Mcity test facility are shown in Figure 410. The objectives of the test facility are to provide an augmented reality environment for CAVs, an Accelerated Evaluation Model and test protocol for AVs, and an implementation of 5G for CAV research. This will enable rapid learning in real-time and speed AV innovation, as well as reducing development costs.

The objectives of the Living Labs are to provide a certified DSRC sustainable test environment with 2500 vehicles and 60 intersections, and to deploy two Level 4 CAVs to serve the community. This provides a reference for national testing and market deployment for partners, as well as enabling fast prototyping of V2V and V2I
applications, optimization of complementary forms of CV technology, gaining early insights, and removal of CAV deployment barriers. Pictures of the driverless shuttles developed by Mcity are shown in Figure 511.

3. Research

The barriers to CAV deployment that the project identified include:

- User trust & acceptance
- Legal, liability & insurance
- Market adoption
Privacy and security
AV testing and evaluation
The insights the project gained are related to:
Societal impact, energy, safety, etc.
Connectivity enabled AV
New business models

The benefits of V2V communication are illustrated in Figure 612. The car shown in the foreground is stopped in the middle of the road, out of sight around a blind turn.

The project also conducted research to understand user behavior and trust. A map of the test route as well as a diagram of the sensors used are shown in Figure 713.

Figure 6 - How V2V Helps Automated Vehicles
The OpenCAV platform used in this test is a modified Lincoln MKZ (hybrid). A diagram of the modifications made is shown in Figure 8.

The MKZs used in the tests had the driver and passenger seats reversed. The test subject, simulating a user of an autonomous vehicle, was seated in the left-front seat and wore various physiological sensors. A researcher sat in the back seat to monitor the results. The car was then driven around while the test subject operated a tablet device.
These tests were conducted with a diverse range of test subjects who differed in gender and ethnicity.

Another objective of the research was to create a CAV database, which included:

- Blind Spot Monitor (BSM), Signal Phase and Timing (SPAT), environmental
- Labeled images, pedestrian kinematic data
- Energy and trip datasets
- CAV deployment data [user behavior, edge cases]
- Near-real-time CV data dashboard [AA – Plymouth Rd. corridor]

This allowed the project to discover value in CV data, such as:

- Measurable safety benefits
- Trip information
- Human driving behavior
- Congestion management
- New business models

In addition, the database gave us early insights into AV development, deployment, and impacts. Current and planned datasets are shown in Figure 915.
The Navya shuttle dataset was initiated on June 4th, 2018, from two shuttles running Monday to Friday, 9AM to 3PM. Over 1000 trips carried hundreds of passengers and generated more than 200 hours of data. The initial dataset released in early August covered 200 trips and included exterior camera video. The full dataset includes a trip summary, GPS detail data, inertial measurements, Mobileye primary target information and counts, forward/rear video, and a data dictionary. Planned future datasets include:

- Mcity LIDAR data – Driving LIDAR data from Mcity, multiple passes, multiple routes
- Mcity Point Cloud – Fixed LIDAR scan point cloud
- Mighty AI – Thousands of labeled images
- AACVTE – Additional Safety Pilot dataset
- Track Data Capture - Recorded at Mcity during Track rental

4. **Consortium Structure**

The consortium consisted of a leadership circle and an affiliate program. The leadership circle is explained in Figure 1016, and the affiliate program in Figure 1117.

![Figure 10 - Mcity Leadership Circle](image)
5. Findings

The project encountered both structural and technical issues. These are summarized in Figure 12 and Figure 13, respectively.

- The OEMs believe this is an existential crisis
  – Not connected, autonomous, or electrified; shared
- Tilt towards private in the public/private partnership
  – Goals not necessarily aligned with DoD priorities (security/verifiability)
  – Significant pull on top talent into private roles
  – "Voice of reason" – code for "it doesn't have to be perfect"
- Technology progress outpaces policy framework creation
  – Complicated by state-by-state or even city-by-city approvals
- Profound implications for the nature of work
B. RISKS OF INTEGRATING UAS INTO THE NATIONAL AIRSPACE SYSTEM

Presenter: Brian Smith, NASA Ames Research Center, NASA Airspace Operations and Safety Program (AOSP)

1. Summary

In the short-term, the project sought to identify practical safety/security risks in deploying machine learning systems, e.g., data poisoning, training set inference, lack of model interpretability, and undesirable model bias. In the mid-term, the project assessed potential safety/security risks of future AI systems that are more powerful and more broadly deployed than those used today. Relevant problems in this space include scalably specifying and supervising reward-based learning, preventing unwanted side effects, generalizing out of domain, and ensuring that systems remain under control. In the long-term, the project will conduct theoretical work addressing the risks posed by artificially engineered (super) intelligences. Specifically, how we might ensure that a system is aligned with our values, and propose procedures for conserving this alignment while supporting recursive self-improvement?

The project found that AI solutions exist within set rules that are explicitly defined. Few AI security solutions "fail" their set rules. They can be made reliable. If anything, one needs to identify the holes/gaps/assumptions present in the explicit set of rules defined for a security task, including the specifications/behavior of the
environments that these AI systems are grown to work in and the completeness/correctness of the rules/cost functions that these AI systems are supposed to meet.

The project recommends using AI in the threat development landscape as a means to test out safety/security systems as well as utilizing AI to generate a wide range of risk scenarios that could breach security and safety protocols. AI might become one basis to provide the harshest of tests.

2. Background

As a result of the highest level of safety standards and risk management, aviation is the safest mode of transportation – a so-called “ultra-safe (and mostly secure) socio-technical system.” The validation process of initial implementations for machine intelligence in aviation had to be rigorous, so not all early attempts were successful. It had to be proven that AI:

1) Operates safely.
2) Is interoperable with the current system.
3) Supports the human-centric system.
4) Is applied through smooth and stable transition in a globally harmonized manner.

The key to achieving well-guided AI is to establish a human-machine coexisting environment, where the machine becomes a ‘sidekick’ that supports humans, instead of being a prospective ‘rival’. While early automation was providing support with simple and repetitive tasks, today AI is expected to deliver further capabilities by learning and mimicking human behaviors. AI is carrying out human tasks and in certain cases, even out-performing them. This can be achieved from the data, which fuels AI. The industry has already worked to build the cornerstone for AI, and with open data sharing, AI could change how we make decisions. The question remains, however: could AI learn and mimic nefarious human behaviors?

- The project identified three problems in the short-, mid-, and long-term timeframes.
- Short-term: Identifying practical safety/security risks in deploying machine learning systems, such as data poisoning, training set inference, lack of model interpretability, and undesirable model bias.
• Mid-term: Assessing potential safety/security risks of future AI systems that are more powerful and more broadly deployed than those used today. Relevant problems in this space include scalably specifying and supervising reward-based learning, preventing unwanted side effects, generalizing out of domain, and ensuring that systems remain under control.

• Long-term: Theoretical work addressing the risks posed by artificially engineered (super)intelligences, i.e., How we might ensure that a system is aligned with our values, and propose procedures for conserving this alignment while supporting recursive self-improvement in security?

Other challenges for AI and security include assembling large quantities of high-quality labeled data that characterize both normal operations and the threat environment. If false cues can be eliminated by careful, comprehensive labeling, then we will be able to use deep learning methods to detect emerging threats and trends. Unfortunately, labeling isn’t easy and requires domain expertise. Another challenge is achieving a breadth of detection capability. In the physical security realm, screening systems need to be able to detect and differentiate knives, bottles, batteries, cash and potential IED devices. What is the breadth of Cyber threats deep learning systems must reliably detect?

These and other challenges are shown in Figure 1420.
Additionally, AI/machine learning systems need to have anomaly-detection skills at least on a par with human operators. Automated anomaly detection is a tough nut to crack, and developers of AI systems shouldn’t be trusted to test and validate their systems. Only those with “skin in the game” – that is, the front-line operators – should test and validate. Machines are best at performing repetitive tasks, analyzing huge datasets, and handling routine cases. Humans, on the other hand, are good at resolving ambiguous information, exercising judgment, and dealing with end users.

There are four phases of AI classification/labeling.

1) **Training or “learning” phase** in which the analyst constructs a model by applying a classifier to a set of training data.
2) **Validation phase** in which the analyst applies the model to a validation dataset in order to assess its accuracy.
3) **Testing phase** to assess the model’s accuracy with test data that was withheld from the training and validation processes.
4) **Deployment phase**, in which the model is applied to predict the class membership of new, unlabeled data.

In practice, an analyst may train and test multiple models using different algorithms and hyperparameter settings. Then, they can compare the models and choose the one that offers the optimal combination of accuracy and detection rate for security anomaly detection.

Market trends in areas such as autonomous ground and aerial vehicles, strongly suggest that many future safety/security-critical systems will be comprised of heterogeneous, dynamic coalitions of systems of systems. For these types of systems, it is crucial to develop sound strategies that would allow security assurance and certification to be done compositionally. The new characteristics of safety-critical systems, such as connectivity, autonomy, and other cyber-physical properties, make assurance more challenging. It is not possible anymore to assure a system is dealing only with safety; other qualitative concerns must be addressed, e.g., security.

- What new ideas may be out there on compositional, evolutionary, and multi-concern assurance and certification of safety/security-critical systems?
- Is there room for reuse, composition, and combination of AI-based assurance arguments, assurance evidence, and contextual information about safety/security-critical products, in a way that makes assurance and certification more cost-effective, precise, and scalable?
The potential in applying machine learning algorithms that exist today to the data and logs that Security Information and Event Management (SIEM) engines collect is immense. AI could reason over the data at global scale in near real-time using the cloud and produce attack scenarios, which you could then tie to a security operations tool that automates the response and defenses based on the outcome of the AI reasoning – making sense of signal and intelligence. With a large volume of globally sourced data, you could use AI to look at anomalies in the behavior patterns of humans, devices, data, and applications at scale and make accurate predictions of the security threats to your enterprise—allowing you to deploy defenses well in advance of a specific attack. The attack surface is rapidly growing, the bad actors are becoming more sophisticated, and the need for tool evolution is compelling. AI is a path to that evolution or at a minimum keeping up with bad actors.

3. Findings and Recommendations

The project found that AI solutions exist within the set of rules that are explicitly defined. Few AI security solutions "fail" the set of rules, because they can be made reliable. If anything, one needs to identify the holes/gaps/assumptions present in the explicit set of rules defined for a security task, including the specifications/behavior of the operational environments that these AI systems are designed to work in.

Cybersecurity systems designers and front-line operators perform work in the four domains illustrated in Figure 1521. As the figure shows, the four domains do not coincide, even though most people expect that they are the same.

The project recommends that users leverage AI’s ability to allow more robust device-related IoT malfunction detection, sophisticated malware detection, and improvements in vulnerability management. The industry needs to work towards finding the sweet-spot between unsupervised and supervised machine learning so that we can fully benefit from our knowledge of current threat types and vectors and combine that with the ability to detect new attacks and uncover new vulnerabilities. Much like AI, machine learning in threat hunting must be guided by humans. Human researchers are able to look beyond the anomalies that the machine may pick up and put context around the security situation to decide if a suspected attack is truly taking place. Users should also consider using AI in the threat development landscape as a means to test out
safety/security systems, as well as utilize AI to generate a wide range of risk scenarios that could breach security and safety protocols. AI might become one basis to provide the harshest of penetration tests.

![Diagram](image)

Figure 15 - Four Domains

C. ENGINEERING LIGHTWEIGHT AUTONOMY

Presenter: Nicholas Weaver, UC Berkeley, International Computer Science Institute

1. Summary

The project defined three problems regarding developing autonomous drones to hunt other drones:

1) How light and cheap can one build a control system for autonomous drones?
2) Is there sufficient processing for on-board image processing?
3) Can one utilize the "Race drone" ecology?

The project found that control computers can be very light, around 20g and <$400 in low volume production, with two 1080p cameras (each under $30). These can be quite capable, with a dual core ARM, significant FPGA, ½ GB DRAM, two IMUs, GPS, WiFi/Bluetooth, and an SD card. Commercial racing drones are cheap, powerful, and amazingly capable. Light-weight autonomy is coming: it is time to be prepared to deal with the coming storm of small, light, cheap, and deadly autonomous threats.
2. **Background & Requirements**

Drones have a large potential for malicious use. This project, which was a side project in addition to the researcher’s other work, sought to build a drone to hunt other drones. The concept was to deploy a "weaponized-party/popper" or "streamer" a few cm above a hostile drone: This streamer would then entangle props and the target drone would crash. The requirements were as follows:

- **Low cost**: <$1000/each flyaway
- **Autonomous**: Can't work with a human in the loop
- **Self-contained**: Communications are unreliable

The project focused on building the computing hardware and software necessary to automate existing commercial drones. These needed the same (or greater) agility and mobility as potential target drones.

3. **Development**

The project chose commercial racing drones as the platform for development. Quad-copter racing drones can fly at speeds up to 150 kph (93 mph) and are agile enough to fly under trees and through abandoned buildings. These can easily carry a 200g (7 oz) payload with 5+ minutes of endurance. Fixed-wing drones have an endurance of about 45 minutes and have a level flight speed ranging from 75 to 150kph (47-93 mph). Both kinds of drones have plenty of on-board power for electronics and can be purchased for around $300 dollars. They are designed around modular hardware, software, and communications protocols. Examples of both types are shown in Figure 1622.

![Figure 16 - Commercial Racing Drones](image)

In order to make the drones autonomous, the project developed a custom control board, which is shown in Figure 1723 along with a list of components.
The envisioned drones would be equipped with two cameras. One camera would be used for flight navigation, and would be forward mounted with a narrow field of view. The FPGA would perform edge detection and optical flow for obstacle avoidance. The other camera would be used for hunting other drones, and would have a wide fish-eye lens with a top-angle mount. The software would request either a low-resolution view or full resolution around a point on a frame-by-frame basis in order to both mimic predator behavior and eliminate the need to write to main memory. The FPGA would undistort the fisheye and write directly into processor cache, and the software could then evaluate 15 targets/second in a "scan/focus/scan" loop. The host processor would run Linux, and anything real-time on a dedicated soft-core in the FPGA.

Currently, the hardware is done, but not debugged.

- Not yet booting to Linux:
  Debugging has been a low priority since this is a side project
- ~$13k for prototypes (x5)
- Quote for <$500/board for quantity 100
- Probably will do a spin with an extra 5mm on the bottom to add a bunch of general purpose I/O and upgrade the FPGA to a 7Z020
The Software/FPGA logic is envisioned but not implemented. The goal is to steal as much existing infrastructure as possible, e.g., PYNQ Linux stack for host software/interfacing.

4. Conclusions and Implications

Firstly, this is only a side project. If the research can accomplish this as a ~20% project with no other support but a little unrestricted fund pool, what could be done if a researcher was full time on this and had a few minions? Second, this level of computation is available at this very moment. Both a GPU or FPGA can be used for real-time image processing from very low cost cameras, and these can be coupled to general purpose CPU for higher level decision making.

Additionally, an anti-drone drone is inherently an offensive drone. The only difference is target selection and payload. Autonomy also changes potential defenses.

- Remote control: Jam the drone and it dies
- Used very successfully against ISIS drones and probably also in Venezuela
- Autonomy: Human control can be negative control
- Drone goes into "Kill All Humans" mode to complete its mission

Despite the relatively light payload of 200g (7 oz), this can be quite worrying to defense planners when integrated in an autonomous race drone. A 40mm grenade weighs about 200g (7 oz) and has a 5m (16’) kill radius. Even worse, stacked munition guns would weigh ~100g (3.5 oz). A carbon fiber barrel with internal rifled steel sleeve could have six stacked 9mm hollow-point rounds built into the barrel, like a miniaturized MetalStorm gun. Two barrels can be mounted side-by-side, and computer control means 6-12 potential headshots. A potential autonomous drone system is explained in Figure 1824. Of particular concern is “Spirit of Butts Farm” strategies, which showed that it is possible to build a small autonomous aircraft that can cross the Atlantic.
Within the next couple years, there will be a tipping point on autonomous drones. Defenses are needed across a broad spectrum, containing aerial attackers as well as “ankle-biters” (small autonomous ground vehicles with a jump ability). $100k or $100M systems cannot be efficiently be used to stop $1000 threats.

D. UAV WITH MUNITION

Presenter: Valdis Berzins, Naval Postgraduate School, Computer Science Department & Andy Hernandez, Naval Postgraduate School, Systems Engineering Department

1. Summary

The project sought to find out how risk-based testing can be applied to autonomous vehicles that operate in contested Cyber environments. The project determined that the number of test cases needed to achieve confidence that the failure rate is less than the tolerance can be derived from maximum acceptable risk level. Risks must be reformulated in game theoretic terms for contested Cyber environments. The project recommends that testing be augmented with appropriate static analysis and the largest effort be allocated to mitigate hazards with the most severe consequences. Adversary capability to modify UAV control code carries maximal risk – severity of consequences is practically unbounded during active conflicts.
2. Introduction

Cyber Physical Systems are engineered systems comprised of interacting physical and computational components. Drone technologies are primary examples of this kind of system. There has been a recent explosive growth in unmanned aircraft, as they are not limited by human performance or physiological characteristics, they offer extreme persistence and maneuverability, and they present alternatives as stand-alone or embedded options for military forces. The success of an unmanned aircraft system depends on how it can overcome possible technical and software faults and failures and meet the desired design-requirements. Developers focus on the safety and reliability aspects of the system and software development processes used for drones, but they must mitigate risk where DoD considers that Risk = F(Severity, Probability).

For systems with high reliability, it is unaffordable and/or impractical to collect enough observations during tests to compute accurate estimates of failure probability. This project sought to develop a risk assessment methodology for drone software using a real time monitoring architecture. Specifically,

- What will be a proper/appropriate methodology for the assessment of software risk in a weapons system drone?
- What will be a proper methodology to mitigate the risk of software failure in a drone’s system?

Our solution was to develop a method for bounding software failure probabilities to high levels of statistical confidence via automated testing.

In an operational context, drones perform intelligence, surveillance, and reconnaissance missions while a ground control station and operators direct UAV activities through different wireless links. Regression testing should be considered in cases where

1) Neither specifications nor code of a software module has changes from a previous release, but the hardware has changed.

2) The specifications have not changed, but the implementation of the code has changed.

3. Brief Discussion of Reliability Analysis

There are two approaches to assessing reliability; a bottom up approach called Failure Mode and Effects Analysis (FMEA) and a top down approach called Fault Tree Analysis (FTA). These are shown in Figure 1925.
FMEA predicts failures and their effects, predicts potential cause(s) of failure modes, and judges sufficiency of measures already taken. FMEA provides a means to assess the adequacy of measures to prevent harmful failure modes and to check reliability of the design (and operations). A failure is defined as either:

- Non-function: no performance
- Malfunction: wrong performance or performance of insufficient quality
- expected, but erratic or too slow
- unexpected

Reliability is defined as the performance and quality of a product or a process that can maintain the intended functions under specific conditions and within a prescribed period.

The criteria for scoring failures using FMEA are shown in Figure 20.
<table>
<thead>
<tr>
<th>Potential Failure Mode</th>
<th>Detection (Likelihood)</th>
<th>Severity (Impact)</th>
<th>Occurrence (Severity of the occurrence)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Minimal</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>2</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>3</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>4</td>
<td>Very High</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>5</td>
<td>Very Low</td>
<td>Low</td>
<td>Very High</td>
</tr>
<tr>
<td>6</td>
<td>Low</td>
<td>High</td>
<td>Very Low</td>
</tr>
<tr>
<td>7</td>
<td>Very High</td>
<td>Medium</td>
<td>Very Low</td>
</tr>
<tr>
<td>8</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>9</td>
<td>Very Low</td>
<td>Low</td>
<td>Very High</td>
</tr>
<tr>
<td>10</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
</tr>
</tbody>
</table>

**Figure 20 - Scoring in FMEA**
An example of Failure Model Effects and Analysis is shown in Figure 2127.

Figure 21 - FMEA Example

FTA enumerates different ways in which a failure can occur and its probability of occurrence. It starts with identifying a specific, top-level event (e.g., “system catches fire”), and then constructing a top-down causal hierarchy for each top-level event. Then, going from the bottom up, the probability of all input events is determined and rolled up to obtain an overall reliability of each top-level event. If the calculated top-level reliability is unacceptable, corrective action is required. An example of Fault Tree Analysis is shown Figure 2228.
4. **Bounding Method (Drone Case Study)**

A case study was conducted to apply the proposed method to a commercial quad-rotor Parrot AR.Drone 2.0. This drone is controlled via WiFi using Apple, Android device, or PC, and has advanced features including image recognition. The drone is shown in two configurations in Figure 23.

Hazards to the drone that were analyzed in the case study were:

1) Loss of communication
2) Loss of propulsion
3) Environmental Damage
4) Loss of battery power
5) Loss of situational awareness

The severity and probability matrices for the risk analysis are shown in Figure 2430.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Could result in irretrievable loss of aircraft, human life, damages exceeding $1,000, or irreversible severe environmental damage that violates law or regulation.</td>
</tr>
<tr>
<td>Critical</td>
<td>Permanent damage to retrievable aircraft requiring complete replacement, permanent partial disability, loss exceeding $1,000 or reversible environmental damage causing a violation of law or regulation or indirectly causes mission failure.</td>
</tr>
<tr>
<td>Marginal</td>
<td>Major repairable damage to aircraft requiring replacement of expensive parts with total repair cost exceeding $150, non-permanent injury or mitigable environmental damage causing a violation of law or regulation.</td>
</tr>
<tr>
<td>Negligible</td>
<td>Minor repairable damage to aircraft requiring replacement of cheap parts with total repair not exceeding $150, or minimal environmental damage not violating law or regulation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Probability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>Expected to occur multiple times in the operation of the aircraft.</td>
</tr>
<tr>
<td>Probable</td>
<td>Will be expected to occur at least once in the operation of the aircraft.</td>
</tr>
<tr>
<td>Occasional</td>
<td>Will be expected to occur at least once after several operations of the aircraft.</td>
</tr>
<tr>
<td>Remote</td>
<td>Unlikely, but can be expected to occur at least once in the life of the aircraft.</td>
</tr>
<tr>
<td>Improbable</td>
<td>Highly unlikely to occur, but still possible to occur at least once in the life of the aircraft.</td>
</tr>
</tbody>
</table>

Figure 24 - Severity and Probability Matrices

A matrix of the mishap categories is shown in Figure 2531.

<table>
<thead>
<tr>
<th></th>
<th>Catastrophic</th>
<th>Critical</th>
<th>Marginal</th>
<th>Negligible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>High</td>
<td>High</td>
<td>Serious</td>
<td>Medium</td>
</tr>
<tr>
<td>Probable</td>
<td>High</td>
<td>High</td>
<td>Serious</td>
<td>Low</td>
</tr>
<tr>
<td>Occasional</td>
<td>High</td>
<td>Serious</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Remote</td>
<td>Serious</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Improbable</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Designed out</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>
Combining these failure modes with estimates of their probability of occurrence per the FTA in Figure 26, the overall risk for the loss of communication is assessed as high. The system risk is displayed in Figure 27.

**Figure 26 - Fault Tree for Communication Loss**

<table>
<thead>
<tr>
<th>Hazard</th>
<th>System Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of Communication</td>
<td>High</td>
</tr>
<tr>
<td>Loss of Situational Awareness</td>
<td>High</td>
</tr>
<tr>
<td>Loss of Propulsion</td>
<td>Serious</td>
</tr>
<tr>
<td>Loss of Battery Power</td>
<td>Medium</td>
</tr>
<tr>
<td>Environmental Damage</td>
<td>Medium</td>
</tr>
</tbody>
</table>

**Figure 27 – Results of FTA for the Parrot Drone**

The proposed method for determining the number of test cases needed \( N \) is outlined as follows. First the tolerance level for residual risk exposure must be determined. Then a risk budget must be allocated and the severity of consequences is determined for each hazard. The maximum acceptable probability of occurrence is then found by using the risk matrix backwards, looking up the worst acceptable probability of occurrence.
occurrence within the given severity and risk budget. Then the number test cases needed are determined where:

- Worst acceptable probability of occurrence is $1/N$,
- Want confidence $1 - 1/N$ that failure rate $< 1/N$,
- Need $N \ln N$ test cases with no failures observed, where $\ln$ denotes natural logarithm.

If the test passes, the risk due to software failure will meet the risk budget with the specified confidence level.

In an operational context, Cyber risks are different because there is an intelligent adversary. In this situation the probability of occurring is not constant and depends on the state – e.g., are we at war? The probability of attack can change drastically without warning, as happened just before the Japanese attack on Pearl Harbor. The very concept of risk needs rethinking for contested environments. While traditional statistical methods are sensible for random failures (minimizing expected loss), game theoretic ideas may better match the (cyber-) conflict context by minimizing worst-case loss [28]. While mitigating the worst possible case might be wasteful, planning using probabilities typical of peacetime is short-sighted. It may appear seductive due to minimizing short-term costs, but it may not mitigate exposure to catastrophic events that are improbable in peacetime but frequent under conflict conditions. Some surrogates for probability of occurrence that may be applicable in contested environments include degree of legal liability, cost, and technical difficulty of exploiting a vulnerability.

5. Conclusions

This study performs a hierarchical top-down decomposition of drone control systems into their software components, analyzing them in terms of features and functions, explaining how they interact with each other, and develops a high level analysis-prototyping design for the assessment of software risk in several types of drones including a weapon system drone. Our method gets around the difficulty of testing systems with high reliability (hence low failure rate) by focusing on obtaining a statistical upper bound on the failure rate, without seeking to determine its exact value. Such a bound can be obtained from a sufficiently large number of test observations that are completely failure-free. For Cyber, testing must be augmented with static analysis, e.g.,
monitoring the statement coverage of the test cases, plus reachability analysis for reachable untested code, plus human inspection of untested code if coverage is less than 100%.

E. TRACKING PROVENANCE OF AUTONOMOUS DECISIONS

Presenter: Doug Lange, Space and Naval Warfare Systems Command, Naval Information Warfare Center Pacific

1. Summary

The addition of autonomy into systems necessitates the use of methods that inform human decision makers concerning automated decisions. Provenance analysis can be used to provide human-comprehensible explanations of decisions made by autonomous components. We have reason to believe that we can utilize provenance data to provide summaries of activity and learn to recognize the quality of decision processes. Systems should be instrumented to track provenance, and we must then make use of the data to learn to model the quality of decisions.

2. Introduction

In the context of autonomous systems, provenance is information about entities, activities, agents, and the relationships between these concepts. It introduces methods of tracing decisions made to decision makers and the information available to them at the time. Analysis of these relationships can bring transparency of the decision-making process to humans, particularly to those responsible for the quality of the outcomes. This information is important in military operations and Command and Control (C2), especially when autonomous artificial agents influence the decision-making process. The Provenance Data Model (PROV-DM) is a generic data model that allows for domain and application-specific representations of provenance data to be translated and interchanged between systems [29]. The notation used by PFROV-DM is illustrated in Figure 2834.
3. Background and Motivation

As noted in the Association for Computing Machinery US Public Policy Council (USACM) statement on algorithmic transparency and accountability [30], “Computer algorithms are widely employed throughout our economy and society to make decisions that have far-reaching impacts, including their applications for education, access to credit, healthcare, and employment.” This makes ethical concerns around algorithms and Human-Autonomy Teaming (HAT) a very important issue, especially since even a well-designed computer system can have unexpected outcomes, biases, or errors. Provenance analytics is commonly used in algorithmically intensive systems such as crowdsourcing apps, but is also used in anomaly detection, accountability and trust. Some ethical aspects of HAT can be directly addressed by data provenance.

4. Intelligent Multi-UxV Planner with Adaptive Collaborative/Control Technologies (IMPACT)

In the near term, critical systems will not be completely autonomous, but rather will consist of humans interacting with autonomous subsystems. An example of this kind of Human-Autonomy teaming is the Intelligent Multi-UxV Planner with Adaptive
Collaborative/Control Technologies Project. An envisioned interface for the IMPACT system is shown in Figure 29.

The Human Autonomy Interface allows for play calling, tailoring, monitoring, and enhanced operator-autonomy dialog. A play is a tactic or course of action for accomplishing a desired objective. A Resource Allocation Agent recommends assets for a desired play, monitors progress across plays, and identifies targets of opportunity. Collaborative Control Algorithms (CCA) dynamically interact with Agents to produce effective mission routing while the Task Manager assists by dynamically balancing the system workload. Essentially, this allows a human operator to control an autonomous system like a coach controls an American football team, calling different plays depending on the assets available and the current situation. Figure 30 shows a diagram of an IMPACT system incorporating elements from five allied nations during the MAPLE FLAG exercise.
The human playcalling can be understood by following the activities (blue rectangles) going from top to bottom in Figure 3137. A task is generated from a message received, and constraints are made alongside the task itself. The operator selects a play from the playbook, or from another source such as the Task Manager. Constraints are derived from the type of play the operator selects, constraints can be amended by humans or automated agents, and planning begins. Planning produces different options (policies are also checked, but not shown in the diagram), and the one selected by the operator will be finalized by the planner and instantiated.
Figure 31 - Detailed IMPACT Diagram
Due to the complex web of relations and dependencies within this system, a small change in elements “higher up the chain” can lead to wildly divergent outcomes and effects. This is shown in Figure 3238, where a dependency is changed partway through the planning process. In Box A, the process starts out the same as a human playcall when a chat message causes a new task and task constraints to be created. The rest of the provenance records events up to the point where a final plan is instantiated. Box B shows that instantiated final plan, and a new chat message changing the dependency. This takes the final plan and puts it through a new planning process. The new task caused by the chat message is taken through the entire planning process again and finally re-instantiated when the human operator decides to act upon new intel.

![Figure 32 - Dependency Change](image)

Although provenance analysis allows operators to trace the chain of causality of an event back to its source or nucleus, it can still be difficult to turn the raw data generated by provenance analysis into a coherent explanation of the actions of an autonomous system. This is where Rhetorical Structure Theory (RST), originally
developed to study computer based text generation, can be applied. The most important part of a text, called the “nucleus”, is identified along with its relationships to other elements of the text. By replacing the nucleus of a text with the “source” of an autonomous action, RST can easily be applied to explain why an autonomous system took the action it did. An example RST diagram is shown in Figure 33.

![Figure 33 - Example RST Diagram](image)

An additional layer of complexity is required to account for anomalies, i.e., an asset straying out of communications range. Figure 34 shows a provenance diagram dealing with this event. When a plan has been set into motion, the "policy_monitor" agent detects when an asset will potentially violate a policy (asset must be within comm range) and the planner begins planning to correct the impending violation. After validating that the new plan option is ok, the new plan is selected by an autonomous agent (usually Plan Monitor) shown here as "operator." This plan will be finalized by the planner once again and is re-instantiated.
Figure 34 – Anomaly (Policy Violation)

5. **Conclusions and Further Work**

Provenance-enabling and analytics could serve as useful tools in Command and Control and Human-Autonomy Teaming, especially with regard to UxVs. Provenance services and capabilities have been implemented in Allied IMPACT, and the combination of provenance analysis and Rhetorical Structure Theory can be used to generate compelling and coherent explanations for the actions of complex autonomous systems.

Future work may include learning to characterize and classify the quality of a planning evolution, assigning responsibility for particular decisions to particular agents or teams to illuminate risk to decision makers, and summarizing complex composite decisions at appropriate levels of abstraction for information decision makers. We also
suggest expanding UML2PROV and attempting to automatically generate PROV-Templates with other modeling languages, as well as expanding the instrumentation of autonomic frameworks and other autonomous decision frameworks.

F. AUTONOMOUS AERIAL SWARM ROBOTICS CYBER CHALLENGES

Presenter: Duane Davis, Naval Postgraduate School, Advanced Robotic Systems Engineering Laboratory (ARSENL)

1. Summary

Problem Description: Simultaneous operation of large teams of small (non-program of record) unmanned aerial vehicles (UAV) presents Cyber challenges that have not been adequately addressed or characterized.

Observations:
Cybersecurity issues can be grouped by the part of the system that they affect:

6) Communications & networking
7) Ground control stations
8) Mission-level autonomy
9) Autopilot & flight control

Most issues are not unique to UAV systems.

Recommendations:
1) “Best practices” address many UAS system Cyber issues
2) Consider UAS Cyber requirements holistically rather than in isolation
3) Base UAS Cyber requirements on risk rather than arbitrary rules

2. Introduction

This section describes a research project called ARSENL. The vision behind ARSENL is to provide a diverse academic and research venue to foster a holistic, multidisciplinary approach to the design, employment, and future concept development of robotic and unmanned systems. The emphasis of this project has been to explore the use of swarms of UAVs to perform coordinated missions.

All of the platforms used in this research were small and relatively inexpensive. These types of platforms were chosen to enable the project to acquire sufficient numbers of them in order to conduct meaningful experiments with swarms and the coordination of multiple swarms. Some of the UAV platforms used are shown in Figure 1.
The project has leveraged open-source and open architecture hardware, designs, and commercial components to speed up development, as shown in Figure 2.

The experiments typically involve multiple swarms, sometimes adversarial. Typical system architecture is shown in Figure 3.
3. Cyber Issues Studied

The first Cyber issue studied was communications and networking. Communications involving UAV swarms typically have the following characteristics:

- Broadcast or mesh (MANET) protocols
- Lossy and disconnected networks (reliability vs latency tradeoffs)
- Usually low power & line-of-sight
- COTS systems frequently use proprietary protocols
- Custom-developed systems are implemented on top of standard protocols

Communications reliability is often spotty, as show in Figure 38Figure 4. The figure illustrates the quality of the signal form the transmitting sortie to the receiving sortie using a graphical representation where green means the signal is good and red means it is poor or missing.
The project’s analysis showed that the swarm communications are:

- Susceptible to denial (jamming, flooding, etc.)
- Cybersecurity issues of well-known protocols are addressable
- Privacy is an encryption issue
- Integrity can be achieved with MACs or signatures
- Cybersecurity issues of proprietary protocols can be problematic
- Does it have the required capabilities?
- What level of trust does it merit?
- Do we have the specifications?
- Is it configurable?
- Etc.

To resolve these issues, we recommend that swarms:
• Require isolation
• May or may not be reasonable (or even possible)
• Utilize “best practices” with standard protocols
• Develop assessment criteria for proprietary protocols
• Will provide a basis for informed decisions
• Decrease vulnerability to denial attacks with failsafes
• EMMW? Maybe, for programs of record
• Hard for custom systems
• Probably impossible for COTS

The second Cyber issue studied was associated with the Ground Control Stations (GCSs). The GCSs of commercial UAVs typically have the following characteristics:

• COTS systems often have proprietary GCSs
• Include both hardware and software
• Limited end-user configurability
• Custom systems can rely on open-source or in-house development
• Typically run on Windows, MacOS, or Linux systems
• Both types of systems rely on the underlying communications infrastructure and may or may not require at least sporadic Internet connectivity

An example GCS interface is shown in Figure 5.

Figure 39 - Example GCS Interface
The project’s analysis showed typical GCSs have the following characteristics and issues:

- COTS system GCSs
- Depend on vendor trust (intent & competence)
- Cyber assessment may or may not be adequate
- Hardware and software both require evaluation
- Open source systems
- Low likelihood of malicious intent
- Cyber vulnerabilities may be present
- Community alignment with DoD objectives & priorities
- Trustworthiness of maintenance processes
- Custom systems
- Correctness was more relevant than security
- Insider threat? (intent & competence)
- OS security requirements may not be standardized

To address these issues, we recommend that GCSs:

- Utilize “best practices” on host systems
- Systems should be assessed in the same manner as other (non-UAS) systems
- Host versus application vulnerabilities
- Formalize the assessment process
- What are the requirements?
- What are the assessment criteria?
- Open source versus in-house development versus a little of both
- Risk- versus rules-based

The third Cyber issue studied was how to achieve mission-level autonomy, which is not usually available in COTS systems without customization. It is usually implemented on a Windows, Linux, or MacOS system (on-board companion computer or ground-based system), and is often open-source or COTS dependent. Examples of software infrastructures used in this context include Robot Operating System (ROS), Mission Oriented Operating Suite (MOOS), MATLAB Robotics Toolkit, and Microsoft Robotics Developer Studio. A typical on-UAV system architecture is shown in Figure 6.
The project’s analysis identified the following issues related to the security of mission-level autonomy:

- Security of implementation platforms
- Hardware and software are not UAS-specific
- Custom and in-house development
- Correctness versus security
- Open source infrastructure
- Low likelihood of malicious intent
- Cyber vulnerabilities may be present
- Trustworthiness of maintenance processes
- COTS infrastructure
- Vetting and validation

In order to best implement mission-level autonomy, the project recommends that developments:

- Utilize “best practices” on companion computer & ground-based autonomy host systems
- Formally assess open-source and COTS robotics software
- Encourage security-focused versions such as SROS
• Develop risk-based utilization requirements criteria
• Provide risk-based security requirements guidance for autonomy software development

The fourth Cyber issue studied was associated with the autopilot and flight control. These functions typically have the following characteristics:
• COTS (i.e., the source of many current UAS Cyber concerns)
• Vendor controlled and aligned with associated GCSs
• Proprietary and protected
• Possible ongoing communication with the vendor
• Update processes and requirements
• Open architecture
• Open source firmware for COTS hardware
• ArduPilot & PX4 most common
• Can be used as-is or customized

A diagram of a typical flight control architecture is shown in Figure 41Figure 7.
Figure 41 - Typical Flight Control Architecture
The project’s analysis identified the following issues related to the security of the autopilot and flight control:

- COTS
- Operational data relay to vendor possible
- Vendor-initiated update possible
- Hidden vulnerabilities?
- Open architecture
- Reliability concerns (will vehicles perform predictably?)
- Open-source communities’ alignment with DoD objectives is not a given
- Hobby vs racer vs autonomy requirements
- Isolated design decisions
- Unexpected codebase changes possible

In order to leverage existing architectures and components for autopilot and flight control while still maintaining security, the project recommends that:

- COTS
- Require network isolation (if risk merits)
- Require firmware transparency (e.g., source code)
- Develop risk-based criteria for utilization
- Open architecture
- Develop formal assessment processes
- Provide a risk-based requirements framework

4. Conclusions & Recommendations

In conclusion, UAS Cyber issues are not necessarily UAS-specific. They are often addressed more generally, and can be characterized according to the portion of the system that they affect. COTS, open-source, and in-house-developed systems have unique characteristics which must be accounted for prior to deployment. We recommend:

- Enforcement of recognized “best practices”
- A risk- versus rule-based approach
- Formal requirement vs risk framework
- Formalized open-source and COTS product evaluation
- Requirements for evaluation of in-house-developed software and firmware
III. CHALLENGES OF NAVAL OPERATIONS TO CYBERSECURITY

Maintaining Cybersecurity in a naval operational environment poses its own unique challenges. Christian Fitzpatrick gave a presentation on the Marine Corps’ efforts to implement signals intelligence and Cyber simulations in their training environments. Anthony Akil analyzed the 2017 Vulnerabilities and Equities Policy as it related to zero-day exploits in military technology. This session was chaired by Anthony Akil.

A. LVC SIMULATION SUPPORT FOR THE MARINE CORPS’ CEMOES

Presenter: Christian Fitzpatrick, Naval Postgraduate School, Modeling Virtual Environments and Simulation (MOVES) Institute

1. Introduction

As the global network continues to expand, our adversaries are taking advantage of the worldwide connectivity to achieve both strategic and tactical effects. In 2007, Russia first engaged in cyber warfare when they clashed with Estonia over the relocation of a Soviet World War II Memorial from the capital of Tallinn. During this political dispute, Estonian networks were targeted in a distributed denial of service (DDoS) attack [31]. As a result, Foreign and Justice Ministry websites were shut down along with online banking sites. Although the Russian government never claimed responsibility, electronic fingerprints indicated the attacks originated from a mix of their government and non-government computers [31].

China also has an active presence on global networks as reported in 2013. The former Mandiant uncovered a secretive People’s Liberation Army (PLA) cyber unit working from an office in the outskirts of Shanghai [32]. Based on months of network analysis, its analysis team collected technical evidence of multiple Cyber-attacks on American corporations, organizations and government agencies [32]. With unlimited funding to employ talented scientists, China’s military is developing a robust Cyber program targeting a broad cross-section of American interests.

Aside from our near-peer competitors, terrorist organizations are achieving a certain level of success operating on global networks using wireless devices. The Islamic State of Iraq and Syria (ISIS) uses the internet to spread its message and actively recruit
educated fighters to join its cause. One well-known insurgent is Mohammed Emwazi, nicknamed “Jihadi John” by the European media. Emwazi was responsible for several brutal ISIS beheadings; but prior to his war crimes, he achieved a computer science degree in 2009 from the University of Westminster [33].

Finally, in 2016, the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) claimed with “high confidence” that Russia had intervened in the U.S. Presidential elections [34]. Their goal was to degrade our democratic process and assist in damaging Candidate Clinton’s election bid [34]. To achieve its goals, Russia supposedly embarked on a sophisticated campaign to influence the American people. Although unproven, many feel that Russian President Putin used cyberspace to achieve these goals. The investigation is still ongoing.

In this new domain, programmers are the combatants. Like other domains (air, land, and sea) with robust training programs, the training sand box for cyberspace operations is not well developed. Modeling and simulation (M&S) is emerging as a critical capability to develop and sustain our Cyber forces and toolsets. The MOVES Institute at NPS is moving out in two areas to support the DoD’s goals in cyberspace training and analysis. First, it is modeling cyberspace behaviors and their effects on the battlefield within existing combat simulations. This activity serves to develop emerging tactics, techniques, and procedures (TTPs) and to perform testing, training, and evaluation (TT&E) on new cyber systems and tools. Second, MOVES is contributing to the creation of cyberspace emulation environments for tactical survey and assessment. The work described below describes MOVES’ support of the Marine Corps Systems Command as they work to transition of the Constructive Electromagnetic Spectrum Operations Emulation System (CEMOES) to the Fleet to support tactical cyberspace training events at each of the Marine Expeditionary Forces (MEFs).

2. Summary

Live training for signals intelligence (SIGINT) and Cyber operators lacks multidomain realism, as their simulation-based training is not networked or distributed. Current training environments emulate signals from a single location on a physical range, making it easy for operators to locate the transmitter and collect data. This does not
emulate the challenging tactical environment our Marines and Sailors face when deployed overseas. They will face an enemy that has various digital signatures and is constantly on the move. To mitigate this training gap, the Marine Corps developed a concept for a distributed simulation system based on the capabilities of software defined radios (SDRs) called the Constructive Electromagnetic Spectrum Operations Emulation System, or CEMOES. By transmitting various signals including commercial cellular, WiFi, and VHF from a select SDR emplaced among other SDRs distributed on a local physical range, CEMOES can help Marines and Sailors learn how to survey “noisy” signal environments to support their tactical mission.

Considering the dramatic size, weight, and power (SWaP), and cost reduction of SDRs that is taking place, current $100,000 and 30 lb. systems are being replaced with $2,000 and 1 lb. systems. Only specially trained warfighters are carrying these radios. However, these niche systems may soon become standard issue to all operators. The CEMOES seeks to prepare the DoD for the eventual coming of standard issue SDRs by creating a training methodology using the computational and transmitting power of SDRs to create noisy, distributed SIGINT/Cyber emulation environments that mirrors the challenging tactical Electronic Warfare (EW) environment they operate in while deployed (see Figure 42-41).

Figure 42 - Initial CEMOES Concept developed in 2014
Following initial testing and demonstration while this technology was a research program at the Office of Naval Research (ONR) Code 30, it was selected as a program of record (PoR) following the submission of a Deliberate Universal Needs Statement (DUNS) endorsed by the Commanding General, II Marine Expeditionary Force (II MEF) in the winter of 2015. Now as a PoR, CEMOES is planned for delivery to each of the three MEFs in FY19, 20, and 21.

3. **Background**

In the 1960s, companies used a single, large-scale computer for their data processing needs. Configured as a circuit-switched network, “dumb” terminals and line printers were connected to a central host via a single connection using proprietary communications protocols [35]. This infrastructure was brittle and could not scale to meet increased demand. Consequently, businesses never considered buying hardware from another vendor to augment their existing system. Instead, they just replaced their hardware entirely. Cross-platform connectivity was unheard of at that time [36].

Seeking a more reasonable approach, the Department of Defense (DoD) began experimenting with a data packet switched network in 1968 [36]. The new project was called the Advanced Research Projects Agency Network (ARPANet) and it would later go on to become the Internet. Today, it serves as a fault-tolerant, vendor-independent network that can tie any and all people together. With its worldwide adoption for business and personal use, cyberspace is now a relevant domain for tactical operations.

Meanwhile in Silicon Valley, microprocessor chips were advancing rapidly as well. In 1971 Intel co-founder, Gordon Moore, made a bold prediction that future processors would double in efficiency every 2 years [37]. His vision has become a reality and is evident as users shift their primary platform from personal computers (PCs) to wireless, mobile devices. Currently, over 3 billion people carry smartphones in their pockets [37]. Each is more powerful than room-sized supercomputers of old.

Given the functionality of these smartphones, users no longer need multiple devices. This has triggered a synthesis of individuals’ personal lives blurring with their professional lives and other affairs. Today, the spectrum is as noisy and congested as it has ever been. Various state and non-state actors are taking advantage of this. For example, the Islamic State of Iraq and Syria (ISIS) is using wireless devices to access the
internet, actively recruit and educate fighters, manage their expenses, and promote their ideology. Considering their recent successes, our military units must be able to operate in this global network and adapt quickly to technical advancements to support signals intelligence (SIGINT) tasks during tactical missions.

4. **Proposed Solution**

The Department of Defense (DoD) has signaled that they need focused cyberspace training capability at the tactical edge as most current training systems are at the enterprise level. Tactical operators working in the Radio Frequency (RF)-to-Cyber environment lack a facility to train and certify their cyber operators. In addition, they don’t have a specific range to enable them to hone their cyber TTPs. The National Cyber Range (NCR) and the DoD Information Assurance (IA) Range were established to meet this need, but again training at those facilities is at the enterprise level. An organic, unit-deployable capability like CEMOES enables our Soldiers, Sailors, and Marines to conduct realistic cyberspace training at the tactical edge. In addition, using CEMOES to stimulate handheld SDRs across an operating unit could facilitate information operations (IO) and military deception (MILDEC) by transmitting into the RF physical environment creating more “noise.”

Upon delivery to the Fleet, CEMOES will be a rapidly deployable support structure to allow for the development, testing, use, and employment of Computer Network Exploitation (CNE) and Offensive Cyberspace Operations (OCO) tools. It will also connect all local Military Operations on Urban Terrain (MOUT) ranges to the Joint Training and Education Network (JTEN) for continuous (weekly) full-spectrum training with integration with other services, Cyber Mission Teams, Red Teams, and Strategic Agencies. Constructive simulations should be integrated to drive tactical scenarios in relevant environments. Sustainment training should be created as well (Cyber 30/60/90, Cyber T&R). For the system to succeed though, CEMOES must include a sharable library of full-spectrum scenarios that models interesting communications embedded in background noise (see Figure 4342).
CEMOES has been under test since 2014. Massachusetts Institute of Technology Lincoln Laboratory (MIT-LL) has been coordinating tests with operators to validate the technology. The first test in the Fall of 2014 took place on an urban range located at Camp LeJeune, North Carolina (see Figure 4443). The range was a perfect fit for demonstrating the capabilities of CEMOES as it had an existing wired infrastructure to support an internet protocol (IP) based network. That network was emplaced to run a moving target system for live-fire training. Using the network, MIT-LL was able to run its packet generation system named Lincoln’s Adaptive Real-Time Information Assurance Testbed (LARIAT). LARIAT can emulate over 100,000 virtual IP addresses and the passing of data packets across the virtual network to model various activities on the internet to include the use of software applications, sending emails and posting on blogs (see Figure 4544). Many of these activities are also conducted on small handheld devices, which is the critical addition CEMOES makes to the functionality of LARIAT.
To guide the development of the virtual and constructive simulation, we will first author a complex script in which multiple actors and units interact to achieve specific goals in and through cyberspace. At a minimum, the script will include all dialogue between actors, any digital content created, media & webpages accessed, and all entity digital signatures. This data will provide a structured representation of the entities and behaviors modeled in the virtual world.
Once all actors and their roles are defined, we will instantiate them as entities in the simulation. Each will have unique variables and parameters to define their view of the world state making them a unique persona. As the simulation advances, their variables will follow a piecewise constant trajectory to define their location, movement status, or available hardware. Their parameters, on the other hand, will remain static throughout and include classification (adversary, friendly, or neutral), scenario role, or technical proficiency. Select entities will be geo-referenced within the exact physical dimensions of a DoD urban training range while others will operate remotely on the global network. The remote entities will still affect the overall state space through various forms of web interaction.

Since there is no “human-in-the-loop,” all entity behaviors must be defined prior to the start of the simulation run. For this purpose, we will use Discrete Event Simulation (DES) event graphs. The world state will differ each time the DES event graph runs, thus creating dynamic outcomes upon execution. Our event graphs will begin with a high-level description of the activity they model. Through action decomposition, the tasks required to reach a goal state will be broken down into sub-tasks. Multiple orderings of those sub-tasks can lead to the goal task and conditional statements determine the exact
sequence of execution. Completion of the goal task indicates the entity has achieved a desired world state.

Figure 46 illustrates an example event graph in the context of a tactical RF-to-cyber scenario where an entity is tasked to conduct an information operations (IO) activity to achieve a tactical effect. The event graph nodes show a methodical process to obtain network access, create content for the IO mission, post the content, await responses until a desired threshold is reached, and the assess the effect. The nodes correspond to an event, or state transition, and each edge corresponds to the scheduling of the next event [38]. Event graphs will be constructed for every behavior detailed within the script and those behaviors will be triggered by various event listeners assigned to each entity. We will be utilizing the DES libraries contained in Java SimKit containing code that will schedule events to occur based on world state and scheduling relationships.

The live simulation will require utilization of the Field Programmable Gate Array (FPGA), Application Specific Integrated Circuit (ASIC) RF Transceiver, and RF Filter Banks embedded within a SDR (Figure 4746). For scenario RF communications, the baseband data specific to the transmission will be stored on the SDR.

The FPGA will digitally up-convert and then modulate the signal based on the device selected to transmit the message in the event graph. The RF Transceiver will then convert the digital signal to an analog signal for transmission over-the-air, allowing for a
wide range of wireless signals to be emulated, without the burden of costly “one off” hardware. In Figure 46, the “Post Content” and “Respond” nodes will follow this process to emulate RF transmissions specific to the scenario.

The receive and digital processing capabilities of an SDR will also be used as some agents may be assigned a communication received “listener” to trigger a specific behavior. If this is the case, the signal must be received, converted to a digital signal by the ASIC, and then digitally down converted by the FPGA. Digital Signal Processing (DSP) algorithms will then be used to determine the content of the message. The REDHAWK SDR framework will enable that data to be shared between the various software radios on the network triggering the event graph aligned to the message heard by the virtual agent’s “listener” [39]. Learning this middleware framework will enable our warfighters to use SDRs for various IO and MILDEC operations as required by the mission. By creating their own RF environment for training, they will become more proficient in using the SDRs to better impact the RF-to-Cyber environment.

![Figure 47 - Internal components of a tactical SDR used for live, constructive simulation](image)

5. **CEMOES**

CEMOES is a methodology to create this signal environment by deploying a **live, virtual, constructive (LVC)** training simulation over a distributed RF network emplaced in a representative tactical setting (see Figure 48). Since it is financially and logistically unfeasible to have thousands, or even hundreds, of role-players on-hand to recreate the RF-to-cyber environment for small-unit training events; our work seeks to replace them with intelligent, **virtual agents**. By leveraging the embedded general
purpose processors (GPP) of tactical software defined radios (SDR), we can dynamically run their automated planning processes in a structured DES. Then, we’ll connect the virtual world with reality by using the internal RF components of the same SDR to transmit detectable waveforms into the physical environment based on a simulated agent’s progression through a planning process to achieve a goal state. **As we anticipate all warfighters carrying hand-held SDRs in the future, our goal is to improve tactical unit proficiency with these systems and make training easily accessible by creating simulation software executable from their organic equipment.**

The MOVES Institute is partnering with MIT-LL in FY 2019 to develop a scenario generation tool to enhance Lincoln Adaptable Real-time Information Assurance Testbed (LARIAT) for tactical cyber training. The system resulting from this collaboration is shown in Figure 4948 [40].
Figure 48 - LVC Environment created using SDRs
6. Role of MOVES

Through the final development of this work, it was critical to have well-developed scenarios for use on the system. For testing this system from 2014 through 2016, subject matter experts (SMEs) in the Marine Corps developed the content required for environment emulation. This process was tedious and demanding. Since it is unrealistic for our operators to develop scenarios prior to each training event, the MOVES Institute is investigating the application of existing constructive simulation to the scenario development effort. In FY19 and early FY20 while one CEMOES is planned for delivery to II MEF, NPS is investigating the application of One Semi-Autonomous Forces (OneSAF) and CyberSAF to the system. CyberSAF is contained in OneSAF version 8.8 and is a government off-the-shelf (GOTS) system developed by Cole Engineering Services, Inc. (CESI). If the CyberSAF is compatible with CEMOES, the Marine Corps seeks to use the simulation as the primary scenario development tool.

The next step in this solution is integrating constructive simulations to make the system more dynamic and ease the creation of scenarios. CyberSAF was selected for
analysis to determine potential integration into LARIAT and the overall infrastructure of CEMOES. At a recent AFCEA Conference, Dr. Daniel Lacks, the Chief Scientist at CESI described CyberSAF as “a OneSAF system configuration, an open source framework designed to provide automation for planning, training, situational understanding, exercise support, testing, experimentation, acquisition, and analysis capabilities in an array of mission-specific kinetic, non-kinetic, and cyber land, sea, air and space environments” [41]. It “addresses interactions between cyber effects, and cyber and kinetic domains, by responding to signals which, for example, may take control and crash a simulated unmanned vehicle; passively watch video feeds generated by the simulation; and activate or deactivate simulated Supervisory Control and Data Acquisition (SCADA) devices” [41]. “OneSAF also provides low fidelity emulation of realistic mission-specific logical environments such as cell towers, IP networks, and satellite links” [41].

We expect to deliver results and integration recommendations in October 2019.

7. **Integration of LVC**

The Live Virtual Constructive (LVC) concept is defined as follows [42]:

- **Live:** A live simulation involves real people operating real systems. Military training events using real equipment are live simulations. They are considered simulations because they are not conducted against a live enemy.

- **Virtual:** A virtual simulation involves real people operating simulated systems. Virtual simulations inject a human-in-the-loop in a central role by exercising motor control skills, decision skills, or communication skills.

- **Constructive:** A constructive simulation includes simulated people operating simulated systems. Real people stimulate (make inputs) to such simulations but are not involved in determining the outcomes. A constructive simulation is a computer program.

The MOVES LVC Laboratory is on a closed network due to use of export-controlled software. This lab seeks to become a testbed to address digital interoperability issues of current tactical C2 systems by creating complex LVC scenarios that interoperate in this simulated environment. The lab systems are shown in Figure 5049.
The LVC Lab is intended to support live virtual simulations such as the control of Software Defined Radios (SDRs) as illustrated in Figure 50.

8. Future Work

This project plans the following work for FY 2020:

- Scenario Development methodology using CyberSAF integrated with LARIAT
- Networking Constructive Simulations to C2 devices for LVC training

Future goals of this project include:

- LVC Lab in all Tactical Units to support SIGINT/Cyber LVC training
- Distance Learning courses to help with network set-up and use

B. ZERO-DAYS, ONE OBLIGATION

Presenter: Anthony Akil, NPS, USN

1. Summary

Zero-day exploits create a tradeoff for nation-states, forcing them to decide what they value more: increasing current and potential operational capability or increasing critical infrastructure and end-user security. Nation states have an obligation to protect their citizens, but they have to decide which of these conflicting objectives best fulfills that obligation. How would utilitarianism inform this decision and U.S. policy? This thesis sought to evaluate the 2017 Vulnerabilities and Equities Policy (VEP) on moral grounds. It used John Stuart Mill’s conception of rule and sanction utilitarianism to define a nation’s moral obligation. It assessed that the VEP, while largely fulfilling the utilitarian obligation, did not completely meet the terms. The VEP as constructed is an agreement between agencies, and permanence and transparency should be increased by
turning it into an E.O. or legislation. The ES role should be shifted from NSA to DHS, and allowance for NDAs should be removed. For further details, see [43].
IV. CYBERSECURITY ARCHITECTURES & HARDWARE

While studies of the fine details of Cybersecurity are important, it is also necessary to examine the architecture and hardware of these systems. Ron Durbin gave a presentation assessing the Cybersecurity risk in weapon system supply chains. Brian Smith’s presentation explained the work of NASA’s Airspace Operations and Safety Program (AOSP) Cybersecurity Group. This session was chaired by Douglas Fouts of the Naval Postgraduate School, Department of Electrical and Computer Engineering.

A. CONTINUOUS MONITORING, FRAGILITY, AND TRUST

Presenter: Ron Durbin, Air Force Institute of Technology School of Systems and Logistics (AFIT/LS)

1. Summary

Authorizing Officials (AO) make risk-based decisions to grant an Authorization to Operate (ATO). For weapon systems, the two primary sources of cybersecurity risk are penetrations and supply chain. We are unaware of an effective process for assessing cybersecurity supply chain risk for operational weapon systems. This project found that mining existing data may provide clues to cybersecurity supply chain risk in operational aircraft. This project recommends a process for identifying the components most likely to have been affected, and also identifies challenges to effective continuous monitoring for new supply chain threats. This project recommends that data sources and data reduction approaches be identified so that those aircraft components most likely to have been subject of a supply chain compromise are examined. For selected components detailed analyses should be performed to rule out compromise. Solutions to challenges in continuous monitoring of supply chain integrity should also be identified.

2. Objectives and Background

This project has three objectives;

- To assure mission success by securing weapon systems against Cyber attacks and incorporating resilience to ensure mission accomplishment in cyber-contested environment.
- To provide Authorizing Officials with credible Cyber risk assessments.
- To accurately assess weapon system supply chain cybersecurity risk.
Laws, regulations, and policies require all information systems be authorized for use (FISMA [44], DoDI 8500.01 [45], and AFI 17-101 [46]). The basis of authorization is that operational utility outweighs security risk. This judgement is absolutely dependent upon accurate assessment of security risk.

The system context for the study is shown in Figure 5150.

Sources of risks are intrusions, hygiene failures, malware, and the supply chain. Intrusions are unauthorized Cyber access to a weapons system or any access that has Cyber effects. Hygiene failures are non-malicious behaviors that place systems at risk. Malware is installation of unauthorized software in a system. Supply chain risks include the incorporation of devices, materials, or components that

- Cause the system to not do that which it must do
- Cause the system to do that which it should not do
- Cause premature failure of subsystems or components

The attack environment is shown in Figure 5251. The risk source model is shown in Figure 5352.
According to the Director of National Intelligence [47], supply chain Cyber risk derives from products that:

- Are defective
- Are counterfeit
- Contain malware
- Contain exploitable weaknesses
- Are from sources with unknown trust

Modifications can be inserted at multiple points in the supply chain. These would ideally (from the attacker’s perspective) permit an adversary to cause a weapon to degrade or fail in a manner and at a time of the adversary’s choosing. It should also be
difficult to detect, i.e., benign until invoked, affect most or all weapons of a particular type, and have a long mean time and high cost to repair. In the best (or worst) case scenario, the weapon will be made operationally ineffective, which will force us to use more costly and less effective means and subject irreplaceable assets such as aircraft and aircrews to unacceptable risks.

Potential supply chain insertion points for malicious modifications are shown in Figure 5453.

3. Proposed Approach

This project proposes to base the estimate of the probability of a supply chain attack ($P_{SCA}$) on an assessment of maintenance anomalies over the previous three years. Additionally, $\Delta P_{SCA}$ will be continuously assessed by examining changes made to system components after $t_0$. A timeline of our proposed approach is shown in Figure 5554.
The project used the following metrics to quantify probability of attacks. We measured the rate of introduction of new components to operational systems in terms of Line Replaceable Units (LRU), Shop Replaceable Units (SRU), and software/firmware. Since the attack path is the introduction of new components, a low rate of replacement suggests lower opportunity for attack. In almost every case there are too many components to permit a comprehensive assessment. We will use our approach to provide objective assessment of susceptibility to supply chain attack and conduct focused, in-depth assessments on the most vulnerable components.

4. Assessing Existing Supply Chain Risk

This project postulates that supply chain malfeasance would cause anomalies during typical aircraft operations. We identified four cases,

1) No anomalies detected, no supply chain attack has occurred
2) No anomalies detected, supply chain attack has occurred
3) Anomalies detected, no supply chain attack has occurred
4) Anomalies detected, supply chain attack has occurred

Initially cases 1 and 3 were excluded and we focused on cases 2 and 4. Additionally, we postulated that instances of mission degradation are documented and that mission degradation attributable to cyber-physical systems is documented in maintenance data systems. These include the Consolidated Aircraft Maintenance System (CAMS) and the Reliability and Maintainability Information System (REMIS). While some attributions will be incorrect due to missing data, false positives and negatives, and Cannot Duplicate (CND) malfunctions, it is, “Far better an approximate answer to the right question, which is often vague, than the exact answer to the wrong question, which can always be made precise.” to quote John W. Tukey.

A diagram of the anomaly filter for addressing case 4 is shown in Figure 5655.
The top-level assessment considers unscheduled maintenance, scheduled updates/upgrades, and incidents. These elements may be assessed in any order, serially or concurrently. The objective is to make an immediate assessment to identify components for in-depth analysis. The aforementioned elements are diagrammed in Figure 57.

![Figure 56 - Anomaly Filter](image)

"...a model is not the truth, it is a lie to help you get your point across." 1

1 Sam Savage, The Flaw of Averages

Figure 57 - Weapon System Supply Chain Risk Assessment

When the maintenance process was examined in greater detail, it was found that the source of the components affects risk exposure. COTS components are inherently less trusted than known developers (trusted h/w, s/w). We immediately assessed the risk of the maintenance process as Low or Moderate, and we recommend an in-depth assessment. A diagram of the maintenance process analysis is shown in Figure 58.
Upgrades involving new development follow a process similar to maintenance, while other upgrades require an assessment of changes. A diagram of the upgrade process is shown in Figure 5958.
The incident process is relatively conservative and more likely to result in an elevated assessment of risk and an in-depth assessment of the target component. A diagram of the incident process is shown in Figure 6059.
Case 2, also known as “the Black Swan”, is unique in that a supply chain attack has occurred but there are no anomalies detected. In this case the existence of a “binary weapon” must be assumed, and there must be a supply chain flaw capable of causing mission degradation or failure in a command and control mechanism. This is a classic example of an Advanced Persistent Threat (APT). No anomalous behavior until deliberately triggered, either automatically by geolocation or some other criterion, or manually via an external entry point in the weapon system (e.g., a legitimate but unused bit-oriented message).

5. Conclusions

We believe that supply chain attacks on cyber-physical systems produce discernible anomalies. Evidence of these anomalies, if it exists, is present in one or more existing data stores. The existence of supply chain tampering in the absence of anomalies may require reassessment of some or all of our approach. We recommend that data
sources and data reduction approaches be identified so that those aircraft components most likely to have been subject of a supply chain compromise are examined. For selected components detailed analyses should be performed to rule out compromise. Solutions to challenges in continuous monitoring of supply chain integrity should also be identified.

B. CYBERSECURITY ENGINEERING PLAN FOR NASA AIRSPACE OPERATIONS AND SAFETY PROGRAM (ASOP)

Presenter: Brian Smith, NASA Ames Research Center, NASA Airspace Operations and Safety Program (AOSP)

1. Summary

The Airspace Operations and Safety Program (AOSP) Cybersecurity Engineering Plan (CEP) describes the technical approach to the organization and management of the AOSP Cybersecurity Engineering implementation. This project found that the AOSP Cybersecurity Group plans to tailor and implement NASA System Engineering (SE) processes and industry best practices in Security Engineering in support of the program’s mission to develop, produce, and transition secure and securable, trustworthy technology products to their partners. This project recommends that the AOSP Cybersecurity Engineering Plan provide guidance for how all technical and administrative cybersecurity engineering activities will be integrated throughout the program.
2. Introduction

Figure 61 - Systems Engineering

The discipline of systems engineering is complex, and practitioners must balance protection needs, security relevance, security risk management, and trustworthiness and assurance. These elements are shown in Figure 61. The AOSP Cybersecurity Engineering Plan will enable AOSP to support the development of secure and securable research technology products within cost, schedule and other applicable constraints in order to enhance, streamline and assure their ready acceptance and integration within the customer’s security environment and operational context upon transition to end users outside of NASA.

The AOSP Cybersecurity Group will tailor and implement NASA System Engineering (SE) processes and industry best practices in Security Engineering in support of the program’s mission to develop, produce and transition secure and securable,
trustworthy technology products to their partners. This plan defines the technical management of the AOSP Cybersecurity Engineering processes and will evolve and be revised to contain any changes and all phases of the program’s life cycle.

This plan also describes how all technical and administrative cybersecurity engineering activities will be integrated throughout the program. It supports the management of program activities by providing the top level technical implementation plan. Additionally, it will act as the primary source document for any lower level technical plan and will provide the basic implementation and processes which all lower level plans will inherit.

3. Approach and Data

AOSP’s plan to use NASA SE processes and industry best practices defines the technical management of the AOSP Cybersecurity Engineering processes and will evolve and be revised to contain any changes and all phases of the research program’s life cycle.

The AOSP Program is and will be responsible for communicating to the AOSP Cybersecurity Engineering Group technologies and products requiring cybersecurity engineering design and development activities. The AOSP Cybersecurity Engineering Group will in turn engage with AOSP/ARMD Program and Project Management to assist with cybersecurity concern mitigation and/or integration arising from the program goals to successfully transition its technology products to the customer environment.

Project Formulation Engagement will assist with formulation activities to ensure cybersecurity principles are infused from the beginning and assure that a clear risk–benefit balance is maintained to manage resources by including cybersecurity risks and concerns. Technology Formulation and Development will provide guidance during technology and development, especially in avoiding surface technology issues that may impact long term viability or adoption of the technology product into the customer target environment. Project KDP/Tollgate reviews will provide guidance and assistance at Key Decision Points (KDPs) during the program, project and technology development life cycle.

The Remaining Secure Life (RSL) concept could prove useful for emerging aviation IT systems coming out of the R&D world. This concept is similar to Remaining Useful Life (RUL) used by fault prognosis systems to predict the remaining useful life of
operational components or systems. Just as prognostics systems seek to detect impending non-malicious failures and assessing remaining useful life based on the damage sustained, so will Security Prognostics assess cyber-health of a system and its Remaining Secure Life – a measure of the urgency with which security issues must be addressed. The study of comprehensive failure modes in the progression of Cyber damage leads to the assessment of Remaining Secure Life (RSL). Some compromises will be fairly benign – while others may require immediate action. Depending on mission context or state of a critical asset, action to shut down the asset may be required and feasible, but in other cases a more measured response may be required.

The applicable documents and authorities are identified in Figure 6261.

![Figure 62 - Applicable Documents and Authority](image)

The implementation of the security engineering technical processes proposed by the AOSP Cybersecurity Group is shown in Figure 6362.
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Business and Mission Analysis Process</td>
</tr>
<tr>
<td>5.2</td>
<td>Stakeholder Needs and Requirements Definition Process</td>
</tr>
<tr>
<td>5.3</td>
<td>System Requirements Definition Process</td>
</tr>
<tr>
<td>5.4</td>
<td>Architecture Definition Process</td>
</tr>
<tr>
<td>5.5</td>
<td>Design Definition Process</td>
</tr>
<tr>
<td>5.6</td>
<td>System Analysis Process</td>
</tr>
<tr>
<td>5.7</td>
<td>Implementation Process</td>
</tr>
<tr>
<td>5.8</td>
<td>Integration Process</td>
</tr>
<tr>
<td>5.9</td>
<td>Verification Process</td>
</tr>
<tr>
<td>5.10</td>
<td>Transition Process</td>
</tr>
<tr>
<td>5.11</td>
<td>Validation Process</td>
</tr>
<tr>
<td>5.12</td>
<td>Operation Process</td>
</tr>
<tr>
<td>5.13</td>
<td>Maintenance Process</td>
</tr>
<tr>
<td>5.14</td>
<td>Disposal Process</td>
</tr>
</tbody>
</table>

Figure 63 - Security Engineering Technical Processes Implementation

Additional systems engineering functions and activities are shown in Figure 6463.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>System Safety</td>
</tr>
<tr>
<td>7.2</td>
<td>Engineering Methods &amp; Tools</td>
</tr>
<tr>
<td>7.3</td>
<td>Specialty Engineering</td>
</tr>
</tbody>
</table>

Figure 64 - Additional SE Functions and Activities

The AOSP Cybersecurity Engineering Group (CEG) uses an architectural methodology to determine and analyze the Protection Needs required by the future customer’s operational context. The group develops three perspectives of the customer’s operational environment. These perspectives are developed from artifacts and information about the operational context provided by the customer and are herein
referred to as enabling products. The perspectives and their respective enabling products are the stakeholder’s perspective, the system perspective, and the trades perspective, and are shown in Figure 6564.

Figure 65 - Architectural Principles

The Protection Needs development activity is diagrammed in Figure 6665. A high level architectural view of the process is shown in Figure 6766.
Many of the systems covered by the SEP involve network-centric operations. A diagram of the network-centric operations domain is shown in Figure 68.

There are a few caveats. While the SEP does utilize ISO/IEC 15288 [48], a systems engineering standard covering processes and lifecycle stages that are summarized in Figure 69, it does not utilize IEC 61508 [49].
IEC 61508 is an international standard published by the International Electrotechnical Commission consisting of methods on how to apply, design, deploy, and maintain automatic protection systems called safety-related systems. Its components are shown in Figure 7069.

There are multiple organizations that have security responsibility for the National Aerospace Standard (NAS). They are as follows:

- Aviation Information Sharing and Analysis Center (A-ISAC) - The Aviation sector-specific Information Sharing and Analysis Center (ISAC) is a non-profit,
member-driven organization formed by critical infrastructure owners and operators to share information between government and industry.

- **Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)** - Within the NCCIC (National Cybersecurity and Communications Integration Center), the ICS CERT program provides research and advisories through the efforts of joint partnerships within industry, industry experts, and the Advanced Analytic Lab (AAL).

- **National Cyber Cybersecurity and Communications Integration Center (NCCIC)** - A 24/7 Cyber situational awareness, incident response, and management center that is a national nexus of Cyber and communications integration for the federal government, intelligence community, and law enforcement.

- **Cyber Information Sharing and Collaboration Program (CISCP)** - A program for public-private information sharing whereby the Department of Homeland Security (DHS) and participating companies share information about Cyber threats, incidents, and vulnerabilities.

- **Enhanced Cybersecurity Services (ECS)** - A voluntary information sharing program that helps U.S.-based public and private entities protect their systems from unauthorized access, exploitation, or data exfiltration.

The cybersecurity engineering group technical effort boundary is shown in Figure 71.

**OPS = Office of Protective Services**

**OCIO = Office of Chief Information Officer**

Figure 71 - Cybersecurity Engineering Group Technical Effort Boundary

The Cybersecurity Engineering Group (CEG) does not control nor is it responsible for:
- Directly funding or executing security mitigation work within an R&D project development effort.

- Operational security control implementation (deployment, configuration, assessment) in NASA environments and systems. This includes physical, intelligence and IT systems security considerations.

- Operational security control implementation (deployment, configuration, assessment) in customer environments and systems. This includes physical, intelligence and IT systems security considerations.

- Lack of communication among high level NASA management as to the expectations, requirements, and implications of the overall security process.

The CEG utilizes modern systems engineering principles that focus on developing “trustworthiness” as a quality attribute of the system as a whole rather than making it “safe”, “secure”, or “verified and validated” in any deterministic fashion. The security engineering framework that it uses is shown in Figure 72.

![Security Engineering Framework](image)

Figure 72 - Security Engineering Framework
The Protection Needs Development Activity is executed with the following foci:

- **Purpose**
  - Define Stakeholder System Security Requirements providing needed capabilities in the Stakeholder’s operational environment.

- **Inputs (from)**
  - Stakeholder Perspective Analysis
  - System Perspective Analysis
  - Trades Perspective Analysis

- **Expected Outcomes**
  - Stakeholder security interests and concerns are identified.
  - Required security characteristics, context and capabilities for all applicable life cycle stages of the technology under development are identified.
  - Stakeholder assets and their categorization are identified.
  - Assets posture vs. threat environment is identified.
  - Asset protection priority and assurances needed are identified.
  - Stakeholder Protection Needs are identified and prioritized.
  - Security derived system constraints are identified.
  - Stakeholder Security Requirements are derived from Stakeholder Protection Needs.
  - Security related system performance measures are identified.
  - Stakeholder agreement and concurrence that their Protection Needs and expectations are met via the Security Requirements developed is achieved.
  - Enabling systems/services needed to support security aspects for stakeholder needs and requirements are identified and catalogued as to their availability.
V. PANEL ON MONTEREY CYBER INSTITUTE

Jeff Paduan (Chair), Naval Postgraduate School, Dean of Research, Jim Newman, Naval Postgraduate School, Space Systems Academic Group, Dan Boger, Naval Postgraduate School, Department of Information Sciences, and John Drummond, SPAWAR, Naval Information Warfare Center Pacific

1. Introduction

The objective of the Monterey Cyber Institute is to respond to the following challenges:

- How can NPS maximize its impact within DoD around the critical topic of Cybersecurity?
- How can the essential role for industry partnerships be supported as suggested by SECNAV Spencer?

NPS is responding to these challenges by elevating the collaborations goal within its 2018-2023 strategic plan, Action H1.1, in order to streamline the processes for working with industry and other academic institutions.

To quote the Secretary of the Navy,

“We all have an interest in ensuring NPS endures as the postgraduate research and educational institution of choice for the Navy-Marine Corps team and our partners. But going even further, I want this institution to be the primary educational and research-based enterprise that partners with the private sector and academia to provide solutions to the vexing problems facing national security across the whole of government.”

The Honorable Richard V. Spencer, 2 February 2018.

Government groups are not coordinated. The National Institute of Standards and Technology (NIST), for example, lacks standards in some areas and penalties for breaking standards in others. Another example is the Department of Homeland Security (DHS), which lacks critical infrastructure needed to manage Cyber risk.

Industry is waking up to the threats. As hackers and state actors become ever more sophisticated and capable, the government is likely to react (or over-react) soon.

2. Why Monterey?

- NPS is a unique graduate school with a defense focus and students with real-world experience in defensive cyber.
NPS has cutting-edge Cybersecurity research, including unique and world-class experience from faculty and students in Computer Science, Electrical Engineering, Defense Analysis, and Operations Research.

Insider Threat Expertise exists at the Defense Manpower Data Center (DMDC), Defense Personnel Security Research Center (PERSEREC) and Naval Postgraduate School.

NPS is in a desirable location capable of attracting leading industry experts; it has close proximity to Silicon Valley and its many technology companies.

There are opportunities for policy work through partnerships with the Panetta Institute, Stanford’s Hoover Institute, and Georgia Tech’s Sam Nunn Institute.

NPS has substantial and available SCIF space.

NPS has proximity to California State University, Monterey Bay (CSUMB), the Defense Language Institute (DLI), and the Middlebury Institute of International Studies (MIIS).

NPS has direct support from SECNAV Spencer

3. How Can the Monterey Cyber Institute (MCI) be successful?

NPS has unique capabilities but is subject to all government rules. MCI, therefore, needs a bridging organization to be successful. Possible bridging organizations include:

- University Accelerated Research Center (UARC)
- Federally Funded Research and Development Corp (FFRDC)
- Air Force WERX (AFWERX)
- In-Q-Tel (IQT)
- Defense Innovation Unit (DIU)
- Other Transactions Authority (OTA)

UARC Model is the best (and possibly only) mechanism. The Georgia Tech Research Institute (GTRI), for example, has a broad range of Cyber expertise, including:

- Quantum computing and sensing
- Trusted microelectronics
- Vulnerability assessment of embedded systems (Relevant to DoD COTS UAV ban)
- Mission-assured C2
- Analytics for Cyber defense, threat, and attribution (Overlaps with NPS CORE Lab interests and capabilities
- Multi-level secure software systems
- Advanced cyberspace operations
Georgia Tech has Cyber policy interests in the “Sam Nunn Center”, and can coordinate with the Panetta and Hoover Institutes. Figure 73 shows how the UARC model could apply to the Monterey Cyber Institute.

Figure 73 – UARC Model for MCI Bridging Organization

4. Questions for Consideration

- How do you see Cybersecurity playing in your field?
- Is there a need for DoD/Industry collaboration?
- What are some sample projects?
  - SCADA controls for industrial machinery?
  - Municipality/first responder threats from Cyber attack?
  - Cyber defense policy?
- Is this already happening? If so, where?
VI. CYBER FUNDAMENTALS & MACHINE LEARNING

This section of the workshop focused on the fundamentals of Cyber and applications of machine learning. David Dampier outlined the current state of Cybersecurity education and proposed a standard curriculum for masters-level and doctorate degrees. Stephen Hayne gave a presentation on NetBrane, a machine learning analytics engine developed to defend against DDOS attacks. John Monaco’s presentation addressed the security risks presented by machine learning when applied to communication between distributed system components. Brian Smith reprised his presentation on the risks of integrating AI the National Airspace System from the first section of the workshop. Finally, Nikolaj Bjørner presented the work of Microsoft Research on their Z3 SMT solver and described some of its applications to Cyber problems. This session was chaired by John Monaco of the Naval Postgraduate School and David Dampier of the University of Texas at San Antonio.

A. FUNDAMENTALS OF CYBERSECURITY

Presenter: David Dampier, University of Texas, San Antonio

1. Summary

Cybersecurity education is going through a transition at this time toward accreditation and standardization. There is very little similarity between what is taught at most institutions teaching Cybersecurity in the U.S., but there is a need to provide some standardization.

This project found that most schools that claim to be Centers of Excellence in Cybersecurity Education are merely centers of interest. The number of graduates in Cybersecurity, although increasing annually, is not enough to meet the demands of government and industry employers. This is exacerbated by the fact that many graduates require extensive training.

This project recommends that standardized curricula be developed for Cybersecurity education. That standardization should be done with an eye toward NIST standards [50], CAE Knowledge Unit standards [51], and industry needs. It should be noted that the Accreditation Board for Engineering and Technology (ABET) is also
releasing Cybersecurity criteria to join other computing disciplines such as computer science, information systems and information technology.

2. Background

Cybersecurity is first and foremost a problem, not a discipline. Any instruction must be presented as an approach to solve the Cybersecurity problem, no matter what specific discipline is involved (e.g., computing, engineering, project management, etc.). Instruction must also be hands-on either through live exercises or through virtualized experiences equivalent in rigor, and graduates must be able to go to work Day One.

There are three components of Cybersecurity:

1) Confidentiality
2) Integrity
3) Availability

There are also other factors to consider, such as risk assessment and non-repudiation. These components are applied in three paradigms:

1) Prevention of potential threats.
2) Detection and analysis of ongoing threats.
3) Post-mortem analysis of past threats.

A diagram of the National Institute for Cybersecurity Education (NICE) Cybersecurity Framework [52] is shown in Figure 7472.
There are ten primary principles of Cybersecurity.

1) Domain Separation: Separating areas where resources are located to prevent accidents and loss of data. Another way to put it is keeping information worlds from colliding.

2) Process Isolation: A process occurs when a task is executed. Keeping processes separated prevents the failure of one process from negatively impacting another.

3) Resource Encapsulation: Resources in this context are hardware, system objects, or processes. These must be separated and used as intended.

4) Least Privilege: This limits what access people have to your resources and what they can do with them.

5) Layering: Having multiple layers of defense protect information. If one layer is defeated, the next layer should catch it. This is also known as redundancy.

6) Abstraction: A fancy word for summarizing or explaining in a way that can be easily understood. Leaving the details hidden to avoid information overload.

7) Information Hiding: Any attempt to prevent people from being able to see information.
8) Modularity: Each module has its own function, is able to be inserted or removed from a project, and is interchangeable with other modules.

9) Simplicity: If something is less complicated, it’s less likely to have problems and easier to troubleshoot and fix.

10) Minimization: To simplify and decrease the number of ways software can be exploited.

3. Proposed Criteria

The structure of the proposed ABET Engineering Accreditation Criteria

Cybersecurity engineering curriculum must provide both breadth and depth across the range of engineering topics implied by the title of the program. This includes probability, statistics, and cryptographic topics including applications appropriate to the program. It must also include discrete math and specialized math appropriate to the program, such as abstract algebra, information theory, number theory, complexity theory, and finite fields, as well as engineering topics necessary to analyze and design complex devices, software, and systems containing hardware, software and human components.

Coverage of computer science topics is also necessary. The first of these topics is the application of security principles and practices to the design, implementation, and operations of the physical, software, and human components of the system as appropriate to the program. The second topic is the application of protective technologies and forensic techniques. The third topic is the analysis and evaluation of components and systems with respect to security and to maintaining operations in the presence of risks and threats. The final topic is the consideration of legal, regulatory, privacy, ethics, and human behavior topics as appropriate to the program.

In regard to faculty, the program must demonstrate that faculty members teaching core engineering topics understand methods of engineering design, engineering problem solving, and engineering practice with specific relevance to security. These program criteria provide a foundation for lifelong learning in a dynamic field. They provide a uniform set of sound principles to help students, employers and programs.

The proposed ABET Computing Accreditation Commission (CAC) Cybersecurity curriculum differs slightly from the EAC curriculum. In addition to the general curriculum requirements, the following specific student outcomes are required:

- An ability to apply security principles and practices to the environment, hardware, software, and human aspects of a system.
An ability to analyze and evaluate systems with respect to maintaining operations in the presence of risks and threats. The CAC curriculum requirements specify topics, but do not prescribe specific courses. These requirements include at least 45 semester credit hours (or equivalent) of computing and Cybersecurity course work. The course work must cover the application of the crosscutting concepts of confidentiality, integrity, availability, risk, and adversarial thinking. Additionally, fundamental topics from each of the following subjects should be covered:

- Data Security
- Software Security
- System Security
- Human Security
- Organizational Security
- Societal Security
- Advanced Cybersecurity topics that build on crosscutting concepts and fundamental topics to provide depth.
- At least six semester credit hours (or equivalent) of mathematics that must include discrete mathematics and statistics.

The knowledge of the following subjects is critical to Cybersecurity education.

- Fundamental understanding of programming as a problem solving tool
- Knowledge of data organization, including numbering systems (binary vs. decimal vs. hexadecimal) and data structures, sizes, and types.
- Knowledge of persistent memory types. These include physical and logical storage, the architecture, geometry, interfaces, and sector addresses of hard drives, and the types of removable media such as Firewire, USB, and multimedia cards.
- Knowledge of volatile memory types. These include RAM, process memory, virtual memory like pagefile or swap, threads, modules and libraries, Windows volatile data, and Linux/Unix volatile data.
- Knowledge of file systems, including information stored by file systems in general and key differences between major file systems.
- Knowledge of network fundamentals. These include the OSI/Internet model, basic protocols, and IP addresses, ports, and services. Familiarity with forensic data that can be obtained from networking devices (IDS/IPS, firewalls, routers, switches, DNS servers) and basic levels of network data analysis is also necessary.
- Knowledge of virtualization, including VM configuration, setup, and guest analysis, the uses of virtualization, types of clouds and hypervisors, and supply chain issues with virtualized hardware.

Current academic programs in Cybersecurity take three forms. The first is a Bachelor of Business Administration (BBA) in Cybersecurity. These can be augmented with a minor in digital forensics or a certificate in pathogenic outbreak investigations. The second is an MS in Information Technology with a concentration in Cybersecurity. The third is a Ph.D. in Information Technology, with a concentration in Cybersecurity. A Venn diagram of the common areas of study between digital forensics and biological defense is shown in Figure 7573.

![Venn Diagram](image)

Figure 75 - Cross Disciplinary Subjects of Digital and Biological Forensics

A sampling of Cybersecurity courses is shown in Figure 7674.
<table>
<thead>
<tr>
<th>Core curriculum</th>
<th>Core Cyber security CBK (6 courses)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business CBK* (18 courses)</td>
<td>Operating Systems Security IS3033</td>
</tr>
<tr>
<td></td>
<td>Telecommunications IS3413</td>
</tr>
<tr>
<td></td>
<td>Network security IS3423</td>
</tr>
<tr>
<td></td>
<td>Info Assurance and Security IS3513</td>
</tr>
<tr>
<td></td>
<td>Programming IS2033 &amp; IS2043</td>
</tr>
<tr>
<td>Core IS CBK (1 course)</td>
<td>Cyber security electives (3 courses)</td>
</tr>
<tr>
<td>Computing for IS</td>
<td>Intrusion Detection/Incident Response IS3523</td>
</tr>
<tr>
<td>Technology Management</td>
<td>Secure Electronic Commerce IS4463</td>
</tr>
<tr>
<td>Project Management</td>
<td>Info Assurance Policy IS4473</td>
</tr>
<tr>
<td></td>
<td>Digital Forensic Analysis IS4433</td>
</tr>
<tr>
<td></td>
<td>Cyber Physical Systems IS4513</td>
</tr>
<tr>
<td></td>
<td>Cyber Law IS3533</td>
</tr>
<tr>
<td></td>
<td>Network Operations IS4033</td>
</tr>
</tbody>
</table>

Figure 76 - Sampling of Cybersecurity Courses

The structure of the first variant, a BBA with a major in Cybersecurity is shown in Figure 7775.

- Intrusion detection
- Incident response
- Digital forensics
- Secure network design
- Secure e-commerce
- Secure s/w development
- Secure network ops
- Unix/Linux security
- Cryptography
- Attack & defend
- Cyber physical systems
- Malware analysis
- Reverse engineering
- Network security
- Cyber law
- Cyber security policy
- Risk assessment
- Security best practices

Figure 77 - Major: BBA in Cybersecurity

The structure of a MS in IT with a concentration in Cybersecurity is shown in Figure 7876.
A world-class online Cybersecurity education should have three traits. The first is a remote lab capability, with experiential learning, scalability, and 24/7 remote access. The second is a modular curriculum that will share common modules, retain unique modules, and combine modules into a course. The third is cross-disciplinary coursework, including an interdisciplinary core and capstone, and a mixture of majors in modules. A diagram illustrating these traits is shown in Figure 7977. Extracurricular activities are described in Figure 8078.
Figure 79 - World-Class Online Cybersecurity Education
B. NETBRANE: DETECTING AND PROTECTING FROM DDOS ATTACKS

Presenter: Stephen C. Hayne, Colorado State University

1. Summary

In order to defend against a distributed denial of service (DDOS) attack, defensive software should be aware of current traffic, topology, and potential next attack. Geographically distributed cloud capabilities and Software Defined Network (SDN) should be quickly deployed to minimize disruption and collateral damage. Once under attack, use DNS/anycast infrastructure to redirect traffic. SDN should be employed to filter attack traffic and tunnel legitimate traffic.

NetBrane is a dynamic machine learning on-premises “cloud” analytics engine. It uses the following elements to detect and counter DDOS attacks: Internet structural information, Line-Rate capture, Traffic modeling and outlier classification, and Hacker Chatter.

This project found that firewall rules based on outliers can reduce attack traffic significantly to pre-attack levels with few false positives. If Colorado State University had NetBrane, the 2014 NTP DDoS would have been blocked within minutes with little impact to services. This project proposes to deploy to an ISP test site with mirrored traffic to minimize network risk within $100k capital expenditure per sensor.
2. Problem Description and Approach

Distributed denial of service attacks can cripple government and business alike. Examples include, but are not limited to GitHub, Mirai, Krebs, SpamHaus, and Akamai. While the monetary cost is significant, the impacts of DDOS attacks are increasingly non-financial and serve as a cover for other subversive operations. If small businesses hosted by ISPs are attacked (e.g., by 300,000+ IOT devices), they can be forced into bankruptcy. Amazon risks $3.5B in transactions/sales during CyberMonday, and cannot be offline for more than four hours during this critical time. The solution to DDOS attacks needs to be distributed and proactive, with continuous high-speed reconnaissance, reliable detection and prediction models, networked structural information to avoid collateral damage, quick and robust filter deployment, and the ability to use tips from insiders to stay ahead of the game.

The approach used by NetBrane sees the tsunami coming and blocks the wave(s) as they hit, allowing it to reduce attack traffic by >80% within a few minutes. NetBrane is a dynamic machine learning on-premises “cloud” analytics engine. It uses the following elements:

- Internet structural information (BGPMon) – prefix hijack alerts
- Line-Rate capture (DPDK) and flow creation (Flowride) – 40G
- Traffic modeling and outlier classification (FPCA) - processes 10G streaming data and detects outliers
- Hacker Chatter (RIPEX) - 7 dark forums monitored/analyzed

A high-level diagram of NetBrane is shown in Figure 8179
A diagram of NetBrane’s architecture is shown in Figure 82-80.

Figure 82 - NetBrane Architecture
Flow Creation engine:

- Flowride → {Protobuf → {JSON, CSV} or sflow / Netflow}
- We deploy an SDN network
- Two options for flow capture:
  - on a separate node, ii) directly on the SDN node with OVS and virtual tap devices

This process is realized using the structure shown in Figure 83.81.
The Flowride metrics are shown in Figure 8482.

For line speeds of 40Gbps at 3.5Mpps and ~35000 active flows, 12 cores are needed. In order to export data to consumers, MessageQueue (RabbitMQ) and interfaces to sFLOW/NetFlow collectors are used. The latter is what most network admins know and already use.

The analytics workflow in NetBrane is shown in Figure 8583. The process is mostly automated, augmented by human assistance for interpretation and validation in the “Assess Risk” step.

![Flowride Performance Metrics](image)

**Figure 84 - Flowride Performance Metrics**

**Figure 85 - Analytics Workflow**
The analysis must cope with missing sensor values which are illustrated in Figure 8684. Network sensors send the data they collect in a stream, and the table shows the effects of interruption at various points in the stream of data (i.e., middle, end, or randomly throughout). The irregular behavior of the sensors could be just due to sensor issues, or it could be due to malicious attack patterns.

<table>
<thead>
<tr>
<th></th>
<th>PCA</th>
<th>PCA(imputed)</th>
<th>MLE(imputed)</th>
<th>PACE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Middle</strong></td>
<td></td>
<td>RM: 97.62% (2), 20 minutes</td>
<td>unable</td>
<td>98.81% (45), 10 seconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CM: 96.43% (3), 20 minutes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>KF: 95.24% (3), 20 minutes</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>End</strong></td>
<td></td>
<td>RM: 92.86% (5), 20 minutes</td>
<td>RM: 92.86% (5), 15 minutes</td>
<td>95.23% (15), 10 seconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CM: 95.25% (4), 20 minutes</td>
<td>CM: 95.25% (4), 15 minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>KF: 91.67% (12), 20 minutes</td>
<td>KF: 91.67% (12), 15 minutes</td>
<td></td>
</tr>
<tr>
<td><strong>Random</strong></td>
<td>unable</td>
<td>RM: 80.95% (7), 20 minutes</td>
<td>RM: 80.95% (7), 15 minutes</td>
<td>90.48% (26), 13 seconds</td>
</tr>
<tr>
<td>(Irregular)</td>
<td></td>
<td>CM: 84.52% (15), 20 minutes</td>
<td>CM: 84.52% (15), 15 minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>KF: 88.1% (19), 20 minutes</td>
<td>KF: 88.1% (15), 15 minutes</td>
<td></td>
</tr>
</tbody>
</table>

Figure 86 - Missing Values (Sensors)

DDOS attacks are not typically a single event. A replay of the NTP attack from 2014 is shown in Figure 8785. The graph shows how the number of network packets evolved over time. There were several “waves” which consumed all bandwidth during each wave.
This was a reflection attack from all over the globe, as shown in Figure 8886.
This pattern of DDOS activity enables machine learning to drive reactive defensive measures. Currently the NetBrane system needs to be initialized during a period of “normal” activity (i.e., pre-attack). This project analyzed a sliding window of history of around 30-45 minutes, but did keep a historical volume (by minute) of all prior available data (configurable) in an SQL database for thresholding. The threshold is set pre-attack, during initialization. Graphs of the packet count and bytes over time data are shown in Figure 89.

The threshold is defined by the following formula,
\[
\max_{t \in H} \{X_t\} + cv \cdot SE \left( \max_{t \in H} \{X_t\} \right)
\]

Where \(X_t\) is series (minutes) of aggregated packets or bytes, \(H\) is the window of history kept, \(cv\) is a specified critical value, and \(SE \left( \max_{t \in H} \{X_t\} \right)\) is the standard error from a locally estimated scatter plot smoothing (LOESS) model. This represents the largest acceptable packet or byte count and accounts for variability among the history.

Fuzzy Principal Component Analysis (FPCA) is applied in two passes, both of which remove outliers. The Eigenfunction distribution(s) are more “normal” and thus reduce the False Detection Rate (FDR). An example is shown in Figure 9088.
Figure 90 - FPCA Two Passes
DDOS attacks typically have network flow patterns that show up as statistical outliers. This is illustrated with data from the NTP attack in Figure 9189.
The project used circle plots to help human analysts see and recognize patterns in network traffic. A diagram explaining a circle plot is shown in Figure 9290.

Cluster analytics reveal different types of network traffic patterns that are shown in Figure 9391. Note that outlier patterns are not necessarily all threat.
Example circle diagrams from both the pre-attack and attack period are shown in Figure 94 and Figure 95, respectively. The distributions are visibly different.

Firewall rules based on outliers can reduce attack traffic significantly to pre-attack levels with few false positives, as illustrated in Figure 96. If CSU had NetBrane, this DDoS would have been blocked within minutes with little impact to services, and the targeted systems identified for patching.
Figure 95 - Attack Period

Figure 96 - NTP Attack Packets over Time
There are multiple benefits to NetBrane. First, it provides automated, distributed DDoS detection and mitigation in minutes. Its proactive defense minimizes collateral damage by deploying defenses informed by network structure, using massively parallel, elastic private cloud-based processing and ready-to-go defense measures informed by network reputation and hacker activity intelligence. Additionally, NetBrane has a small deployment footprint (6U).

The competition to NetBrane is assessed in Figure 97.

<table>
<thead>
<tr>
<th>Approach</th>
<th>Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDN networks</td>
<td>works for Web... expensive must allow others to host your content (see Krebs)</td>
</tr>
<tr>
<td>Massive over-provisioning</td>
<td>works for the big few, e.g., Google, Microsoft, not for the little guy</td>
</tr>
<tr>
<td>Shared scrubbing Data Centers</td>
<td>expensive, susceptible to collateral damage (SpamHaus)</td>
</tr>
<tr>
<td>Firewall(s)</td>
<td>Ineffective if your access is saturated</td>
</tr>
<tr>
<td>IDS</td>
<td>reactive, alert overload, human-level response, little automation</td>
</tr>
</tbody>
</table>

Figure 97 – Assessment of Competing Approaches

3. **Status and Future Work**

Currently, a prototype of the 40G flow-creation tool and an advanced prototype of the 40G traffic line-capture tool have been created. The existing analytics infrastructure can process up to 10G of streaming lab data, and the Hacker Chatter tool has 7 dark forums monitored/analyzed.

The next step is to deploy to a real test site. This site will mirror traffic, thereby incurring zero network risk. There will be a $50k capital expenditure per sensor on-premises, including server, storage, and tap. $500k in funding from DHS and $150k in-kind from ISP are also required.

C. **TIMING SIDE CHANNELS DUE TO HUMAN-COMPUTER INTERACTION**

Presenter: John Monaco, Naval Postgraduate School, Computer Science Department
1. Summary

There is a growing opportunity for unintended interference and communication between distributed system components. Emerging machine learning and statistical modeling techniques are capable of detecting and exploiting this kind of information leakage. The detection, measurement, and mitigation of such attacks remains a challenge.

This project found that the urgency of a message is the need to transmit that message to maintain near-real-time responses in a distributed system. However, the time the message transmits can provide information about the internal state of a component which should remain hidden. There is a tradeoff between these two competing criteria.

This project recommends that the tradeoff between message urgency and information leakage be systematically controlled by either leveraging existing sources of noise or obfuscating the signal by introducing noise.

2. Background

Distributed systems have a propensity to leak information through the timing of messages between system components, despite those messages being encrypted. A way malicious third parties can exploit this information leakage to perform device fingerprinting, traffic analysis, and other forms of reconnaissance is shown in Figure 98.

![Figure 98 - Timestamps Exposed](image-url)
The timing patterns of messages have been historically referred to as “the senders’ fist”, in the initial context of telegraph messages. A diagram of how the sender’s fist was used prior to modern computing is shown in Figure 99. During World War I, the timing patterns were analyzed as a means of authenticating whether a message originated from a known trusted sender or not.

A diagram of how the sender’s fist can be used in the 21st century to impact Cybersecurity is shown in Figure 100.
The host’s OS platform and version can be identified from DOM event timestamps. The threats introduced by this capability are de-anonymization, device tracking, and passive analysis. The following diagrams show how the timing of various processes can be used to identify the host system. Figure 10199 shows how these patterns can be distinguished in the time domain and in the frequency domain.

Figure 101 - Clock Tick Reveals OS Family

Figure 102100 explains the reason for these differences in the timing patterns. The actual time refers to the actual time of a key press, or more generally to the occurrence of any data triggering event. The software becomes aware of these events when the data is sampled at a slightly later time, which is typically driven by an internal systems clock.
Several computational approaches can be used to automatically categorize these distinctions. Figure 103 illustrates the use of an entropy measure for remotely fingerprinting a system’s clock rate based on the timings between transmitted messages.

Time delay embedding can also be used to identify hosts based on differences revealed in phase space. This is shown in Figure 104 and Figure 105.
3. Mitigation Strategies

There are three mitigation strategies to deal with information leakage: concealment, impediment, and obfuscation. Obfuscation using a timing buffer is shown in Figure 106104.

Figure 104 - Time Delay Embedding

Figure 105 - Host Differences Revealed in Phase Space
There is, of course, a tradeoff between information gain and the time lag (i.e., usability and security). This is illustrated in Figure 107.

A Keystroke-Level Online Anonymization Kernel, or “kloak”, can be used to obfuscate typing behavior on the host. The function of a kloak is shown in Figure 106.
A related question is whether use of a cloak can make it easier to identify the individual cloak user.

![Figure 108 - Keystroke-Level Anonymization Kernel](image)

In general, the homogeneity of a system can be an indicator for side channel attack severity, with more homogenous systems having a higher risk than less homogeneous systems. This is shown in Figure 109.

![Figure 109 - Homogeneity as an Indicator](image)

In conclusion, timestamps are pervasive. Each device and user has a “fist” that can be used to identify and subvert a system. This project recommends that the tradeoff between usability and security be systematically controlled by either leveraging existing sources of noise or obfuscating the signal by introducing noise from new sources.

**D. AI AND SAFETY/SECURITY THREATS**

Presenter: Brian Smith, NASA Ames Research Center, NASA Airspace Operations and Safety Program (AOSP)
1. **Summary**

In the short-term, the project sought to identify practical safety/security risks in deploying machine learning systems: data poisoning, training set inference, lack of model interpretability, and undesirable model bias. In the mid-term, it assessed potential safety/security risks of future AI systems that are more powerful and more broadly deployed than those used today. Relevant problems in this space include scalably specifying and supervising reward-based learning, preventing unwanted side effects, generalizing out of domain, and ensuring that systems remain under control. In the long-term, how might we ensure that an engineered (super)intelligence is aligned with our values, and what procedures can be used to conserve this alignment while supporting recursive self-improvement in security? For details, see Smith’s previous presentation in II.B.

E. **SECURING & BREAKING CYBER USING SMT**

Presenter: Nikolaj Bjørner, Microsoft

1. **Summary**

This project sought to enable trusted code development using automated theorem proving. It also sought to uncover security vulnerabilities with scalable and intelligent search. Z3 is a state-of-art Satisfiability Modulo Theories (SMT) solver from Microsoft Research which is used in a wealth of applications, including securing TLS/crypto libraries for Project Everest, fuzzing binaries for Project Springfield (originally called SAGE), and securing ACLs for Azure. This project recommends that verification tools be developed leveraging SMT technologies and integrated engineering processes. It also recommends that newer trends in Cyber, such as Software Defined Networking (SDN) and blockchain, be advanced. Finally, it recommends leveraging modern Cloud computing infrastructures for advancing the scale of SMT, propositional satisfiability (SAT) and automated theorem proving (ATP) technologies. SMT solving technologies are advanced and developed at a number of institutions. Besides Z3, the Yices solver is developed at SRI international and CVC4 is co-developed at Stanford University and University of Iowa.
2. **Background**

Models – a set of values for variables that make a formula true – are important for cyber applications. Classical theorem provers do not produce models, but SAT and SMT solvers like Z3 do. Z3 solved to date hundreds of billions of constraints created by SymEx tools, including SAGE checking Win7-10 and Office, and is used by Pex, Static Driver Verifier, and many other tools. It has uncovered several thousand security vulnerabilities. A diagram of Z3’s symbolic analysis process is shown in Figure 110108.

![Figure 110 - Symbolic Analysis with Z3](image)

A list of symbolic analysis engines is shown in Figure 111109. On the right, a set of advances in symbolic solving in Z3 are listed. They correspond roughly to publications that describe the symbolic solving methods.
3. **Verifying the Cloud & Cloud Powered Verification**

We first put cloud scale verification in context of current Microsoft Azure networking. Microsoft operates one of the largest networks in the world, with 50+ Azure regions, 8,000+ ISP sessions, 180+ edge sites, 44 ExpressRoute locations, and 33,000 miles of lit fiber. A map of Microsoft’s network is shown in Figure 112110. There is a broad diversity of paths, with 2 per DC (metro), 3 per Region (terrestrial), and 3+ per Continent (subsea). This network is optically innovative with low-cost 100G QSPF optimized for metro networks. SDN control allows for intelligent traffic management and automatic failure recovery. Network verification is integral to Microsoft Azure’s network operation.
There are two perspectives on theorem proving and the cloud. The first, using theorem proving to improve networks, is illustrated in Figure 113, and the second, using networks to improve theorem proving, is illustrated in Figure 114.

The first perspective is illustrated by the methods to maintain the relationship between reality, intent, validation, and feedback that is shown in Figure 115. Another
example is analyzing Access Control List (ACL) policies for a data center, as shown in Figure 116114. Intent in Azure datacenters are mainly captured at an architecture level, thus it is possible to extract contracts for the correct behavior of a data-center network from databases that store the data-center designs. The contracts can be checked locally against the ACLs and routing tables on each router.

![Reality? Intent? Validation Feedback Diagram](image)

**Figure 115 - Intent = Reality?**

![Intra-datacenter traffic does not cross the T2 set. Intra-cluster traffic does not cross the T1 set.](image)

**Figure 116 - Scaling ACL & Reachability Checks with Local Contracts**

The second perspective is illustrated by use of parallel computation to enable solution of larger SAT/SMT problem, as illustrated in Figure 117115.
Figure 117 - Scaling SAT/SMT with Lookaheads
THIS PAGE INTENTIONALLY LEFT BLANK
VII. INSIDER THREATS

Insider threats are a problem common to all kinds of security systems. William Roof explained how a user’s personal information can be gathered from their social media and used by attackers to gain access to otherwise secure systems. Ryan Kelly gave a presentation on how to effectively counter insider threats with man-machine teaming. Sharon Runde explained other issues surrounding insider threats and recommended the use of runtime monitoring to mitigate these risks and vulnerabilities. This session was chaired by Shelley Gallup.

A. THE INSIDER THREAT PROBLEM

Presenter: Shelley Gallup, Naval Postgraduate School, Department of Information Sciences

1. Summary

The old adage “finding a needle in a haystack” does not quite fit the Insider Threat problem. Instead, it is more like “finding a needle in a needle stack.” The threat is often hidden and careful, the insider knowing all that is needed to be part of the “crowd.” It is a cumulative problem—layering of sufficient resources and data about an individual to find that part that is different, potentially consequential. This part has to be enough of a trigger that it gets the human and machine system to notice. Knowing in advance that there is a possible insider threat to the organization is in the category of “we don’t know what we don’t know.” And what is it that creates knowledge of a potential threat? If known, what happens next? Since March 2013 students and faculty of the Graduate School of Operations and Information Sciences (GSOIS) have wrestled with these questions and problems from multiple perspectives [53] [54] [55]. These include the use of crowd sourcing to prioritize the major issues, with the result that policy, data availability, data sharing, and technology head the list. Technically, the ability to match profiles to potential threats is feasible, but “tuning” the system to lower false positives is a must, and difficult for a number of reasons. From the themes provided in the crowd sourcing game, numerous projects have been the subject of thesis work outlined below.
2. **Summary of Previous Work**

An NPS thesis by Richard Mascolo investigated the question “Insider threat operations: Is collaboration a key factor?” Insider threats (InTh) are often unknown, inconspicuous, and hard to detect. To effectively manage this problem, big data must be shared, processed, and developed into threat indicators across multiple organizations and then managed by InTh hub operations. Barriers to data sharing and processing limit threat discovery, processing, and management required for highly effective collaboration. By determining enablers and barriers to data sharing and processing within InTh organizations and their contributory effects to InTh efficiency, a prototype solution can be designed to improve collaboration. Enabling collaboration internally at the hub and with other organizations is likely to improve the efficiency and provide a lower false-positive rate.

Recommendations included a common SharePoint portal, a risk factor number to establish a common baseline of both individual and team risk, a common approved software package, regular working groups, cross training initiatives, crowdsourcing aggregation, and lateral processes. All of these solutions have the potential to help establish a single networked strong/weak tie collaborative opportunity. The greatest difficulty here is not technical but bureaucratic, where seams of organizational data sharing produce legal and other restrictions. What is needed at this time is multiple datasets from organizations that would be expected to share data, for the purpose of technical and procedure testing.

Another NPS thesis by William Campbell on “System of Systems Approach to Insider Threats” examined insider threat detection and analysis processes and proposed an approach to enhance the hub analytical cell. Insider threat hubs rely heavily on internal sources of data such as user activity monitoring. This ignores additional external data sources of insider threat indicators. An ExtendSim simulation was created to show the effects of the inclusion of multiple nodes and to simulate hub operations based on Defense Security Service (DSS) and National Geospatial Intelligence Agency (NGA) insider threat hubs. Each simulation tested the processing rates of the hub analytical cell in order to demonstrate the relationship between throughput and false positive rates. Alerts were processed based on highest priority (first-in-first-out basis), the source of the
alert, and the Unique Identifier associating the alert with a specific user. The major finding of this thesis is that a process of identifying insider threat indicators with only User Activity Monitoring (UAM) ignores external sources of data and technology and contributes to a gridlock of priority 1 and 2 alerts, while ignoring priorities 3 and 4. It is possible that knowing this, potential threats would seek to be in priority 3 or 4, thereby “spoofing” the system.

A third NPS thesis by Jay Sellen addressed insider threat data sharing. Insider threat is a significant problem for both governmental and private organizations. Individuals can do immense harm with their trusted accesses. To combat this threat, organizations have created departments with trained analysts whose sole purpose is to deter, detect, and mitigate the insider threat. These analysts monitor employees and analyze activities to detect dangerous practices, whether witting or unwitting, and report these actions to supervisors for mitigation. When organizations share insider threat information with other organizations, it can improve their abilities to deter, detect, and mitigate the insider threat. The challenge lies in merging external and existing data with as little human interaction as possible. This thesis examined the work that takes place in an insider threat department and identified requirements for a solution that would allow for information sharing between organizations, as illustrated in Figure 118116.

![Figure 118 – Requirements for Data Sharing](image)

133
3. **Recommendations**

Recommendations from this project emerged in the following:

1) *Work through policy issues enabling shared data across an enterprise.* As noted above, there are many similarities to the theses that were completed, with data sharing as the number one need. There are many challenges here. Legal, HIPPA (federal and state health information laws), financial disclosures, and financial health are just a few. Also, the most recent efforts seem aimed at only participants with security clearances. Both unclassified and classified domains may reveal behaviors that have correlation with willful or unintended actions. The lack of cross-domain sharing of data is just another layer that creates difficulty in aggregating information for analysis.

2) *Bring machine learning into the stream of data, and across domains.* Learning systems must be employed as the amount of data is simply too much for available analysts to process manually. This would likely be a human-machine team at the outset, followed by increasing reliance on increasingly subtle correlations.

3) *Organize in ways that enhance the analyst’s ability to move an indication forward.* Organizationally it is not clear what the path is for analysts to move indicators forward to higher and higher levels of concern. In this research effort several organization schemes were offered, however none were tested by the hub. This was at least partly because the concept of a “hub” continues to evolve and is not yet clear.

**B. PERSONAL INTELLIGENCE (PERSINT)**


1. **Summary**

   Personal intelligence, or PERSINT, offers a wealth of personal information to Cyber attackers for use in “getting inside” networks and computer systems. Users can reduce the instances of PERSINT-driven insider Cyber threats by removing all personal references from the system access process. Administrators must understand what users post on the Internet and develop training to counter the “you are your own insider” threat.

2. **Background**

   The goal of this presentation was to begin a dialog concerning the intelligence collection threat posed by Cyber criminals with unfiltered access to personal information. Although personal information is available in many forms, across many venues, this presentation focused on information available on various social media and genealogy Internet sites.
NATO defines HUMINT as "a category of intelligence derived from information collected and provided by human sources." Critical intelligence information provided by humans may be either with or without their knowledge, and with or without their understanding of the potential consequences.

Personal Intelligence (PERSINT) is generated by people who willingly share personal information, with little or no understanding or concern for the potential consequences. It includes analysis of personal information, knowingly or unknowingly shared by people about themselves, their families, their friends and their co-workers. PERSINT-exploitable Internet portals may include social media, chat rooms, genealogy sites, dating sites, political blogs and other venues where people provide personal information, at all levels, to an unknown and potentially hostile audience. As society moves forward in using facial and voice recognition, we can expect computer applications and Internet sites that capture facial images and voice recordings to provide a fertile PERSINT hunting ground.

3. Examples of PERSINT in Advanced Persistent Cyber Threats

Advanced persistent threats (APTs) often show characteristics of military field operations, especially when compared to other types of Cyber threats. APTs require team planning and are organized into five phases. Phase One is reconnaissance, where attackers seek to understand and develop a target. Phase Two is incursion, where attackers gain entry into a system to deliver a Cyber payload. This step is where PERSINT is most damaging. Phase Three is discovery, where attackers patiently identify the target’s strengths and weaknesses from the inside. Phase Four is capture, where attackers manipulate discovered weaknesses to access targeted information. Phase Five is exfiltration. In this phase, attackers retrieve, analyze, and exploit captured information.

During the incursion phase systems are highly susceptible to insider Cyber threats that may attempt to gain access by posing as trusted users. Attackers often target user passwords to mask the appearance of intrusion attempts. When chosen by users, passwords often reflect personal information such as friends, family, and pet names, as well as birthdates, personal events, etc. Much of this information, in bits and pieces, is available from users’ social media, blog, dating, and genealogy posts. Gathering information from social media, Cyber attackers assemble the PERSINT puzzle by
employing sophisticated algorithms or brute-force approaches to gain access to the network, its backbone, and the data it should protect.

Five examples of readily available personal information examined in this presentation are Facebook, Instagram, Tumblr, Reddit, and Ancestry.com.

1) Facebook is a social networking website where users can post comments, share photographs and post links to news or other interesting content on the web, chat live, and watch short-form video. A sample of the personal information available on Facebook is shown in Figure 119.

![Facebook Screen Shot](image)

**Figure 119 – Facebook**

![Facebook Screen Shot](image)

2) Instagram is a photo and video-sharing social networking service owned by Facebook, Inc. Examples of personal information available on Instagram are shown in Figure 120.

![Instagram Screen Shot](image)
3) Tumblr is a microblogging and social networking website, parented by Verizon/AOL/Yahoo, which allows users to post multimedia and other content to a short-form blog. An analysis of a Tumblr profile is shown in Figure 121.

- Pet’s Name
- Pet’s DoB is 8 years prior to post date
- People who like the post (with photo thumbnails)
- Additional comments about pet’s birthday and relationship with owner

Figure 120 – Instagram

- Clear political leanings and posting of common political slogans
- Follows and comments on media reports

Figure 121 – Tumblr
4) Reddit is massive collection of forums where people can share news and content, or comment on other members’ posts. It is a subsidiary of Advance Communications/Condé Nast. An example Reddit post is shown in Figure 122120.

Figure 122 – Reddit

5) Ancestry.com LLC is the largest for-profit genealogy company in the world, operating a network of genealogical, historical record and genetic genealogy websites. A screenshot of an Ancestry.com family tree is shown in Figure 123121.

Figure 123 – Ancestry.com
By gathering PERSINT from these platforms, an attacker can generate a list of potential passwords and answers to security questions in order to gain access to a system. A diagram of this process is shown in Figure 124.

![Diagram of PERSINT Puzzle Pieces]

**Figure 124 - PERSINT Puzzle Pieces**

4. **Recommendations**

In order to counter PERSINT collection through online platforms the presenter recommended that administrators establish multi-step, multi-biological, or hybrid system access logins to counter the availability of answers to “secret questions” on social media. These counter-measures include password/numeric code combinations, a combination of fingerprint and facial recognition, a fingerprint and iris scan combination, or some other two-factor authentication. He also suggested assigning randomly generated strong passwords to users (16 characters or greater) rather than allowing user to create their own passwords. Additionally, administrators should require users to memorize their passwords or store passwords in an encrypted password app on their mobile devices. No sticky notes, physical documents, or un-encrypted password files should be allowed.

C. **INSIDER THREAT ANALYSIS**

Presenter: Ryan Kelly, US Army

1. **Summary**

When attempting to analyze insider threats, overcoming the problem of information overload is key. Computers are not as good at solving this problem; although
they can analyze vast amounts of data they are less adept at taking context into account than humans. The project found that insider threat analysts organized in a team were marginally more accurate than those organized as individuals [56]. This project also tested a trustworthiness construct in order to reduce false positives in computational risk ratings. This project recommends that risk be perceived two-dimensionally in terms of trustworthiness and distrust factors, and that self-equity factors be leveraged to mitigate false positive in computational risk ratings.

2. Introduction

Information overload is a common problem when attempting to analyze insider threats. Programming a computer to do the job might seem like an obvious solution, but while computers can better handle large amounts of data they are currently incapable of continuously adapting to contextual changes like human analysts due to variations in contextual relevance.

Additionally, there is the induction problem. Pedro Domingos framed the induction problem in his 2015 book “The Master Algorithm” with the question “How can we ever be justified in generalizing from what we’ve seen to what we haven’t?” [57, p. 58]. David Hume also stated that, “it is impossible to discover causes and effects for any new observation, and any supposition thereon is completely arbitrary” [58, p. 17]. Therefore, humans must perform insider threat analysis, but there are known limitations to human information processing capacity [59].

Given than information overload occurs every time information processing demand is greater than capacity [60], the problem this project sought to solve is that insider threat analysts must overcome information overload to keep up with insider threats [61]. The project also sought to determine the best way to reduce information overload based on informational and temporal constraints. Several theories used to combat information overload are shown in Figure 125123 [62] [63] [64] [65] [60] [66] [67].
3. **Laboratory Experimentation**

The project conducted experiments to assess effects of teamwork and completeness of relevant information on the accuracy of insider threat assessments. Experiment stimulus scenarios from the National Insider Threat Task Force training course (2 exonerate, 2 implicate) were organized in an online environment. The “Adjudicative Guidelines for Access to Classified Information” (32 U.S.C. 147) informed the insider threat analysis. Participants all had top secret clearance, were trained in insider threat, were at a minimum bachelor’s degree educated, and were at GS-12 or equivalent pay grade. They were also incentivized with a one ounce “American Eagle” silver coin to make the work realistic as possible. An example scenario is shown in Figure 126124.

A diagram of the experiment design is shown in Figure 127125. Ignorance is defined as the lack of relevant information that can affect how insider threat analysts make attributions for anomalous behavior.

---

**Figure 125 - Theories to Combat Information Overload**

**Classic organization theory:** Distribute the information among more people to better accommodate the load.

Specialization theory (Daft, 2012; Thompson, 1967) *vs.*

Process loss theory (Staats, 2012; Steiner, 1972)

**Cognitive load theory:** Reduce the information.

Information overload theory (Schick et al., 1990; Sweller, 1988) *vs.*

Ignorance theory (Denby & Gammack, 1999; Holtzman, 1988)

---

**Figure 126 - Test Scenario 2**

---

Figure 127 - Experiment Design
4. Findings

This project found that analysts organized in a team were marginally more accurate than those organized as individuals. Specialized teamwork significantly increases the time of ITA compared to participants’ individual work, and ignorance and teamwork interact with perception of information overload. Participants were little better than random chance on exoneration outcomes. Details of the findings are shown in Figure 128126.
While machine learning models are good at detecting insider threats, they also suffer from low base rates which leads to a problem of false positives. Learning machines predict future deviant behavior from past deviant behavior. Because insider threats generally have criminal history, it does not necessarily mean that those with criminal history are likely to become insider threats. To assume it does is example of a logical fallacy called affirming the consequent (if P then Q. Q then P). Additionally, it does not necessarily mean that those with no criminal history will not become insider threats. To
assume they will not is an example of a logical fallacy called denying the antecedent (if P then Q, not P then not Q). This, in essence, is a classic optimization problem: How does one best reduce false positives while minimally increasing false negatives?

D. PROBLEMS FROM INSIDER THREATS

Presenter: Sharon Runde, Naval Postgraduate School, Information Sciences Department

1. Summary

This project found that cracking down on threats because of ‘one bad apple’ causes adverse effects for the majority of loyal employees. Cyber hygiene and S/W & H/W vulnerabilities were identified as issues, as well as complex networks and the fact that system security is a moving target. This project recommends the use of runtime monitoring systems for mitigating identified threats and vulnerabilities, as well as further research into better prediction methods.

2. Background

When designing a system to deal with insider threats the designer must determine who the humans involved are and what their relationships are. Example: LT Schmuckerby.

There are two types of errors, Type I and Type II. These are shown in Figure 129.

<table>
<thead>
<tr>
<th>I don’t see anything</th>
<th>Nothing is there (H0 is True)</th>
<th>Something is there (H0 is False)</th>
</tr>
</thead>
<tbody>
<tr>
<td>I see something</td>
<td>Wrong (Type I error)</td>
<td>Right!</td>
</tr>
<tr>
<td></td>
<td>Wrong (Type II error)</td>
<td></td>
</tr>
</tbody>
</table>

Figure 129 - Types of Errors

These categories were illustrated using examples on supply chain risks as follows. In the first case there are no anomalies detected and no supply chain attack has occurred. This is obviously the best case. In the second case there are no anomalies detected and a supply chain attack has occurred. This is a Type II false negative and can be either malicious or accidental. In the third case there are anomalies detected but no supply chain attack has occurred. This is a Type I false positive, and is accidental. In the fourth case
there are anomalies detected and a supply chain attack has occurred. Designers should focus on the second and fourth cases (IV.A.4).

- Methods to prevent insider threats include:
  - Physical security
  - System logins
  - Access restrictions
  - Data flow control
  - Background checks
  - Reporting activity
  - Monitoring activity [53] [54] [55]

Methods to deter insider threats are:

- Security policies
- Training
- Consequences
- Threat of detection

In order to know that an insider threat has materialized, a designer must answer the following questions:

- When do you know?
  - 5 ways of knowing: Agreement, The world as a formula, Multiple Realities, Conflict, Unbounded Systems Thinking [68]

- How do you know you know?
  - Gaining empirical evidence
  - Analyzing risk exposure (including risk exposure, impacts, mitigation strategies)
  - Can AI help us profile users and identify anomalies?
  - How can AI help us detect and predict new threats, to include group activity?

3. **Solutions and Future Work**

Runtime monitoring can perform real-time analysis, but that may already be too late to prevent insider attacks. In order to increase the probability of detection, psychological theories such as General Deterrence Theory, Social Bond Theory, Theory of Planned Behavior, and Situational Crime Prevention should be leveraged.
Further research should explore:

- Detecting Malicious Insiders in Military Networks
- Monitoring Technologies for Mitigating Insider Threats
- Insider Threat Prediction Tools: Evaluating the Probability of IT Misuse
- Insider Threat Control: Using a SIEM Signature to Detect Potential Precursors to IT Sabotage

It should also explore the epistemological question of how developers design an information system to know anything. Is the human in the loop or on the loop?
A. INTRODUCTION

The panel sought to define what Cyber education should be, not exclusively as a discipline but in terms of what every junior officer should know. The United States Naval Academy (USNA) graduates 1050 Midshipmen annually into the Navy and Marine Corps. They all must be prepared to lead in a complex cyber-enabled warfighting battlespace. The goal was to establish a baseline of Cybersecurity training and education for all 4,500 USNA midshipmen, in other words, an “all-many-few” approach to Cyber education.

Currently, the majority of USNA incoming students have little to no understanding of Cybersecurity, the functioning of the internet, programming/coding, or the interdisciplinary nature of Cybersecurity. The panel recommended that:

1) Cybersecurity fundamentals be taught to all students.
2) Cybersecurity be infused to the largest extent possible across all academic fields.
3) Opportunities for studies and experience in the Cyber domain be increased.

These recommendations anticipated those laid out in the White House’s Executive Order on America’s Cybersecurity Workforce dated May 2, 2019, which is duplicated in full in Appendix A. The challenge from the Navy is to standardize Cyber education.

Another question the panel sought to answer was how to define cybersecurity in an academic setting. Initially, USNA sought ways to align it with standards established by the Accreditation Boards for Engineering and Technology (ABET), however, none existed at the time (pre-2017). A collaborative study was done along with other ABET accredited schools to define criteria for cybersecurity academic accreditation. Wordle favored defining cybersecurity in the business area, while USNA created an entirely new department, the Cyber Science Department, to specifically manage USNA primary efforts in the classroom as related to Cyber education. The Cybersecurity BA degree at UT San Antonio is housed in the College of Business.

ABET New Cybersecurity Fundamental Topics are as follows:
• Data Security: protection of data at rest and in transit.
• Software Security: development & use of software that reliably preserves security properties of information and systems.
• System Security: establishing & maintaining security properties of systems, including those of interconnected components.
• Human Security: protecting individual’s personal data and privacy; threat mitigation combined with the study of human behavior as it relates to cybersecurity.
• Organizational Security: protecting organization from cybersecurity threats & managing risk to support successful accomplishment of the organizations’ missions.
• Societal Security: aspects of cybersecurity that can broadly impact society as a whole for better or for worse.

DoD Objectives for Cyberspace are as follows:
1) Ensuring the Joint Force can achieve its missions in a contested cyberspace domain;
2) Enhancing Joint Force military advantages through the integration of Cyber capabilities into planning and operations;
3) Deterring, pre-empting, or defeating malicious Cyber activity targeting US critical infrastructure that is likely to cause a significant Cyber incident;
4) Securing DoD information and systems, including on non-DoD-owned networks, against Cyber espionage and malicious Cyber activity;
5) Expanding DoD Cyber cooperation with allies, partners, and private sector entities.

In order to cultivate talent, educational institutions and stakeholders should:
• Embed software and hardware expertise as a core competency:
  o Establish a career track for computer science related specialties (including hardware engineers, software developers, and data analysts) that offers meaningful challenges, rotational billets at other Federal departments and agencies, specialized training opportunities tied to retention commitments, and the expansion of compensation incentives for the Cyber Excepted Service (CES).
• Establish a Cyber top talent management program:
  o Provide most skilled Cyber personnel with focused resources and opportunities to develop key skills over the course of their careers.
  o Use competitive processes, including individual and team competitions, to identify the most capable DoD military and civilian Cyber specialists and
then empower those personnel to solve the Department’s toughest challenges.

- Create a Cyber ready workforce:
  - Invest in building future talent, identifying and recruiting sought-after talent, and retaining current Cyber workforce.
  - Provide ample opportunities for professional development and career progression of Cyber personnel.
  - Ensure that Cyber requirements are filled by the optimal mix of military service members, civilian employees, and contracted support to serve mission requirements.

- Enhance the Nation’s Cyber talent:
  - DoD play essential role in enhancing the Nation’s pool of Cyber talent in order to further the goal of increasing national resilience.
  - Increase efforts to promote science, technology, engineering, mathematics, and foreign language (STEM-L) disciplines at the primary and secondary education levels throughout the US.
  - Partner with industry and academia to establish standards in training, education, and awareness that will facilitate the growth of Cyber talent.

USNA strategic challenges include:

- Educating all of our students on the importance of cybersecurity and the Cyber domain as a warfighting area.
- Developing cyber-related course(s) of study.
- Creating a viable path for accessions of junior officers into the Information Warfare Community.

It should be noted that “Wordle” is a free on-line tool that displays representations of words based on a word count in a “word cloud”. This is helpful in visualizing the relationship between concepts, and can allow for more accurate categorization, such as the connection between Cybersecurity and business school.
B. DISCUSSION

- How do you define cybersecurity?
- How do you bound cybersecurity?
- What do you include in a cybersecurity education curriculum?
- What are some ideas for content?
- Where does cybersecurity fit?
- Who owns it, or should anyone own it?

1. NPS Panelist 1

Duane Davis: NPS is unique among institutions, our students come from a wide variety of undergrad programs and our purpose is to give them technical skills that they can take back to the fleet and apply critically in operational environments.

We have specialized departments (Computer Science and Electrical and Computer Engineering) that provide deep technical Cyber programs. The Cyber Academic Group (CAG) focuses on operational Cyber billets that require technical expertise. Cyberspace operations is inherently multidisciplinary. Our program has Educational Skill Requirements (ESR) defined by the sponsors (OPNAV N2/N6 and FCC). The ESRs are a laundry list of broad, operationally focused technical and policy topics. All students in the cyberspace operations curriculum complete a set of core courses drawn from CS, ECE, and IS. Upon completion of the core, students choose a specialization track to focus on a specific aspect of cyberspace operations: engineering, computation, or systems and operations.

Our curriculum is focused on operations (offensive, defensive, adversarial, etc.). A student needs not only a technical background but an operational perspective as well. We have Cyber policy and planning courses to get the students thinking not just from a technical standpoint but also considering questions such as what is the right thing to do within our authorities and how can we leverage friendly Cyber capabilities to prevent an adversary from achieving their objectives over ours?

Challenges include students drawn from information warfare community that have non-traditional or non-technical undergraduate degrees. These students are often more suited for specific tracks in the cyberspace operations program. Students in the engineering track, for instance have to meet specific requirements to qualify for electrical
engineering degree (due to ABET requirements). Students not meeting those requirements may take the computation track (administered by CS), but may still have difficulty meeting certain requirements if they are not prepared technically or mathematically. Students in all three tracks must be brought up to speed very quickly. Thesis topic selection can also be difficult for students with less technical backgrounds who often don’t understand the domain or field well upon program entry. This is a situation that NPS has a great deal of experience with, however, and overall NPS does an excellent job at taking students that don’t have a background, getting them up to speed, and turning them into Cyber operators by the time they graduate.
USNA Panelist

Tracy Emerson: Freshmen start with an introduction to cybersecurity. These students don’t know anything about computers or cyber. They may be adept at operating their phone but not more than that. The challenge facing instructors is how to educate beyond that.

USNA developed a re-vamped introductory course. Previously, it was taught in a linear way. This caused problems with retention of information. Now it is more circularly taught, is interdisciplinary, and is taught with an eye towards the adversary.

Students need to understand the basic concept of computers and cyber. They are also introduced to ideas such as policy, laws, ethics, human factors, social engineering, and how it plays into cyberspace. This helps define Cyber as a discipline.

As the semester moves along, they build on baseline topics. Things like what is a program? Not necessarily the ability to be a programmer, but an understanding of a program and its vulnerabilities. They need to understand why it is important.

Finally, in a virtual environment the students can do reconnaissance in a UNIX and API environment. They also do an attack lab to familiarize themselves with the perspective of a hacker. They then take lessons learned and use them defend the network, and harden the network by the end of 14 weeks. Again, the idea is basic familiarity so that students can understand why it is important.

Students then do a case study and make a presentation and paper on something relevant in Cyber related to class topics. The overarching goal is to help students understand why Cyber is important. The transformation in the students is amazing.

In their junior year they take a subsequent class from ECE. They focus on electromagnetic spectrum and how Cyber ties into it. This class builds on fundamental lessons from their freshman year.

Some students select Cyber operations as their major. It is the fastest growing department (around 10% each year). In one year, the Cyber and CS departments took in 110 and 70 new students, respectively. The Cyber department is attractive to students who are keen towards technical disciplines as well as drawn to humanitarian social sciences because it is interdisciplinary. These students understand that Cyber is important and they will tell you that’s why they choose the degree. They get a strong technical
underpinning in key traditional CS classes such as data structures, Python, C, SQL, JS, and others as required. Part of the core matrix includes Cyber physical systems to learn where the vulnerabilities are located and to include SCADA. They also take system architecture classes as well as courses on networking and wireless systems, which are taught from a Cyber perspective. The labs and instruction always look towards an adversarial perspective, as opposed to a CS student who does not necessarily focus in class on an adversary. The CS department and the Cyber department take a different approach to teaching the concepts.

The students in the Cyber department also get some of the softer science topics such as policy, law, and ethics as well as human factors and social engineering. This distinguishes the approach taken by the USNA. Even technical students appreciate that understanding the battlespace requires a holistic assessment that includes the softer sciences.

In their senior year they have a semester of offensive operations in a virtual network to learn to use and manipulate tools so they can learn to defend well. They take two electives – anything from reverse engineering and digital forensics to a Cyber economics class. How does economics play into cyber?
3. **NPS Panelist 2**

Sharon Runde: NPS was asked to create a Cyber 101 course that All-Hands Navy would take. We wanted to put together a course that will give every student a fundamental, baseline understanding of what Cyber is.

We started with 17 people teaching the “All-Hands” course. The key topic areas were laid out to create a “Cyber turn of mind.” We aren’t analog or even digital anymore.

Learning objectives were defined and refined to align with NWC, NPS, and USNA. As our organizations are all part of the Navy, we wanted to make sure that we are all focusing on the same areas of interest and concern. One challenge was how to organize such a course. Options included:

1) Covering core topics and then branching out.

2) A fish-bone organization (this becomes extremely labor intensive for administration).

3) A true all-hands approach with few opt-outs.

Another challenge is fitting this new mandatory course into an already full curricula. Right now it is an elective, but there will eventually be a directive from OPNAV and N2/N6 making it mandatory.

The most important thing we want to accomplish is ensuring every student that walks out of NPS understands what Cyber is and how it impacts their job, as well as their counterparts’ jobs. We also have a strong focus on each topic area being operationally relevant.

A lesson learned from the pilot is class control to keep certain students from taking over the sessions. At the beginning we also started teaching the course very linearly but learned that all the topic areas need to be woven together.
4. Audience Comments/Questions/Discussion

An audience member stated that only 2-4 out of 20 freshman knew anything about Cyber other than their phone, and that there is a program called Cyber Patriot which last year had 6000 teams from across the US enter. The Academies have criteria that determine which plebes are nominated. Perhaps one of those criteria should be participation in a team.

The panel pointed out that it may be possible to find a great hacker that isn’t on any kind of team – maybe we “blue chip” a hacker. We may not be reaching recruitable individuals. Ideally we would reach them around 16-17 years old and ask them if they have heard of cyber. The UK did a survey found that girls were turned off by Cyber by the age of 13-14 because no-one encouraged them to keep coding or being involved.

A comment regarding the intro class was that his class is online and the intro is one that the students get without competition between technically and non-technically savvy people. Students completed the content on-line and then came together face-to-face.

Another audience member completely agreed with the change to focus on Cyber. The goal has been to produce officers to fight the war. Slide rules can’t be the norm anymore. The battlefield now includes cyberspace. While we still need people on the ground, the physical space is only part of it. To fight the Cyber war we need the education in the academies.

The panel responded by stating that West Point is also now accepting 30 students into a new Cyber Military Occupational Specialty, who will progress faster since they have their own MOS. West Point has a typical URL restriction. Of everyone that did a direct accession, 20 of the top 350 students were accepted. These students came from CS, ECE, Physics, Math, etc. These backgrounds directly relate to the likelihood of being successful in the cryptologic and Cyber battlespace. The flexibility of establishing a Cyber department has afforded them the opportunity to offer more to students. USNA, on the other hand, is incredibly demanding and they are limited in what they can do, but what they still want is to imbue students with a lot of things such as Cyber psychology – if there’s a bad guy, why is the adversary doing what they’re doing? Sometimes it’s obvious, but many times you can’t tell why adversaries do what they do. It will change
the way students think about what they are operationally doing in this Cyber space. 50 out of 1050 is still a small fraction of student becoming Cyber experts. We now have ‘flying vulnerabilities’ because everything is networked.

An audience member then pointed out that nuclear students have to understand how every piece of the ship works before they get their “dolphins”. Due to the increasing incorporation of Cyber systems and concepts in all aspects of the Navy, it makes sense to move Cyber to the forefront of all students’ education, or it will master you before you master it.

The panel stated that Cyber hygiene was a key tenet, and that teaching these life lessons is really critical. The goal is that everyone in the Navy should have a fundamental understanding of Cyber hygiene, but what else is needed? The problem space will keep growing because everyone else also has the same fundamental understanding. Students need to understand that even they can be an unwitting adversary.

Another audience member mentioned professional certification tracks. These bring not just the content, but get students to look at getting certifications. For example, CISSP forces the student to think beyond the box.

The panel said that outsiders have said they could take the CISSP exam at the end of the USNA classes. The Navy currently doesn’t pay for certifications, but they have thought about it. One difficulty facing educators is how to keep up and keep content fresh without having to change an entire curriculum? Staying current in this field is very challenging. The difference between “education” and “training” is important here as well. Professional certifications are great, but they focus on current systems and requirements and become obsolete over time. Done correctly, education develops critical thinking skills that remain relevant even as technologies, tactics, and adversaries evolve.

At NPS, the courses are current because our curriculum is taught at the TS/SCI level and we interact with our sponsors to see what they are concerned about so that those in-time concerns can be addressed in the classroom. Also, since we do research, the faculty is on the leading edge of the Cyber domain. The curriculum is also informed and driven by their research and is implicitly kept up to date.

One audience member found it interesting that Cyber is interdisciplinary and both courses described were ‘survey-ish’ in nature and were done before the students were
grounded in their disciplines. The member asked if there were any consequences of doing that, any observations, and what could the students get out of it if the courses were taken early in their matrix?

The panel stated that NPS has gone back and forth, and that there is no definitive answer. On one side, the course is broad and doesn’t go deep and gives an overview of what to expect later. On the other side, if the students have some cyber/computer classes first then they will have an appreciation for the material. It may not matter when they take the class, but if taken early they move together as a cohort. Since the course is intended for “all hands” and supports curricula that may have no other Cyber content, its placement in some matrices is largely arbitrary.

For USNA, the midshipmen take 90 credits as core, while the plebe course is extra. The course fit best in their freshman year. Some people don’t believe Cyber is interdisciplinary which politically makes it difficult to implement, but offering the class early gives them the opportunity to take something rooted in logic, even if it isn’t very technical. It has benefited midshipmen because they transition into their classes having had the opportunity to have logical, technical thinking. If other states follow Mississippi’s example and increase STEM at the high school level, USNA’s curriculum can be adjusted accordingly.

An audience member pointed out that we don’t need a bunch of programmers. What USNA and NPS have in common is that we are training officers. Dr. Hamming said we are training officers and then we are training scholars. Having the Hopper Hall, USNA’s new Cyber building is a wonderful thing.

The panel noted that the Hopper Hall will have classified spaces and the entire Cyber department as well as seven majors will be co-located in the building. It would be great to have a SCADA lab but the panel is not sure if that is feasible yet. Currently, everything is scattered across campus in different buildings. Having everything in one building will encourage collaboration among different departments. We have an invitation to visit the new building, and the USNA is trying to push more project based learning.

Finally, an audience member asked how attendees of the Workshop could help the general population learn more about computer science. CS has changed and evolved over
time. Berkeley also has a college that teaches CS. Should educators plan to integrate new objectives for cyberspace into the curriculum?

The panel stated that in order to cultivate talent, we should draw from the larger national policy expressed in the Executive Order duplicated in Appendix A.
IX. CONCLUSION

We are convinced an urgent national need exists to provide Cyber systems/secure software-intensive systems that operate dependably in today’s contested computing environments. Given the state of industry, there are obvious challenges to fully secure functioning Cyber systems. These challenges include the development of a standardized and relevant Cyber curriculum as well as a deeper understanding of how emerging AI and machine learning techniques can be leveraged to weaken or strengthen a Cyber system. Cyber researchers and developers are making progress on solving various aspects of the problem, but much remains to be done.

A. SUMMARY

The 20th Monterey Workshop on Cyber was held at the Naval Postgraduate School in Monterey, CA, on Nov. 27-29, 2018. The NPS Provost, Cyber Academic Group Chair and Dean of Research co-chaired the workshop and led the program committee with members from all NPS schools and departments. The program consisted of five unclassified sessions, two panels, and one classified session. The presentations addressed Cyber problems associated with unmanned/autonomous vehicles, Cyber challenges of Naval Operations, Cyber fundamentals, AI/machine learning, insider threats and command and control. The workshop program in section I.C has details. Following traditions of past Monterey Workshops, participants from universities, industry and government were present and worked together to achieve consensus on how to best satisfy urgent national needs.

The first of the two workshop panels discussed establishment of the Monterey Cyber Institute. In the second panel on Cyber Education, panelists and attendees exchanged curriculum related concepts and shared teaching experiences from Cyber education programs at the Naval Postgraduate School, the U.S. Naval Academy, and the University of Texas at San Antonio. These institutions host some of the largest Cyber education programs in the country, with more than 4,500 students.

The workshop concluded Cyber education will benefit from a unified vision and standardization. Institutions have different, sometimes conflicting views of what kind of preparation Cyber professionals need. These differences have to be reconciled, aligned
with the needs of the Cyber community, and implemented at educational institutions. There are accreditation bodies currently addressing these issues, but it is likely to take time for this process to converge on a community consensus. These recommendations were later re-affirmed by a recent Executive Order, reproduced in Appendix A. Additionally, the panel determined Cyber professionals need both theoretical understanding and hands-on experience with Cyber operations and related tools. Simulated Cyber environments also have a critically important role in Cyber education and training.

The workshop recognized current and potential contributions of AI and machine learning to Cyber operations. These include both defensive applications, such as early intrusion detection, and offensive, such as automated harvesting of information leaked through network traffic. Cyber test facilities were described, including some that already have massive and growing datasets available, particularly with respect to autonomous vehicles. These datasets aim to support new applications of machine learning that integrate both Cyber and physical systems. Availability of data is an enabling factor for progress, since ample storage and processing capabilities of the type needed for applying machine learning are readily available [90].

A great deal of discussion occurred relating to verifying the accuracy and security of decision aids and autonomous subsystems. Multiple approaches were presented, see Chapter II for details. It was pointed out that due to the low cost of entry, Cyber threats related to autonomous vehicles are rapidly evolving and that counter-measures must evolve rapidly to keep up. This puts a premium on balancing risks – delay in deploying solutions may introduce as much risk exposure as deploying imperfect solutions rapidly. Another theme that emerged was how to mitigate risk posed by insider threats without alienating the loyal and conscientious majority of the Cyber workforce via intrusive surveillance.

As illustrated by the recent renaming of the Space and Naval Warfare Systems Command's Systems Centers (SSC-Pacific and SSC-Atlantic) to Naval Information Warfare Centers (NIWC-Pacific and NIWC-Atlantic), the proliferation of Cyber systems through all aspects of the military has propelled Cyber issues to the highest research priorities, as well solidifying their place in modern C4I - Command, Control,
Communications, Computers & Intelligence. In order to ensure the Navy’s continued dominance of the world’s oceans, researchers must help the Navy identify, develop, deliver, and sustain information warfighting capabilities to ensure freedom of action across all warfighting domains in, through, and from cyberspace, and to deny the same to the Navy’s adversaries. This is dependent on the provision of Cyber systems that can operate dependably in contested environments. The Defense Information Systems Agency is addressing one aspect of this by developing capabilities for continuous assurance of user identity on mobile devices by monitoring multi-factor biometrics [91].

B. FUTURE WORK

Secure communications are of vital importance in all aspects of life, and especially so in a military context. During World War II, computer scientist Alan Turing devised a number of techniques for speeding the breaking of German ciphers, including improvements to the pre-war Polish bombe method, an electromechanical machine that could find settings for the Enigma machine [69]. It has been estimated that this contribution shortened the war by two years and saved 14 million lives [70] [71]. Now network communication is a critical part of the infrastructure supporting our economy, our daily lives, and national security. Diverse communication infrastructure – cabled, wireless and optical – has been deployed from the sea floor to the land, air and space [72] [73]. Personal communication, commercial coordination, and internet of things depend on it, as well as military C4I and undersea communications [74]. Communications are a key aspect of tomorrow’s technology-led battlefields, as recognized in the recent Executive Orders issued by the White House on May 2 and 15, 2019 [75] [76]. These are reproduced in Appendices A and B, respectively.

In these Executive Orders, the President unequivocally made cybersecurity his priority. The Executive Order dated May 15, 2019 was titled Securing the Information and Communications Technology and Services Supply Chain. This order called for increased vigilance with regard to the potential of foreign adversary contamination of the information and communication technology supply chain. While this order does not directly relate to NPS or USNA programs, it does increase the demand for Cyber savvy personnel. This demand is reinforced and partially addressed by the Executive Order dated May 2, 2019.
This Executive Order was titled *America’s Cybersecurity Workforce*, and provided a mandate for USNA and NPS products and services. The Order acknowledges America’s Cybersecurity Workforce as a crucial element in preserving peace and continuing prosperity, saying, “America’s cybersecurity workforce is a strategic asset that protects the American people, the homeland, and the American way of life.” The Order also acknowledged that the Cyber workforce is not where it needs to be. The President required the development of an annual cybersecurity competition to be held between all Federal cybersecurity employees, as well as an annual Presidential Cybersecurity Education Award to recognize the best elementary and secondary school educators. Educational institutions not affiliated with the Federal government should mirror these efforts to enhance the nation’s cybersecurity workforce. In addition to increasing workforce mobility and incentivizing top performers, the Order called for improving access to training and increasing innovation. The Monterey Workshop discussed precisely these topics.

Communication has always been vulnerable, historically to jamming and interception, and now to many other disruptions, including Cyber effects. Current communication modes need better protection, and we need to address emerging new options for networked communications, such as 5G wireless, software-defined radios, software-defined networking, quantum technologies, and others yet to be developed, such as adaptive short-wave radio for over-the-horizon wireless networking. Making our networked communications reliable, robust and secure is one of the most important goals for the Cyber community as new capabilities spread and introduce new vulnerabilities in information and communication technology and services. This is a necessary step in carrying out the third offset strategy for national security, whose goal is to make humans more effective in combat [89].

As stated by former Secretary of Defense Jim Mattis, “It is now undeniable that the homeland is no longer a sanctuary” [77]. The increasing cyber-connectedness of the modern world has enabled adversaries to target the confidence and social cohesion of a population and its political processes without ever physically crossing its borders [78]. This new threat vector makes cybersecurity vital to safeguarding not just the nation’s
military and industrial infrastructure and processes, but also the very core of our society [79].

Data science is a “multi-disciplinary field that uses scientific methods, algorithms and systems to extract knowledge and insights for structured and unstructured data” [92]. Current trends are to process large amounts of data to derive statistical conclusions for use in decision making. However, commercial use of the term “Artificial Intelligence” for this activity may be dangerously misleading, because current popular applications of machine learning are not intelligent in the human sense [80]. They are not aware of risks associated with outcomes of their decisions, and operate by seeking to minimize the error rate without distinguishing between trivial errors and those with catastrophic consequences. They also do not consider whether or not derived statistical correlations correspond to cause-effect relationships and whether or not they would be reliable guides for planning future actions. The inclusion of human operators in the decision-making loop will thus be necessary in the near to mid-term, and further improvements in use of man-machine teaming to reduce residual risks of using machine learning should be pursued.

The success of Cyber operations depends on high-quality software that must be agile and intelligent, with intelligence instilled in the software. Well-engineered software is also needed for software-defined radios that adaptively choose frequencies to circumvent environmental factors with jamming attempts, software-defined networks that dynamically and programmatically alter their configurations in order to monitor networks and improve their performance [19], communications technology and services [81], control systems for satellites, medical devices [82], or weapons systems [83], and many other applications.

The ability of a system to operate in all situations is critical to Cyber operations. Reliability is challenging for systems that can learn and adapt [84]. The system behavior can be modified, updated, and advanced during operation while its operational context is affected by external factors. In the case of the recent Boeing 737 MAX groundings, a failed sensor incorrectly altered the system’s operational context and caused two planes to crash [85]. If the control system could learn and adapt as an intelligent, adaptive system, it could compensate for such failures.
The Proceedings of the 20th Monterey Workshop is available through the NPS Library. The workshop series has discussed many topics and has guided directions taken by research sponsors including the Army Research Office, National Science Foundation, Office of Naval Research, Air Force Office of Sponsored Research, Defense Advanced Research Projects Agency, and other organizations. The past Monterey Workshops proceedings are available on the websites of various sponsoring organizations, which can be found by Googling “Monterey Workshop”, or via the (under construction) website https://my.nps.edu/group/monterey-workshop.
REFERENCES


APPENDIX A: EXECUTIVE ORDER 5/2/2019

AMERICA’S CYBERSECURITY WORKFORCE

By the authority vested in me as President by the Constitution and the laws of the United States of America, and to better ensure continued American economic prosperity and national security, it is hereby ordered as follows:

Section 1. Policy. (a) America’s cybersecurity workforce is a strategic asset that protects the American people, the homeland, and the American way of life. The National Cyber Strategy, the President’s 2018 Management Agenda, and Executive Order 13800 of May 11, 2017 (Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure), each emphasize that a superior cybersecurity workforce will promote American prosperity and preserve peace. America’s cybersecurity workforce is a diverse group of practitioners who govern, design, defend, analyze, administer, operate, and maintain the data, systems, and networks on which our economy and way of life depend. Whether they are employed in the public or private sectors, they are guardians of our national and economic security.

b) The United States Government must enhance the workforce mobility of America’s cybersecurity practitioners to improve America’s national cybersecurity. During their careers, America’s cybersecurity practitioners will serve in various roles for multiple and diverse entities. United States Government policy must facilitate the seamless movement of cybersecurity practitioners between the public and private sectors, maximizing the contributions made by their diverse skills, experiences, and talents to our Nation.

(c) The United States Government must support the development of cybersecurity skills and encourage ever-greater excellence so that America can maintain its competitive edge in cybersecurity. The United States Government must also recognize and reward the country’s highest-performing cybersecurity practitioners and teams.

d) The United States Government must create the organizational and technological tools required to maximize the cybersecurity talents and capabilities of American workers—especially when those talents and capabilities can advance our national and economic security. The Nation is experiencing a shortage of cybersecurity
talent and capability, and innovative approaches are required to improve access to training that maximizes individuals’ cybersecurity knowledge, skills, and abilities. Training opportunities, such as work-based learning, apprenticeships, and blended learning approaches, must be enhanced for both new workforce entrants and those who are advanced in their careers.

(e) In accordance with Executive Order 13800, the President will continue to hold heads of executive departments and agencies (agencies) accountable for managing cybersecurity risk to their enterprises, which includes ensuring the effectiveness of their cybersecurity workforces.

Sec. 2. Strengthening the Federal Cybersecurity Workforce. (a) To grow the cybersecurity capability of the United States Government, increase integration of the Federal cybersecurity workforce, and strengthen the skills of Federal information technology and cybersecurity practitioners, the Secretary of Homeland Security, in consultation with the Director of the Office of Management and Budget (OMB) and the Director of the Office of Personnel Management (OPM), shall establish a cybersecurity rotational assignment program, which will serve as a mechanism for knowledge transfer and a development program for cybersecurity practitioners. Within 90 days of the date of this order, the Secretary of Homeland Security, in consultation with the Directors of OMB and OPM, shall provide a report to the President that describes the proposed program, identifies its resource implications, and recommends actions required for its implementation. The report shall evaluate how to achieve the following objectives, to the extent permitted by applicable law, as part of the program:

(i) The non-reimbursable detail of information technology and cybersecurity employees, who are nominated by their employing agencies, to serve at the Department of Homeland Security (DHS);

(ii) The non-reimbursable detail of experienced cybersecurity DHS employees to other agencies to assist in improving those agencies’ cybersecurity risk management;

(iii) The use of the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NICE Framework) as the basis for cybersecurity skill requirements for program participants;
(iv) The provision of training curricula and expansion of learning experiences to develop participants’ skill levels; and

(v) Peer mentoring to enhance workforce integration.

(b) Consistent with applicable law and to the maximum extent practicable, the Administrator of General Services, in consultation with the Director of OMB and the Secretary of Commerce, shall:

(i) Incorporate the NICE Framework lexicon and taxonomy into workforce knowledge and skill requirements used in contracts for information technology and cybersecurity services;

(ii) Ensure that contracts for information technology and cybersecurity services include reporting requirements that will enable agencies to evaluate whether personnel have the necessary knowledge and skills to perform the tasks specified in the contract, consistent with the NICE Framework; and

(iii) Provide a report to the President, within 1 year of the date of this order, that describes how the NICE Framework has been incorporated into contracts for information technology and cybersecurity services, evaluates the effectiveness of this approach in improving services provided to the United States Government, and makes recommendations to increase the effective use of the NICE Framework by United States Government contractors.

(c) Within 180 days of the date of this order, the Director of OPM, in consultation with the Secretary of Commerce, the Secretary of Homeland Security, and the heads of other agencies as appropriate, shall identify a list of cybersecurity aptitude assessments for agencies to use in identifying current employees with the potential to acquire cybersecurity skills for placement in reskilling programs to perform cybersecurity work. Agencies shall incorporate one or more of these assessments into their personnel development programs, as appropriate and consistent with applicable law.

(d) Agencies shall ensure that existing awards and decorations for the uniformed services and civilian personnel recognize performance and achievements in the areas of cybersecurity and cyber-operations, including by ensuring the availability of awards and decorations equivalent to citations issued pursuant to Executive Order 10694 of January 10, 1957 (Authorizing the Secretaries of the Army, Navy, and Air Force To Issue
Citations in the Name of the President of the United States to Military and Naval Units for Outstanding Performance in Action), as amended. Where necessary and appropriate, agencies shall establish new awards and decorations to recognize performance and achievements in the areas of cybersecurity and cyber-operations. The Assistant to the President for National Security Affairs may recommend to agencies that any Cyber unified coordination group or similar ad hoc interagency group that has addressed a significant cybersecurity or cyber-operations-related national security crisis, incident, or effort be recognized for appropriate awards and decorations.

(e) The Secretary of Homeland Security, in consultation with the Secretary of Defense, the Director of the Office of Science and Technology Policy, the Director of OMB, and the heads of other appropriate agencies, shall develop a plan for an annual cybersecurity competition (President’s Cup Cybersecurity Competition) for Federal civilian and military employees. The goal of the competition shall be to identify, challenge, and reward the United States Government’s best cybersecurity practitioners and teams across offensive and defensive cybersecurity disciplines. The plan shall be submitted to the President within 90 days of the date of this order. The first competition shall be held no later than December 31, 2019, and annually thereafter. The plan for the competition shall address the following:

(i) The challenges and benefits of inviting advisers, participants, or observers from non-Federal entities to observe or take part in the competition and recommendations for including them in future competitions, as appropriate;

(ii) How the Department of Energy, through the National Laboratories, in consultation with the Administrator of the United States Digital Service, can provide expert technical advice and assistance to support the competition, as appropriate;

(iii) The parameters for the competition, including the development of multiple individual and team events that test cybersecurity skills related to the NICE Framework and other relevant skills, as appropriate. These parameters should include competition categories involving individual and team events, software reverse engineering and exploitation, network operations, forensics, big
data analysis, Cyber analysis, Cyber defense, Cyber exploitation, secure programming, obfuscated coding, cyber-physical systems, and other disciplines;

(iv) How to encourage agencies to select their best cybersecurity practitioners as individual and team participants. Such practitioners should include Federal employees and uniformed services personnel from Federal civilian agencies, as well as Department of Defense active duty military personnel, civilians, and those serving in a drilling reserve capacity in the Armed Forces Reserves or National Guard;

(v) The extent to which agencies, as well as uniformed services, may develop a President’s Cup awards program that is consistent with applicable law and regulations governing awards and that allows for the provision of cash awards of not less than $25,000. Any such program shall require the agency to establish an awards program before allowing its employees to participate in the President’s Cup Cybersecurity Competition. In addition, any such program may not preclude agencies from recognizing winning and non-winning participants through other means, including honorary awards, informal recognition awards, rating-based cash awards, time-off awards, Quality Step Increases, or other agency-based compensation flexibilities as appropriate and consistent with applicable law; and

(vi) How the uniformed services, as appropriate and consistent with applicable law, may designate service members who win these competitions as having skills at a time when there is a critical shortage of such skills within the uniformed services. The plan should also address how the uniformed services may provide winning service members with a combination of bonuses, advancements, and meritorious recognition to be determined by the Secretaries of the agencies concerned.

(f) The Director of OMB shall, in consultation with appropriate agencies, develop annually a list of agencies and subdivisions related to cybersecurity that have a primary function of intelligence, counterintelligence, investigative, or national security work, including descriptions of such functions. The Director of OMB shall provide this list to the President, through the Deputy Assistant to the President for Homeland Security and Counterterrorism (DAPHSCT), every year starting September 1, 2019, for consideration
of whether those agencies or subdivisions should be exempted from coverage under the Federal Labor-Management Relations Program, consistent with the requirements of section 7103(b)(1) of title 5, United States Code.

Sec. 3. Strengthening the Nation’s Cybersecurity Workforce. (a) The Secretary of Commerce and the Secretary of Homeland Security (Secretaries), in coordination with the Secretary of Education and the heads of other agencies as the Secretaries determine is appropriate, shall execute, consistent with applicable law and to the greatest extent practicable, the recommendations from the report to the President on Supporting the Growth and Sustainment of the Nation’s Cybersecurity Workforce (Workforce Report) developed pursuant to Executive Order 13800. The Secretaries shall develop a consultative process that includes Federal, State, territorial, local, and tribal governments, academia, private-sector stakeholders, and other relevant partners to assess and make recommendations to address national cybersecurity workforce needs and to ensure greater mobility in the American cybersecurity workforce. To fulfill the Workforce Report’s vision of preparing, growing, and sustaining a national cybersecurity workforce that safeguards and promotes America’s national security and economic prosperity, priority consideration will be given to the following imperatives:

(i) To launch a national Call to Action to draw attention to and mobilize public- and private-sector resources to address cybersecurity workforce needs;

(ii) To transform, elevate, and sustain the cybersecurity learning environment to grow a dynamic and diverse cybersecurity workforce;

(iii) To align education and training with employers’ cybersecurity workforce needs, improve coordination, and prepare individuals for lifelong careers; and

(iv) To establish and use measures that demonstrate the effectiveness and impact of cybersecurity workforce investments.

(b) To strengthen the ability of the Nation to identify and mitigate cybersecurity vulnerabilities in critical infrastructure and defense systems, particularly cyber-physical systems for which safety and reliability depend on secure control systems, the Secretary of Defense, the Secretary of Transportation, the Secretary of Energy, and the Secretary of Homeland Security, in coordination with the Director of OPM and the Secretary of
Labor, shall provide a report to the President, through the DAPHSCT, within 180 days of the date of this order that:

(i) Identifies and evaluates skills gaps in Federal and non-Federal cybersecurity personnel and training gaps for specific critical infrastructure sectors, defense critical infrastructure, and the Department of Defense’s platform information technologies; and

(ii) Recommends curricula for closing the identified skills gaps for Federal personnel and steps the United States Government can take to close such gaps for non-Federal personnel by, for example, supporting the development of similar curricula by education or training providers.

(c) Within 1 year of the date of this order, the Secretary of Education, in consultation with the DAPHSCT and the National Science Foundation, shall develop and implement, consistent with applicable law, an annual Presidential Cybersecurity Education Award to be presented to one elementary and one secondary school educator per year who best instill skills, knowledge, and passion with respect to cybersecurity and cybersecurity-related subjects. In developing and implementing this award, the Secretary of Education shall emphasize demonstrated superior educator accomplishment — without respect to research, scholarship, or technology development — as well as academic achievement by the educator’s students.

(d) The Secretary of Commerce, the Secretary of Labor, the Secretary of Education, the Secretary of Homeland Security, and the heads of other appropriate agencies shall encourage the voluntary integration of the NICE Framework into existing education, training, and workforce development efforts undertaken by State, territorial, local, tribal, academic, non-profit, and private-sector entities, consistent with applicable law. The Secretary of Commerce shall provide annual updates to the President regarding effective uses of the NICE Framework by non-Federal entities and make recommendations for improving the application of the NICE Framework in cybersecurity education, training, and workforce development.

Sec. 4. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:
(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP

THE WHITE HOUSE,

May 2, 2019.
APPENDIX B: EXECUTIVE ORDER 5/15/2019

SECURING THE INFORMATION AND COMMUNICATIONS TECHNOLOGY AND SERVICES SUPPLY CHAIN

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 et seq.), and section 301 of title 3, United States Code,

I, DONALD J. TRUMP, President of the United States of America, find that foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services, which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services, in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people. I further find that the unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. This threat exists both in the case of individual acquisitions or uses of such technology or services, and when acquisitions or uses of such technologies are considered as a class. Although maintaining an open investment climate in information and communications technology, and in the United States economy more generally, is important for the overall growth and prosperity of the United States, such openness must be balanced by the need to protect our country against critical national security threats. To deal with this threat, additional steps are required to protect the security, integrity, and reliability of information and communications technology and services provided and used in the United States. In light of these findings, I hereby declare a national emergency with respect to this threat.
Accordingly, it is hereby ordered as follows:

Section 1. Implementation. (a) The following actions are prohibited: any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service (transaction) by any person, or with respect to any property, subject to the jurisdiction of the United States, where the transaction involves any property in which any foreign country or a national thereof has any interest (including through an interest in a contract for the provision of the technology or service), where the transaction was initiated, is pending, or will be completed after the date of this order, and where the Secretary of Commerce (Secretary), in consultation with the Secretary of the Treasury, the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the United States Trade Representative, the Director of National Intelligence, the Administrator of General Services, the Chairman of the Federal Communications Commission, and, as appropriate, the heads of other executive departments and agencies (agencies), has determined that:

(i) the transaction involves information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and

(ii) the transaction:

(A) poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;

(B) poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or

(C) otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

(b) The Secretary, in consultation with the heads of other agencies as appropriate, may at the Secretary’s discretion design or negotiate measures to mitigate concerns identified under section 1(a) of this order. Such measures may serve as a precondition to
the approval of a transaction or of a class of transactions that would otherwise be prohibited pursuant to this order.

(c) The prohibitions in subsection (a) of this section apply except to the extent provided by statutes, or in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted prior to the effective date of this order.

Sec. 2. Authorities. (a) The Secretary, in consultation with, or upon referral of a particular transaction from, the heads of other agencies as appropriate, is hereby authorized to take such actions, including directing the timing and manner of the cessation of transactions prohibited pursuant to section 1 of this order, adopting appropriate rules and regulations, and employing all other powers granted to the President by IEEPA, as may be necessary to implement this order. All agencies of the United States Government are directed to take all appropriate measures within their authority to carry out the provisions of this order.

(b) Rules and regulations issued pursuant to this order may, among other things, determine that particular countries or persons are foreign adversaries for the purposes of this order; identify persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries for the purposes of this order; identify particular technologies or countries with respect to which transactions involving information and communications technology or services warrant particular scrutiny under the provisions of this order; establish procedures to license transactions otherwise prohibited pursuant to this order; establish criteria, consistent with section 1 of this order, by which particular technologies or particular participants in the market for information and communications technology or services may be recognized as categorically included in or as categorically excluded from the prohibitions established by this order; and identify a mechanism and relevant factors for the negotiation of agreements to mitigate concerns raised in connection with subsection 1(a) of this order. Within 150 days of the date of this order, the Secretary, in consultation with the Secretary of the Treasury, Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the United States Trade Representative, the Director of National Intelligence, the Administrator of General Services, the Chairman of the Federal Communications
Commission and, as appropriate, the heads of other agencies, shall publish rules or regulations implementing the authorities delegated to the Secretary by this order.

(c) The Secretary may, consistent with applicable law, redelegate any of the authorities conferred on the Secretary pursuant to this section within the Department of Commerce.

Sec. 3. Definitions. For purposes of this order:

(a) the term “entity” means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization;

(b) the term “foreign adversary” means any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons;

(c) the term “information and communications technology or services” means any hardware, software, or other product or service primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means, including transmission, storage, and display;

(d) the term “person” means an individual or entity; and

(e) the term “United States person” means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States.

Sec. 4. Recurring and Final Reports to the Congress. The Secretary, in consultation with the Secretary of State, is hereby authorized to submit recurring and final reports to the Congress on the national emergency declared in this order, consistent with section 401(c) of the NEA (50 U.S.C. 1641(c)) and section 204(c) of IEEPA (50 U.S.C. 1703(c)).

Sec. 5. Assessments and Reports. (a) The Director of National Intelligence shall continue to assess threats to the United States and its people from information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. The Director of National Intelligence shall produce periodic written assessments of these threats in consultation with the heads of relevant agencies, and shall
provide these assessments to the President, the Secretary for the Secretary’s use in connection with his responsibilities pursuant to this order, and the heads of other agencies as appropriate. An initial assessment shall be completed within 40 days of the date of this order, and further assessments shall be completed at least annually, and shall include analysis of:

(i) threats enabled by information and communications technologies or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and

(ii) threats to the United States Government, United States critical infrastructure, and United States entities from information and communications technologies or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the influence of a foreign adversary.

(b) The Secretary of Homeland Security shall continue to assess and identify entities, hardware, software, and services that present vulnerabilities in the United States and that pose the greatest potential consequences to the national security of the United States. The Secretary of Homeland Security, in coordination with sector-specific agencies and coordinating councils as appropriate, shall produce a written assessment within 80 days of the date of this order, and annually thereafter. This assessment shall include an evaluation of hardware, software, or services that are relied upon by multiple information and communications technology or service providers, including the communication services relied upon by critical infrastructure entities identified pursuant to section 9 of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity).

(c) Within 1 year of the date of this order, and annually thereafter, the Secretary, in consultation as appropriate with the Secretary of the Treasury, the Secretary of Homeland Security, Secretary of State, the Secretary of Defense, the Attorney General, the United States Trade Representative, the Director of National Intelligence, and the Chairman of the Federal Communications Commission, shall assess and report to the President whether the actions taken by the Secretary pursuant to this order are sufficient and continue to be necessary to mitigate the risks identified in, and pursuant to, this order.
Sec. 6. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP
THE WHITE HOUSE,
May 15, 2019.
INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Fort Belvoir, VA 22060

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California 93943

3. Research Sponsored Programs Office, Code 41
   Naval Postgraduate School
   Monterey, CA 93943

4. Dean of Research
   Naval Postgraduate School
   Monterey, CA 93943

5. Prof. Luqi, Computer Science
   Naval Postgraduate School
   Monterey, CA 93943