CySIS Research
Paulo Shakarian, CySIS Laboratory Director
What is CySIS?

The CySIS Lab is primarily focused on conducting basic research relating to challenging problems in cyber security, social network mining, security informatics, and artificial intelligence with the goal of creating intelligent systems that have a significant impact on real-world problems.
Moving Beyond “Typical” Academic Research

CySIS was designed from the ground up to create technology that can transition to real-world use.

- **Use-inspired research.** We look to tackle difficult problems pulled directly from real-life scenarios

- **Continual theory-application though process.** What are the theoretical challenges that, if overcome will lead to significant application improvements? What do we learn from studying the applications that can drive theory.

- **Rigorously tested prototypes.** Much computer science research relies on “standard” datasets for testing – we look to move beyond these standard datasets to conduct experiments that more closely resemble the real world.
Why CySIS Tech

Local government/law enforcement
◊ Learn about technology that can help with your mission

Entrepreneurs/businesses
◊ Learn about our technology licensing opportunities

Technologists
◊ Learn how artificial intelligence can impact cyber-security and social media
Major Application Areas

Cyber Attribution
- Hacker forum mining
- Understanding hacktivism

Exploit markets
- Viral cascade prediction
- Diffusion inhibition

Cyber Security
- Understanding social influence

Law Enforcement and Military
- Violence prediction
- Malware analysis
- Causal analysis of ISIS

Social Media
- Extremist groups in social media
- Missing persons Intelligence Synthesis Toolkit
<table>
<thead>
<tr>
<th>Count</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Conference papers accepted</td>
<td>Including KDD, ASONAM, ICCM, and CIKM</td>
</tr>
<tr>
<td>6</td>
<td>Journal papers submitted</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Invention disclosures</td>
<td>3 provisional patents</td>
</tr>
<tr>
<td>3</td>
<td>Book chapters submitted</td>
<td>2 published</td>
</tr>
<tr>
<td>2</td>
<td>Books published</td>
<td><em>Diffusion in Social Networks</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Cyber warfare: Building a Scientific Foundation</em></td>
</tr>
</tbody>
</table>
Funding Going Forward

6 grant awards this year from a variety of funders:
- ASU Global Security Initiative
- FindMeGroup
- Army Research Office
- Office of Naval Research
- Air Force Office of Scientific Research
- DoD Minerva
Malware Task Identification

- Given a piece of malware, can we identify what it does?
- We combine dynamic malware analysis with cognitive models to emulate a human malware analyst.
- High precision and recall on numerous datasets – outperform the state of the art commercial offering.
Violence Prediction

- Given a social network derived from arrests of criminal gang members, can we predict violent offenders?
- Tough problem – violent human activities inherently difficult to predict and relatively rare (when compared to other crimes)
- Currently employed analytical methods by the Chicago police provide low precision and recall.
- Features relying on social network topology proved to be more powerful than geographic or temporal features.
Predicting Viral Cascades

Can we predict information cascades in social media that will increase ten-fold?

This problem is difficult because the relationship between cascade size and frequency follow a power-law – cascades that grow order-of-magnitude or greater are very rare.

We create measurements based on the community structure of those who adopted and show it provides a leading indicator of cascade growth.
Cyber attribution

We study capture-the-flag data to develop algorithms and methods for cyber-attribution as it provides real ground truth.

Using a variety of standard machine learning techniques, we find that deceptive activity causes the majority of the mis-classified cases.

We are currently using defeasible logic as a technique to better identify deception.

For more information, see the poster at the break.

Simari, G., Shakarian, P., Falappa, M., AMAI, 2015
Data-driven study of ISIS

We study over 2,200 ISIS combat incidents to create rules that describe their tactical behaviors.

To avoid spurious correlations, we borrow ideas from causal reasoning to extract if-then temporal relationships that move beyond correlation.

We uncovered interesting relationships that provide novel insight into ISIS behavior.

*For more information, see the poster at the break.*

\[ \epsilon_{avg} = \frac{\sum_{r' \in R(r)} p_{r,r'} - p_{\neg r,r'}}{|R(r)|} \]

\[ r \equiv c \leftrightarrow p \mapsto g \]
Books

Published by Elsevier and currently available

*Introduction to Cyber-Warfare*

A collection of Cyber-Warfare case studies where the relevant technical, social, political, and military issues are addressed.

Covers cyber-attack, espionage, and infrastructure attack, including details on Stuxnet, Gauss, the attacks on Saudi Aramco, and others.

Currently used as a text at Naval Postgraduate School.

9 out of 10 rating on Slashdot
In Fall, 2015, Springer will be publishing a new volume:

**Diffusion in Social Networks**

Provides an in-depth overview of social network diffusion based on perspectives from the following fields:

- Data mining
- Artificial intelligence
- Epidemiology
- Physics
- Theoretical biology

A preprint, along with companion slides can be found at: [http://lab.engineering.asu.edu/cysis/diffusion/](http://lab.engineering.asu.edu/cysis/diffusion/)
- Trusted and privacy preserving data processing and analysis,
- Real-time data processing and analysis,
- Parallel and distributed data processing and analysis, and
- High dimensional and multi-modal data processing and analysis, into new key technology elements whose different instantiations are deployed for direct impact to various industries, including energy, healthcare, security, and finance.

- Collaborative federally funded research
  - Industry funded research
  - Data (analysis, management) services

- Industrial Advisor Board (IAB) driven research
- Industry-funded pre-competitive research
- Internship opportunities

http://cascaderesearch.org
GLOBAL SECURITY INITIATIVE

A university-wide interdisciplinary hub for global security research

VISION: A security and intelligence landscape transformed through interdisciplinary research and discovery, in which defense, development and diplomacy operate collaboratively to drive positive outcomes for complex global challenges.

GSI is sponsoring the Cybersecurity and Digital Forensics Center, bringing together multidisciplinary subject matter experts to define the new frontiers of cyber defense technology and examine the impact on laws, policy, and society.
Questions?
shak@asu.edu