DoD Centers of Excellence Meeting with AFIT

Center of Excellence in Cyber Security
@ Norfolk State University

Dayton, OH
24 January 2019
1. **COE Overview**  
   - George Hsieh (PI), Norfolk State University

2. **COE Research Infrastructure and Cybersecurity Testbed**  
   - George Hsieh

3. **Cyber Training, Intrusion Detection and Response**  
   - George Hsieh

4. **Cyber Intelligence and Cyber Defense**  
   - Sachin Shetty (Co-PI), Old Dominion University

5. **Cyber Modeling, Simulation and Decision Support**  
   - Jose Padilla (Co-PI), ODU

6. **Ethical Decision Making in Cyberspace**  
   - Mary Ann Hoppa (Co-PI), NSU

7. **Cyberpsychology and Human Behavior in Cyberspace**  
   - Scott Debb, NSU
Organization

- **Lead Institution: Norfolk State University**
  - Computer Science; Information Assurance Research, Education and Development Institute (IA-REDI)
  - PI: George Hsieh, Co-PI’s: Jonathan Graham & Mary Ann Hoppa

- **Academic Collaborator: Old Dominion University**
  - Virginia Modeling, Analysis and Simulation Center (VMASC)
  - Co-PI’s: Sachin Shetty & Jose Padilla

- **Cooperative Agreement Management**
  - Ms. Evelyn Kent (OUSD Program Manager)
  - Dr. Laurent Njilla (AFRL Program Manager)
  - Dr. Tim Kroecker (AFRL Deputy Program Manager)
Mission & Objectives

• Mission
  – Increase knowledge and application of cyber security based on multidisciplinary and collaborative research
  – Increase capacity in research, education, and professional development for faculty and students

• Objectives
  – Conduct basic research to develop a cloud-enabled, big-data-analytics-capable Cyber Analysis, Simulation and Experimentation Environment (CASE-V) for enhancing situational awareness and decision support capabilities for cyber defense and cyber training
  – Perform research-related education and outreach activities
  – Be a valued resource for the Nation and HBCU/MI Community
Research Program

Applications

- Cyber Defense (APT)
- Cyber Training (APT)

Platforms

Cyber Analysis, Simulation & Experimentation Environment (CASE-V) Framework & Test-bed

Enabling Technologies

- Big Data Analytics & Cloud Computing
- Cyber Situational Awareness
- Systems, Emulations & Simulations
- Cyber Decision Support
Research Thrusts

- **Cyber Intelligence and Cyber Defense**
  - Explore innovative theories, methodologies and techniques in cyber intelligence and cyber defense for CASE-V (Lead: Sachin Shetty)

- **Cyber Modeling, Simulation, Analysis & Decision Support**
  - Develop foundational modeling, simulation, analysis, intelligent systems & decision support capabilities for CASE-V (Lead: Jose Padilla)

- **Cyber Training and Intrusion Detection & Response**
  - Develop integrated training and intrusion detection & response capabilities for CASE-V (Lead: Jonathan Graham)

- **CASE-V Framework & Testbed**
  - Develop the CASE-V framework, infrastructure, and testbed (Lead: George Hsieh)
Project Status

• **Made significant progress in research**
  – Established a solid foundation of CASE-V framework & testbed
  – Developed a broad spectrum of techniques and components ready for integration into CASE-V testbed

• **Established strong partnerships**
  – AFRL/Rome, Sandia National Labs, SPAWAR
  – DoE Consortium for K-20 Cybersecurity Workforce Pipeline

• **Made broad impact**
  – NSU and HBCU community in capacity building
  – Research-related education, outreach & workforce development

• **Enabled NSU to reach a significantly higher level of excellence**
  – Growing recognition as a leader in cybersecurity research and related activities
  – Ready to accelerate, expand, and reach for the next higher level of excellence
Broad Impact

- **Planning for two new degree programs**
  - MS in Cyberpsychology pending approval by Commonwealth of Virginia
  - Doctoral in Cybersecurity (early planning stage)

- **Enrollment in MS in Cybersecurity program (launched in August 2015)**
  - growing fast

- **Internship programs**
  - DoD COEs internship program: 8 ('18), 7 ('17), 3 ('16)
  - COE in Cyber Security summer internship program at NSU
    - 4 interns supported by COE each year (2015 - 2018)
    - Additional 16 interns for 2018 supported by DoE Consortium project & NSU
  - SPAWAR Cybersecurity internship program: 3 ('18), 2 ('17)

- **Workforce development**
  - Two former research assistants pursuing PhD now (VT and Purdue)
  - One current URA (also former 2017 intern @ AFRL/Rome) receiving DoD Cybersecurity scholarship
  - Ten former RAs and interns graduated in 2017 & 2018: currently @ AFRL/Rome (1), SPAWAR (3), Sandia National Labs (2), Purdue University (1), private industry (3) including Nvidia
Plans for Next 2+ Years

- **Continue with the established four research thrusts**
  - Put more emphasis on machine learning for cyber and security for machine learning
  - Put more emphasis on Internet of Battle Things (IoBT) security and trust
  - Put more emphasis on warfighters behavior in cyberspace

- **Expand CASE-V testbed capabilities and usage**
  - Enhance CASE-V platform capabilities, automation and usability
  - Deploy and integrate CASE-V components and techniques onto CASE-V platform
  - Complete installation of fiber link to ODU and deploy ODU developed capabilities
  - Collaboration with selected research partners (e.g., AFRL, SPAWAR, Sandia, DoE Consortium schools)

- **Expand strategic partnerships**
  - AFRL, SPAWAR, MLRCP, NSWC Dahlgren, DoD TRMC
  - George Mason University, Virginia Tech, MITRE, Virginia Cyber Range

- **Expand internship, outreach, and workforce development programs**
  - Joint advisement of student research projects
  - Pipeline for federal internship programs & NSU’s degree programs
1. **COE Overview**  
   – George Hsieh (PI), Norfolk State University

2. **COE Research Infrastructure and Cybersecurity Testbed**  
   – George Hsieh

3. **Cyber Training, Intrusion Detection and Response**  
   – George Hsieh

4. **Cyber Intelligence and Cyber Defense**  
   – Sachin Shetty (Co-PI), Old Dominion University

5. **Cyber Modeling, Simulation and Decision Support**  
   – Jose Padilla (Co-PI), ODU

6. **Ethical Decision Making in Cyberspace**  
   – Mary Ann Hoppa (Co-PI), NSU

7. **Cyberpsychology and Human Behavior in Cyberspace**  
   – Scott Debb, NSU
Research Infrastructure

• **State-of-the-art facilities and equipment**
  – New NSU Cybersecurity Complex (Phase 2) specially designed for COE in Cyber Security (Opened in April 2018)
  – New CASE-V testbed system is operational, and installation & configuration of platform and application layer capabilities continuing*

• **NSU Cybersecurity Complex (Phase 2)**
  – Total investment in construction and equipment: ~$2.5M (with $1M from DoD Equipment Program: FY14 & FY16)
  – Special security arrangement
    ▪ Dedicated firewall and intrusion prevention system
    ▪ Isolated from NSU network
    ▪ Secure internet access via web and virtual private network

• New private optic fiber link between NSU & ODU in place (provided by City of Norfolk)

• **ODU Cloud Research and Cybersecurity Research Labs (new)**

Wide-Area Networking
CASE-V Testbed System

- **Multi-functional, modular & robust architecture:** OpenStack cloud platforms, Hadoop big data platforms, shared storage, high-performance networks, redundancy
- **Substantial capacity:** HDD: ~820 TB, server-grade CPU cores: ~1,700, RAM: ~7.5 TB, 10/40 Gb switches
- Installation & operation by COE students and faculty in coordination with NSU IT Department
CASE-V Datacenter
CASE-V Testbed Enhancement Proposal * Submitted to FY19 DoD Equipment Program (Under Review)

- Add new clusters for high-performance computing, e.g., machine learning, modeling & simulation, real-time data analytics: two GPU-accelerated server clusters with Nvidia GPUs, all-SSD iSCSI SAN
- Improve core network performance: upgrade to 40 Gb port speed
Agenda

1. COE Overview
   – George Hsieh (PI), Norfolk State University

2. COE Research Infrastructure and Cybersecurity Testbed
   – George Hsieh

3. Cyber Training, Intrusion Detection and Response
   – George Hsieh

4. Cyber Intelligence and Cyber Defense
   – Sachin Shetty (Co-PI), Old Dominion University

5. Cyber Modeling, Simulation and Decision Support
   – Jose Padilla (Co-PI), ODU

6. Ethical Decision Making in Cyberspace
   – Mary Ann Hoppa (Co-PI), NSU

7. Cyberpsychology and Human Behavior in Cyberspace
   – Scott Debb, NSU
Sample Research Activities: Cyber Training & Intrusion Detection

- **Machine learning & data analytics**
  - Malware classification using deep learning techniques
  - Open source cybersecurity intelligence using Tweeter, natural language processing, and Elastic Stack

- **Cyber training & experimentation**
  - Gh0st attack scenario
  - Automated attacker scenarios

- **Cyber defense & response**
  - Gh0st attack forensic analysis
  - Elastic Stack and anomaly detection

- **CASE-V automation & user interface**
  - Responsive web application using MEAN Stack
  - Task automation using JavaScript and Python scripts
Sample Research Activities: Digital Forensic Analysis

- Automated guide for digital forensics first responders
- Automated guide for digital forensics analysis
- Developing digital forensics case studies
- Comparing mobile forensic tools
- Detecting traces of malware after a remote access Trojan attack
- Graphically inspired authentication techniques: thematical graphical user authentication
Malware Classification

• **Rationale**
  - Vast amounts of data and files need to be evaluated for malicious intent
  - To evade detection, malware authors introduce polymorphism and produce new malware belonging to same "family" with same forms of malicious behavior
  - Group them into families, and detect new malware as malicious and of a certain family

• **Objectives**
  - Provide malware classification experimentation environment on CASE-V testbed
  - Develop malware classification capabilities for Hadoop big data platform
  - Develop enhanced malware classification techniques

• **Current Status**
  - Completed V1.1 implementation (M.S. Project by Mamta Kumari *)
    - Based on image processing approach (treating a binary executable as an image)
    - Use deep learning ML algorithm (CNN) for self-learning
    - Use malware datasets provided by Microsoft for Kaggle BIG 2015 Challenge
  ⇒ Processing time much reduced to support (near) real-time and scalability

Malware Classification using Deep Learning

• Implementation
  - Integrate transfer learning technique (to facilitate model building and leverage pre-built models such as VGG-16) [Model #2]
  - Use TensorFlow, Keras, Python Imaging Library, Scikit-learn, etc.

• Performance

<table>
<thead>
<tr>
<th>Model Number</th>
<th>Training Time Taken CPU</th>
<th>Training Time Taken GPU</th>
<th>Validation Accuracy</th>
<th>Loss</th>
<th>Number Of Epochs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>600-700s per epoch</td>
<td>250s-300s per epoch</td>
<td>0.9698</td>
<td>0.129</td>
<td>50</td>
</tr>
<tr>
<td>2</td>
<td>60 s per epoch</td>
<td>20s per epoch</td>
<td>0.9707</td>
<td>0.1252</td>
<td>50</td>
</tr>
<tr>
<td>3</td>
<td>500s per epoch</td>
<td>250s per epoch</td>
<td>0.9679</td>
<td>0.13</td>
<td>50</td>
</tr>
</tbody>
</table>
• **Objectives**
  - Develop an automated threat intelligence collection and analysis system using Twitter data
    - Natural Language Processing (NLP): data pre-processing
    - Machine Learning: Information Extraction
    - Elastic Stack: Search and Visualization

• **Status**
  - Completed V1.0 implementation (M.S. Project by Satya Vadapalli*)
    - Linux platform, Java and Eclipse
    - Twitter4J - Twitter API binding library for Java to collect data through Twitter Streaming API based on a set of specified keywords
    - Stanford CoreNLP
    - Entity Extraction Library to identify and label cyber-domain entities from unstructured text (Oak Ridge National Labs): vulnerabilities, software products, software vendors

TwitterOSINT Architecture
Cyber Training & Experimentation Environment

- **Motivations**
  - Learning by doing: hands-on practices and explorations
  - Awareness: see what attackers can do and how dangerous they can be

- **Gh0st RAT malware as a case study**
  - One of the most notorious and widely deployed APTs, with many variants still going around
  - Exploit Windows vulnerability to take full control of victim systems remotely
  - Hard to detect with evasion & obfuscation techniques

- **Cyber kill chain as work flow model**

- **Two types of virtual lab environments**
  - Desktop/laptop (e.g., Windows) based environment
    - Simplified emulation of attacker actions
    - Require modest level of computing resources and IT knowledge
    - Suitable for use by individual learners and beginners
    - End user can be tasked with setting up the environment
  - Cloud or datacenter based environment
    - Can emulate more complex enterprise networks and attacker actions
    - Require higher level of computing resources and IT knowledge
    - Suitable for shared use by community of learners
    - Lab set up and operation by trained personnel or advanced learners
Emulated Attacker – Gh0st

- **Desktop VM Environment (VirtualBox)**
  - Version 1.1 completed (M.S. Project by Brandon Johnson*)
  - Use Metasploit in Kali Linux to launch exploits and actions
  - Use Gh0st as first use case
  - Developed Ruby scripts to automate Metasploit tasks to download and install Gh0st (upon victim clicking on a malicious link in phishing email)
    - Less error prone
    - Faster execution ⇒ reduced detection risks
  - Three VMs: Gh0st C2 server & Gh0st victim: Windows 7; and Kali Linux

<table>
<thead>
<tr>
<th>VM Name</th>
<th>Role</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gh0stRATClient</td>
<td>Gh0st Client (Attacker)</td>
<td>192.168.56.51</td>
</tr>
<tr>
<td>VictimMachine</td>
<td>Gh0st Server (Victim)</td>
<td>192.168.56.31</td>
</tr>
<tr>
<td>Kali Linux</td>
<td>Gh0st Deployment (Attacker)</td>
<td>192.168.56.101</td>
</tr>
</tbody>
</table>

- **To deploy onto CASE-V OpenStack platform**

• **Objectives**
  − Encompass life cycle of cyber kill chain of advanced targeted threats
  − Integrate attack, defense, detection, forensic analysis, incident response, and recover capabilities

• **Status**
  − Completed V1.0 implementation (through a M.S. Thesis by Kaila Perry*)
  − Collaborated with Sandia Tracer FIRE (Forensic and Incident Response) environment
  − Based on XenServer 6.5
  − Use Gh0st as a use case

• **To port onto CASE-V OpenStack platform**

Enterprise APT Experimentation Environment (V1.0)
UI & Automation Framework for CASE-V Testbed

• **Goals**
  - Support different platforms, programming languages and API’s
  - User-friendly, extensible, robust, secure, scalable
  - Responsive web interfaces and dynamic information updates
  - Use best-in-class technologies and architectures

• **Prototype Development**
  - Version 1 completed (B.S. Seminar Project by Cody Butler and George Thompson*)
  - Use MEAN Stack (MongoDB, Express.js, AngularJS & Node.js) and Bootstrap
  - Developed scripts (Python, Linux shell, Windows shell) to execute tasks

• **To deploy onto CASE-V platform and continue developing**

Digital Forensics @ NSU

- **Digital forensics courses**
  - CSC-494 Digital Forensics
  - CSC-672 Advanced Digital Forensics
  - CYS-672 Computer and Network Forensics

- **Digital forensics future curriculum goals**
  - Develop a certificate in Digital Forensics
  - Attain NSA/DHS CAE Focus area in Digital Forensics (Dr. Jonathan Graham and Dr. Cheryl Hinds)
  - Attain National Center of Digital Forensics Academic Excellence (CDFAE) by the U.S. Department of Defense Cyber Crime Center (DC3) (Dr. Jonathan Graham and Cheryl Hinds)
Automated Guide for Digital Forensics First Responders

- **Objective**
  - Develop a portable step-by-step guide for digital forensics first responders

- **Status**
  - Undergraduate Capstone Project (Advisor: Dr. Cheryl Hinds, Student: Peter Fenton*)
    - Created a mobile iOS application for first responders based on authoritative guidelines for digital first responders
    - Preliminary evaluation showed that the application was friendly and easy to use

- **Next steps**
  - Port the application to Android platform

Automated Digital Forensics Analysis

• **Objective**
  - Develop a portable step-by-step guide for digital forensics analysts

• **Status**
  - Undergraduate Capstone project (Advisor: Dr. Jonathan Graham, Students: Erica Baker and Jasmine Mabrey*)
    - Created a database of locations of digital forensics artifacts, references validating these artifacts, and additional information on how to extract these artifacts
    - Created a front end to guide the analysts on how to locate the artifacts

• **Next steps**
  - Determine how to automate the processing of the digital forensic images

Detecting Traces of Malware after a Remote Access Trojan Attack

• Objective
  – Identify traces left behind after a Remote Access Trojan Gh0st attack

• Status
  – MS Computer Science Project (Sandi Samuel*)
    ▪ Was able to identify Gh0st signature strings in network traffic and in RAM
    ▪ Was able to identify several suspicious files with common system names, but appearing in unlikely locations
    ▪ Was able to identify a malware file which had been executed, but was then deleted

• Next steps
  – Experiment with other Trojans to determine patterns which can be used to identify new malware

Graphically Inspired Authentication Techniques: Thematic Graphical User Authentication

• **Objective**
  - Find a password scheme that is both user friendly and secure

• **Status**
  - MS Computer Science Project (Advisor: Dr. Cheryl Hinds, Student: Joshua Sherfield*)
    - Users selected several graphical images for their passwords
    - Authentication required users to click on their pre-selected images when presented on successive screens

Agenda

1. **COE Overview**
   - George Hsieh (PI), Norfolk State University

2. **COE Research Infrastructure and Cybersecurity Testbed**
   - George Hsieh

3. **Cyber Training, Intrusion Detection and Response**
   - George Hsieh

4. **Cyber Intelligence and Cyber Defense**
   - Sachin Shetty (Co-PI), Old Dominion University

5. **Cyber Modeling, Simulation and Decision Support**
   - Jose Padilla (Co-PI), ODU

6. **Ethical Decision Making in Cyberspace**
   - Mary Ann Hoppa (Co-PI), NSU

7. **Cyberpsychology and Human Behavior in Cyberspace**
   - Scott Debb, NSU
Research Thrust 1: Sample Research Projects

- **Attack Detection**
  - Transfer Learning for Malware Detection (completed)
  - Man-in-the Cloud Defender- SGX-based User Credential Protection for Synchronization applications in Cloud Computing Platform (completed)
  - Scalable Mining of Large Cyber Security Datasets (completed)

- **Cyber Security Risk Management**
  - Network Diversity Modeling for cyber risk assessment (completed)
  - Cyber Security Risk Assessment for Cloud Services (ongoing)

- **Cyber Resilience**
  - Software Defined Networking based resilience for Cyber Physical Systems (ongoing)
  - Analysis of Stepping Stones using Vulnerability Graphs (ongoing)
  - Modeling Attacker’s Opportunity for Improving Cyber Resilience (ongoing)
Life in the Security Operation Center

- Intrusion Detection System alerts
- Network configuration
- Security Risk Assessment
- Prioritized Mitigation Plan
- Users and data assets
- Vulnerability reports
- Apache HTTP Server 2.4 vulnerabilities
- Security advisories
Life in the Security Operation Center

- 160 Vulns
- 158 Vulns
- 47 Vulns
- 107 Vulns
- 60 Vulns
- 15 Vulns

Vulnerability Scanner

External Attacker

Server Network

DMZ Router

Database Network

DMZ Router

Network Server

Vulnerability Scanner

Frontend

Backend

Router

Firewall

Network

Server

Database

Vulnerability Scanner

External Attacker

192.168.1

192.168.1.5

smrsh (supplied by Sendmail) is designed to prevent the execution of commands outside the restricted environment. However, when double pipes (|) or a mixture of dot and slash characters are entered, a user may bypass the checks performed by smrsh. This can lead to the execution of commands outside the restricted environment.

Solution: Upgrade to the latest version of Sendmail (or at least 8.12.8).

Risk factor: Medium
CVE: CAN-2002-1165
BID: 5045

The remote sendmail server, according to its version number, may be vulnerable to a remote buffer overflow allowing remote users to gain root privileges.

Sendmail versions from 5.79 to 8.12.8 are vulnerable.

Solution: Upgrade to Sendmail 8.12.8 or later.
Research Challenges

- **Cognitive overload to the decision maker**
  - Overwhelming number of alerts
  - Lack of insight into impact of attack *impairs effective decision making*

- **Cyber defense Remediation Plan**
  - Which *vulnerability* to patch first?
  - Balance between *operational resilience* and security risk

- **Isolated Alerts**
  - Lack of strategies to integrate and *correlate alerts*

- **Missing Information**
  - Requires *reach-back* and updates from higher command levels

- **Attacker strategies/tactics**
  - Lateral Propagation
  - Stepping Stones/*Pivot Points*
Research Objectives

- Development of data-driven modeling techniques to assess and measure cyber risk
- Development of techniques to incorporate criticality of assets in cyber risk measurement.
- Characterize adversarial opportunity to conduct lateral propagation of attacker
- Development of prioritized mitigation plan for effective cyber defense remediation
- Development of optimal resource allocation scheme that balances tradeoff between operational resilience and cyber risk.
Measure Cyber Risk - Attack Graphs

• Adversaries penetrate network through a chain of exploits
  – Each exploit lays foundation for subsequent exploits
• Chain is called an attack path
• All possible attack paths form an attack graph
• Generate attack graphs to mission critical resources
• Report only those vulnerabilities associated with the attack graphs
Bayesian Attack Graph

A 192.168.51.59  
Web Server

B 192.168.51.60  
Database Server

C 192.168.51.61  
Proxy Server

D Remote Attacker

<table>
<thead>
<tr>
<th>B</th>
<th>C</th>
<th>Pr(A)</th>
<th>Pr(¬A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1.00</td>
<td>0.00</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0.65</td>
<td>0.35</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1.00</td>
<td>0.00</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

Pr(A)=0.61  
Unconditional Probability

<table>
<thead>
<tr>
<th>D</th>
<th>Pr(B)</th>
<th>Pr(¬B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.85</td>
<td>0.15</td>
</tr>
<tr>
<td>0</td>
<td>0.00</td>
<td>1.00</td>
</tr>
</tbody>
</table>

Pr(B)=0.60

<table>
<thead>
<tr>
<th>D</th>
<th>Pr(C)</th>
<th>Pr(¬C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.70</td>
<td>0.30</td>
</tr>
<tr>
<td>0</td>
<td>0.00</td>
<td>1.00</td>
</tr>
</tbody>
</table>

Pr(C)=0.49

<table>
<thead>
<tr>
<th>Pr(D)</th>
<th>Pr(¬D)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.70</td>
<td>0.30</td>
</tr>
</tbody>
</table>

Pr(D)=0.70

Probability of successful exploit

0.65

1.00
Cyber Risk Scoring and Mitigation (CRISM)

• **Objective**
  − Economic modeling and cyber risk management to measure and price cyber risk and develop prioritized mitigation plan

• **Approach**
  − Modeling to quantify the impacts of threats to cyber systems and networks to determine mitigation priorities
  − Modeling impact of the proposed defense on operational resilience and cost

• **Accomplishment**
  − Developed automatic cyber risk measurement tool
  − Bayesian attack graph modeling techniques to categorize attack paths by impact, cost and degree of difficulty


Criticality Analysis

• Model data-driven criticality of a node in ICS considering node heterogeneity.

• Optimal resource allocation scheme based on nodes’ criticality

• Examine relationship between cost models of resource budget allocation for removal of vulnerabilities on critical nodes and impact on availability.

• Empirical validation within an industrial control system (ICS) test-bed
Criticality Analysis

Network Scanning → Network Logs → Graph Generation → Attack Graph

Minimized Network Risk in Optimized Resource Allocation

Resource Allocation → Critical Paths → Critical Path Analysis

Host Scanning → Host Logs → Criticality Calculation → Node Ranking

Wireshark TCP/DNP3 dump
Node Criticality

- **Criticality of a node in ICS:** $C(i) = \alpha l(i) + \beta CEN(i) + \gamma d(i)$
  - $C(i)$ is the criticality of node $i$, driven by three properties $l(i), CEN(i)$, and $d(i)$ respectively indicate locality, centrality and physical damage properties of critical node $i$.

- **Locality ($l$):** Relative position of a node in architecture defined in IEC 62443
  - Mapped from running services and processes and collected from hosts’ scan logs.
  - A higher score assigned to an asset indicates proximity to the physical processes.

- **Centrality ($CEN$):** Centrality of node $i$ defined as: $CEN(i) = (\sum_{j=1}^{N} x_{ij})^{1-\delta} (\sum_{j=1}^{N} w_{ij})^{\delta}$
  - $x_{ij}$ indicates the degree of node $i$, $w_{ij}$ indicates normalized packet exchanged between node $i$ and $j$, and $\delta$ determines relative importance of the number of links to tie weights.

- **Damage Factor ($d$):** Potential damage to the physical plant: $d(i) = \left(\frac{P_l(i)}{P_T}\right)^{L^* - 1}$
  - $P_l(i)$ is loss of load for compromised system $i$, $P_T$ indicates system’s total load, and $L^*$ indicates the diverge point of power flow (P-V curve).
  - Derived from SCADA by extracting current and voltage values in DNP3 message.
Attack Graph and Criticality Analysis

- Analyst
- IPS/AV
- Mail
- IT Network
- WS
- DMZ
- SIEM
- APP. Server
- WebS
- DMZ/IDS
- OT Network
- SCADA1
- SCADA2
- OT/IDS
- ADM/IDS
- RTU1, Substation-1
- RTU2, Substation-2
- Breaker
- Breaker
- 0. attackerLocated (internet)
  1. victim browse a malicious website
  2. canAccessMaliciousInput (workStation, user, IE)
  3. remote exploit of CVE-2009-1938
  4. execCode (workStation, userAccount)
  5. multihop access
  6. netAccess (webServer, tcp.80)
  7. remote exploit of CVE-2006-3747
  8. execCode (webServer, apache)
  9. multihop access
  10a. netAccess to SCADA (SCADA Server, tcp.3306)
  10b. netAccess to SCADA (SCADA Server, tcp.3306)
  11a. local escalate of privilege CVE-2018-5313
  11b. local escalate of privilege CVE-2018-5313
  12a. escalatePrivilege (SCADA 1, UserAccount)
  12b. escalatePrivilege (SCADA 1, UserAccount)
  13. direct network access

CP: Conditional probability
C: Criticality of the node
R: Node’s Risk
**Resource Allocation, Remediation Plan and Cost Model**

**Exponential Cost Model:**

\[ V_i(A_i) = e^{-\sigma_i A_i}; \quad 0 \leq A_i \leq 1; \quad \text{where, } \sigma_i = \frac{1}{\max A_i} \]

Allocation of budget \( B_D \) to nodes is optimized when objective function \( R \) is minimized. The optimized function is:

\[ R(A_i) = \sum_{i=1}^{N} e^{-\sigma_i A_i C_i} - \lambda [\sum_{i=1}^{N} A_i - B_D] \]

where, \( A_i = \frac{\ln(\sigma_i C_i) - \ln(\lambda)}{\sigma_i} \) and \( \ln(\lambda) = \frac{\sum_{i=1}^{N} \frac{\ln(\sigma_i C_i)}{\sigma_i}}{\sum_{i=1}^{N} \frac{1}{\sigma_i}} - B_D \)

---

**Exponential Cost Resource Allocation**

<table>
<thead>
<tr>
<th>Nodes</th>
<th>( C )</th>
<th>( \max A )</th>
<th>( C / \max A )</th>
<th>( A )</th>
<th>( V(%) )</th>
<th>( R )</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS</td>
<td>3.1</td>
<td>4.94</td>
<td>0.63</td>
<td>0</td>
<td>72</td>
<td>2.232</td>
</tr>
<tr>
<td>WebS</td>
<td>7.38</td>
<td>4.94</td>
<td>1.49</td>
<td>0</td>
<td>14.4</td>
<td>1.06</td>
</tr>
<tr>
<td>SCADA1</td>
<td>13.36</td>
<td>4.94</td>
<td>2.7</td>
<td>4.371</td>
<td>4.8</td>
<td>0.641</td>
</tr>
<tr>
<td>SCADA2</td>
<td>12.35</td>
<td>4.94</td>
<td>2.5</td>
<td>3.98</td>
<td>5.14</td>
<td>0.634</td>
</tr>
<tr>
<td>RTU1</td>
<td>12.68</td>
<td>4.94</td>
<td>2.57</td>
<td>4.11</td>
<td>3.91</td>
<td>0.495</td>
</tr>
<tr>
<td>RTU2</td>
<td>12.28</td>
<td>4.94</td>
<td>2.49</td>
<td>2.54</td>
<td>4.45</td>
<td>0.552</td>
</tr>
</tbody>
</table>

- Initially test-bed network’s total risk was **8.65** units.
- After exponential cost resource allocation, the risk reduces to **4.98** units which is 58% of total risk.
Transfer Learning to Detect Unknown Malware

**Motivation**

- Need for techniques to detect unknown malware based on learned models from known malware which exhibit common traits.
Transfer Learning to Detect Unknown Malware

- **Approach and Research Results**
  - Developed a framework for unknown attacks detection by applying transfer learning technique based on the known attacks.
  - Developed feature-based transfer learning approach via feature spectral transformation with HeMap for detecting network attacks.
  - Improved optimization solution to enhance the accuracy of HeMap CGD and hierarchical transfer learning algorithms with clustering enhancement.

Juan Zhao, Sachin Shetty, Jan Wei Pan, “Feature-Based Transfer Learning for Network Security,” IEEE Milcom, October 2017
Juan Zhao; Sachin Shetty; Jan Wei Pan; Charles Kamhoua; Kevin Kwiat , “Transfer Learning for Detecting Unknown Network Attacks EURASIP”, Journal on Information Security, 2019 (To Appear)
Cyber Resilience using SDN

• Research Goal
  - Modeling and analysis methodology for cyber-physical dependencies in order to quantify cyber threats in Energy Delivery Systems and automatic network reconfigurations at run time to mitigate risk and provide operational resilience

• Approach
  - Risk scoring and diversity modeling using Software Defined Networks (SDN)
  - Multiple SDN controller design for cyber resilience

Modeling Cost of SDN based Security Resilience

- **Research Goal**
  - Develop cost model to select countermeasures that balances tradeoff between security risk and network QoS

- **Approach**
  - Enable dynamic managing of risk and choice of countermeasures for autonomous attack containment
  - Non-dominated sorting based multi-objective optimization framework which can be implemented within a SDN controller to address the joint problem of optimizing between security and QoS parameters


Data Provenance in Cloud using Blockchain

Goal
- Develop blockchain based data provenance capability for cloud to allow tracking of data from its creation to its current state or end state which enables transparency and accountability.
Data Provenance in Cloud using Blockchain

- Prototype on open source OwnCloud platform
- Introduced provenance feature by tracking file operation activities

Agenda

1. **COE Overview**
   - George Hsieh (PI), Norfolk State University

2. **COE Research Infrastructure and Cybersecurity Testbed**
   - George Hsieh

3. **Cyber Training, Intrusion Detection and Response**
   - George Hsieh

4. **Cyber Intelligence and Cyber Defense**
   - Sachin Shetty (Co-PI), Old Dominion University

5. **Cyber Modeling, Simulation and Decision Support**
   - Jose Padilla (Co-PI), ODU

6. **Ethical Decision Making in Cyberspace**
   - Mary Ann Hoppa (Co-PI), NSU

7. **Cyberpsychology and Human Behavior in Cyberspace**
   - Scott Debb, NSU
Research Trust 2: Context

Theories

Models <-> Data
## The Challenge

<table>
<thead>
<tr>
<th>Create</th>
<th>Create models to explore interesting dynamics in cybersecurity.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop</td>
<td>Develop theories specific to cyber.</td>
</tr>
<tr>
<td>Gather</td>
<td>Gather appropriate data to validate models and theories.</td>
</tr>
</tbody>
</table>
# The Challenge

<table>
<thead>
<tr>
<th>Create</th>
<th>Create models to explore interesting dynamics in cybersecurity.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop</td>
<td>Develop theories specific to cyber.</td>
</tr>
<tr>
<td>Gather</td>
<td>Gather appropriate data to validate models and theories.</td>
</tr>
<tr>
<td>Disseminate</td>
<td>Make simulation models and data available for reuse.</td>
</tr>
</tbody>
</table>
On Data

- **Objective**
  - Generate APT data/scenarios

- **Approach**
  - Monte Carlo Markov Chain + STIX (Structured Threat Information eXpression)

- **Results**
  - Feasible APTs

- **Publication:**
Results

- **APT MCMC**
  - Describe the state space of STIX-described APTs
  - Sample trajectories many times to identify potential APTs

- **Generated APT**
Humans in Cybersecurity

'Tricked' RSA Worker Opened Backdoor to APT Attack

Equifax Breach Caused by Lone Employee’s Error, Former C.E.O. Says

NSA case highlights growing concerns over insider threats
# Why model humans?

| Cybersecurity cannot be achieved with technology alone. | • Technology is an “arms race”.  
• Social engineering is the differentiator.  
• “Only amateurs attack machines; professionals target people” (Schneier, 2000). |
|---|---|
| People vary in their security knowledge and behaviors. | • Human behavior is complex and adaptive.  
• Modeling and simulation aid in answering “what if” questions in systems that have nonlinear relationships. |
On Models

- Modeling the attacker (insider threat)
- Human mobility as vector for malware spread
- Location prediction
- Cyberloafing
Modeling the Attacker

• **Research Question:**
  – Why do individuals choose to attack?

• **Theoretical grounding:**
  – Rational Choice Theory
  – Social Learning Theory
  – Routine Activity Theory
  – Theory of Planned Behavior

• **Model Base:**
  – Agent_Zero (Epstein, 2010)

• **Publication:**
  – Vernon-Bido et al. (2016)
Results

Model Purpose:
– Compare the influence of group size, success rate, and opportunity on the decision to attack.

Model Result:
– Opportunity showed the greatest influence in the attack decision in the model.

Next Steps:
– Incorporate learning into the model
– Examine assumptions of predisposition
– Study the environment

Average number of attacks/person by success rate and opportunity.
Malware and Mobility

• **Research Question:**
  – How could people’s mobility patterns influence the spread of malware?

• **Theoretical grounding:**
  – Contagion Theory

• **Model Base:**
  – Susceptible-Infected-Recovered (SIR) Model

• **Publication:**
  – Kavak et al. (2017)
Results

- **Model Purpose:**
  - Determine the potential extent of the spread of malware through WiFi access points.

- **Model Result:**
  - Malware rapidly spreads during the first 7 days. Encryption type and density influence the number of access points infected.

- **Next Steps:**
  - Develop data-driven human mobility model.
  - Examine the spread of malware through mobile devices connecting to open access points.

\[ \begin{align*}
S_{\text{pass1}} & \quad S_{\text{pass2}} & \quad R \\
S_{\text{WEP}} & \quad & \\
S_{\text{nopass}} & \quad I & \quad R_{\text{hidden}} \\
\end{align*} \]
Location Prediction

- **Research Question:**
  - How can we identify people’s locations through social media?

- **Data for prediction:**
  - Geo-located tweets
  - Tweet content

- **Model Base:**
  - Hu et al. (2016)

- **Publication:**
Results

• **Tweet Rate**

• **Model Purpose:**
  - Accuracy of prediction of home location

• **Model Result:**
  - 80-87% accuracy (within 100 meters).
  - 71-76% of Hu et al. (2016).

• **Next Steps:**
  - Introduce home location into malware spread study.
  - Determine work location.
Cyberloafing

• **Research Question:**
  – How could cyberloafing have an impact cybersecurity?

• **Theoretical grounding:**
  – Activities associated with cyberloafing include (Hassan, Reza and Farkhad, 2015).
  – Potential problems of cyberloafing (Conlin, 2000; Stewart, 2000).

• **Model Base:**
  – None
    – Internet addiction (Ozler and Polat, 2012,)
    – Insufficient work activities and **workload** (Askew, 2012)
    – Peer-influence (Khansa et al, 2017)
    – Boredom (Lim, 2012)
    – Self-control (Kim and Byrne, 2011)
    – Stress (Kim and Byrne, 2011)
    – **Sanctions** (Urgin and Pearson, 2013)

• **Publication:**
  – Vernon et al. (2018)
Results

• **Model Purpose:**
  - Determine what factor has greater influence in the intention to cyberloaf.

• **Model Result:**
  - Sanctions are not the most effective deterrent to cyberloafing.
  - Workload consistency appears to have the strongest influence on reducing perceived cyber risk.

• **Next Steps:**
  How can (much) cyberloafing be positive for an organization?
  How does a lower threat level lead us to a false sense of security?
On Theory

- **Research Question:**
  - How could we measure cyberloafing?

- **Theoretical grounding:**
  - Cyberloafing factors and mechanisms

- **Model Base:**
  - SD
  - Garbage can
  - SEM

- **Publication:**
  - In progress
GC Model

- Problems
- Choices
- Managers
On Dissemination

• **Research Question:**
  – How could we facilitate model reuse?

• **Theoretical grounding:**
  – Simulation, Interoperability

• **Model Base:**
  – None

• **Publication:**
  – None
Simulation Platform

- **Goal:**
  - Integrate and facilitate the modeling and reuse of socio-technical systems

- **Paradigm:**
  - ABM/DES

- **Format:**
  - Web-based/Cloud-deployed

- **Target:**
  - Non-simulationists
  - Educators
  - Policy/Decision makers
Simulation Platform (Existing)

-globals [  
  percent-similar ;; on the average, what percent of a turtle's neighbors  
  are the same color as that turtle?  
  percent-unhappy ;; what percent of the turtles are unhappy?  
]

turtles-own [  
  happy?           ;; for each turtle, indicates whether at least % -similar-wanted percent of  
  that turtle's neighbors are the same color as the turtle  
  similar-nearby ;; how many neighboring patches have a turtle with my color?  
  other-nearby ;; how many have a turtle of another color?  
  total-nearby ;; sum of previous two variables  
]

to setup  
  clear-all  
  [  
    create turtles on random patches.  
    ask patches [  
      if random 100 < density [   ;; set the occupancy density  
        sprout 1 [  
          set color one-of [red green]  
        ]  
      ]  
    ]  
  ]  
  update-turtles  
  update-globals  
  reset-ticks  
end  

;; run the model for one tick

; to go  
  if all? turtles [ happy? ] [ stop ]  
  move-unhappy-turtles  
  update-turtles  
  update-globals  
  tick  
end  

;; unhappy turtles try a new spot

to move-unhappy-turtles  
  ask turtles with [ not happy? ] [ find-new-spot ]  
end  

to find-new-spot  
  rt random-float 360  
  fd random-float 10  
  if any? other turtles-here [ find-new-spot ] ;; keep going until we find an unoccupied patch  
    move-to patch-here ;; move to center of patch  
  end  
end  

to update-turtles  
  ask turtles [  
    ;; in next two lines, we use "neighbors" to test the eight patches  
    ;; surrounding the current patch  
    ;; set similar-nearby count (turtles-on neighbors) with [ color = [ color ] of myself ]  
    ;; set other-nearby count (turtles-on neighbors) with [ color != [ color ] of myself ]  
    ;; set total-nearby similar-nearby + other-nearby  
    ;; set happy? similar-nearby >= (%-similar-wanted * total-nearby / 100)  
    ;; add visualization here  
    ;; if visualization = "old" [ set shape "default" ]  
    ;; if visualization = "square-x" [  
      ifelse happy? [ set shape "square" ] [ set shape "square-x" ]  
    ]  
  ]  
end  

to update-globals  
  let similar-neighbors sum [ similar-nearby ] of turtles  
  let total-neighbors sum [ total-nearby ] of turtles  
  set percent-similar (similar-neighbors / total-neighbors) * 100  
  set percent-unhappy (count turtles with [ not happy? ]) / (count turtles) * 100  
end

;; Copyright 1997 Uri Wilensky.  
;; See Info tab for full copyright and license.
Cyber Attacker Model (Proposed Platform)

- Reusable modules
- Tree-like diagram specification
- Online accessible
- Collaboration ready

Reusable modules

Model specification

Online execution

Workspaces (collaboration)
Modeling Contribution: GARE

![Diagram of Garbage Can Cyber Model](Diagram.png)
A former employee pleaded guilty today to a federal offense stemming from an attempted e-mail "spear-phishing" attack in January 2015 that targeted dozens of government and employee e-mail accounts.

Defendant pleaded guilty in the U.S. District Court to one count of attempted unauthorized access and intentional damage to a protected computer. In the guilty plea, defendant admitted scheming to cause damage to the computer network through e-mails that s/he believed would deliver a computer virus to particular employees. An e-mail spear-phishing attack involves crafting a convincing e-mail for selected recipients that appears to be from a trusted source and that, when opened, infects the recipient's computer with a virus.

Defendant admitted that s/he attempted to compromise, exploit, and damage U.S. government computer systems that contained sensitive nuclear weapon-related information with the intent of allowing foreign nations to gain access to that information or to damage essential systems. This former federal employee was arrested before s/he could do any damage and he now is being held accountable for actions that could have threatened our national security.

Defendant is a former U.S. Government employee who, motivated by greed, was thwarted in his attempt to sell information to a foreign intelligence service to enable a cyber-attack against our information systems,” said Assistant Director in Charge. Defendant, a U.S. citizen who had been living in Davao City in the Philippines since 2011, was terminated from employment in 2010. Defendant was detained by Philippine authorities in Manila, Philippines and deported to the United States to face U.S. criminal charges.

According to court documents, defendant initially came to the attention of the FBI in 2013 after defendant entered a foreign embassy in Manila and offered to sell a list of over 5,000 e-mail accounts of all officials, engineers and employees of a U.S. government agency. Defendant said that s/he was able to retrieve this information because s/he was an employee of a U.S. government agency’s top secret security clearance and had access to the agency’s network. Defendant asked for $15,000 for the accounts, stating they were "top secret." When asked what s/he would do if that foreign country was not interested in obtaining the U.S. government information the defendant was offering, the defendant stated s/he would offer the information to China, Iran or Venezuela, as he believed those countries would be interested in the information.

Thereafter, defendant met and corresponded with FBI undercover employees who were posing as representatives of the foreign country. During a meeting, s/he showed one of the undercover employees a list of approximately 5,000 e-mail addresses that s/he said belonged to government employees. Defendant offered to sell the information for $23,000 and said it could be used to insert a virus onto government computers, which could allow the foreign country access to agency information or could be used to otherwise shut down the government servers. The undercover employee agreed to purchase a thumb drive containing approximately 1,200 e-mail addresses of government employees; an analysis later determined that these e-mail addresses were publicly available. The undercover employee provided defendant with $5,000 in exchange for the e-mail addresses and an additional $2,000 for travel expenses.

Over the next several months, defendant corresponded regularly by e-mail with the undercover employees. A follow-up meeting with a second undercover employee took place in which defendant was paid $2,000 to cover travel-related expenses. During this meeting, defendant discussed having a list of 30,000 e-mail accounts of government employees. Defendant offered to design and send spear-phishing e-mails that could be used in a cyber-attack to damage the computer systems used by former employer. Over the next several months, the defendant identified specific conferences related to nuclear energy to use as a lure for the cyber-attack, then drafted emails advertising the conference. The emails were designed to induce the recipients to click on a link which the defendant believed contained a computer virus that would allow the foreign government to infiltrate or damage the computers of the recipients. The identified several dozen government employees whom s/he claimed to have accessed to information related to nuclear weapons or nuclear materials as targets for the attack.

Defendant sent the e-mails to the targets identified. The e-mail contained the link supplied by the FBI undercover employee which defendant believed contained a computer virus, but was, in fact, inert. Altogether, the defendant sent the e-mail s/he believed to be infected to approximately 60 government employees located at various facilities throughout the country, including laboratories associated with nuclear materials.

Defendant was detained after a meeting with the FBI undercover employee, during which defendant expected to be paid approximately $80,000 for sending the e-mails. The charge of attempted unauthorized access and intentional damage to a protected computer carries a maximum sentence of 10 years in prison and potential financial penalties. Under the advisory federal sentencing guidelines, defendant faces a prison term of 24 to 30 months and a fine of up to $95,000.

SD

Relationship
1. **COE Overview**  
   – George Hsieh (PI), Norfolk State University

2. **COE Research Infrastructure and Cybersecurity Testbed**  
   – George Hsieh

3. **Cyber Training, Intrusion Detection and Response**  
   – George Hsieh

4. **Cyber Intelligence and Cyber Defense**  
   – Sachin Shetty (Co-PI), Old Dominion University

5. **Cyber Modeling, Simulation and Decision Support**  
   – Jose Padilla (Co-PI), ODU

6. **Ethical Decision Making in Cyberspace**  
   – Mary Ann Hoppa (Co-PI), NSU

7. **Cyberpsychology and Human Behavior in Cyberspace**  
   – Scott Debb, NSU
Ethical Cybersecurity Decision-Making

- MLRCP-funded research in 2018
- Aiming for two follow-on publications this year
  - Framework
  - Cybersecurity Code of ethics tenets recommendations
- Lessons-learned
  - There is no code of ethics for cybersecurity professionals
  - Algorithms can reflect the biases of their human creators
  - *The Professional Ethics Toolkit* (Meyers) is a good starting point for addressing the “say-do” gap in the classroom or in the workplace
Status: Outreach

• **Individual & group networking**
  – VA Air & Space Museum; Jefferson Lab; KBR Wyle

• **Continue to grow internship relationships & student mentoring**

• **Support upcoming Cyberpsychology conference (Summer 2019)**

• **Lessons-learned**
  – Keep “quid pro quo” in mind; make commitments reasonable
  – A better centralized method for opportunity dissemination is needed
  – Collect/share lessons-learned to document & improve internship programs / experiences
  – Leverage efforts of NSU Cybersecurity Center leadership
Capacity Building and Sustainment

• COEcyber operations and support
  – **Goal**: Partner with and recruit the highest quality research faculty, staff and students.
  – **Lessons-learned**
    – Competition is stiff for the best candidates
    – Citizenship continues to be an issue
    – Publications / presentations must be a priority or they won’t happen
    – Capstone candidates benefit from more training/support to produce high-quality projects

• MS Cybersecurity
  – **Goal**: Increase number and quality of graduates (approx. 30 per year)
  – **Lessons-learned**
    – “Career changers” need better transition support
    – High quality capstones require more time
    – Certificates may be more appropriate for some candidates

• Funding
  – **Goal**: Successfully compete and deliver upon new relevant funding opportunities to ensure self-sustainment
Agenda

1. COE Overview
   – George Hsieh (PI), Norfolk State University

2. Cybersecurity Testbed
   – George Hsieh

3. Cyber Training, Intrusion Detection and Response
   – George Hsieh

4. Cyber Intelligence and Cyber Defense
   – Sachin Shetty (Co-PI), Old Dominion University

5. Cyber Modeling, Simulation and Decision Support
   – Jose Padilla (Co-PI), ODU

6. Ethical Decision Making in Cyberspace
   – Mary Ann Hoppa (Co-PI), NSU

7. Cyberpsychology and Human Behavior in Cyberspace
   – Scott Debb, NSU
• **M.S. CyberPsychology**
  – Proposed MS CyberPsychology degree, approved by NSU BOV
  – Currently under SCHEV review
  – Anticipated start date: Fall 2019
  – 2.5 year fully online research-based program
  – Would be the first cyberpsychology graduate degree program in the US

• **CYPSY24**
  – NSU to host the 24\textsuperscript{th} Annual Cyberpsychology, Cybertherapy and Social Networking conference June 24-26
  – Internationally recognized premier cyberpsychology conference
  – First HBCU to host CYPSY
  – 3 Keynotes:
    – Grainne Kirwan: Forensic Cyberpsychology (IADT, Ireland)
    – Lee Hadlington: Cyberecognition & Security in Cyberspace (Demonfort Univ., UK)
    – Mark Derriso: Human-Machine Communication (AFRL, USA)
CyberPsychology @ NSU

Applied Research

• Gen Z’s Attitudes Towards Cybersecurity
  – Examining attitudes towards basic cybersecurity practices and areas of awareness
  – Age & ethnicity-based comparisons (oversampling of AA)
  – Personality factors as moderating variables
  – Online Security Behavior and Beliefs questionnaire (Li et al., ODU / NC A&T)

• Social Media use & Social Support
  – Collaborating with University of Sydney (Australia)
  – Cross-cultural comparisons—US, UK, AUS

• Ethical Decision Making
  – Examining overlapping constructs with cybersecurity codes of ethics
  – Application of ethics standards to potential automated procedures for ethical advising in real time

• Cognitive Dissonance
  – Decision making in the context of adhering to cybersecurity best-practices
  – Currently waiting for IRB approval for lab-based EEG / Eye Tracking study

• Online self presentation
  – Assessment of AA/Gen Z perception of how they present themselves online vs. offline
  – Cross cultural comparisons—US, UK, Saudi Arabia
• COE in Cyber Security has established strong foundation for CASE-V platform and targeted components

• COE is ready to accelerate its development and usage of the CASE-V testbed

• COE is ready to start collaboration with selected external research partners on developing and using the CASE-V testbed (or its components implemented on separate environments)

• COE plans to put more emphases on machine learning, IoBT security, and warfighters behavior in cyberspace

• COE will continue to expand its strategic partnerships and contribution to internship and workforce development activities

COE in Cyber Security sincerely appreciates the support and guidance from our DoD partners
Contact Information

- George Hsieh, PI, Computer Science, NSU, 757-823-8313, ghsieh@nsu.edu
- Mary Ann Hoppa, Co-PI, Computer Science, NSU, 757-823-8654, mahoppa@nsu.edu
- Sachin Shetty, Co-PI, VMASC & MSVE, ODU, 757-686-6233, sshetty@odu.edu
- Jose Padilla, Co-PI, VMASC, ODU, 757-686-6213, jpadilla@odu.edu
- Scott Debb, Faculty Researcher, Psychology, NSU, 757-823-8943, smdebb@nsu.edu
- Jonathan Graham, Co-PI, Computer Science, NSU, 757-823-9445, jmgraham@nsu.edu