2nd Cyber Security Workshop

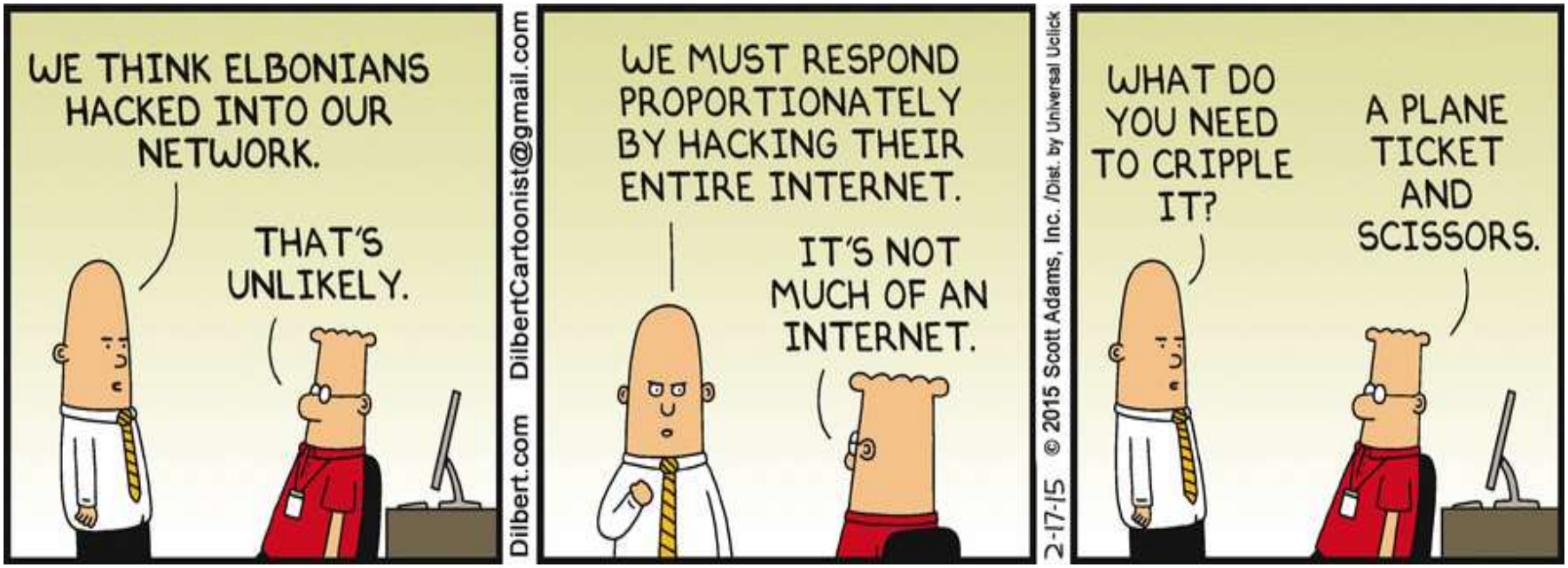
Academia Panel: Research Transforming Cyber T&E

Moderator: Dr. John B. Foulkes, JBF Consulting LLC

Panelists:

- *Dr. Kevin Fall, Software Engineering Institute, Carnegie Mellon University*
- *Dr. Bharat B. Madan, Old Dominion University*
- *Dr. Jeff McNeil, Professor, Clemson University CBBS*
- *Dr. Robin Poston, FedEx Institute, University of Memphis*
- *Dr. James Riordan, Cyber Systems and Technology, MIT Lincoln Laboratory*
- *Dr. Fred Wright, Cyber Technology and Information Security Laboratory, Georgia Tech Research Institute*

Academia Panel: Research Transforming Cyber T&E



Academia Panel: Research Transforming Cyber T&E

Panel Theme:

Increased attention to proactive approaches to cyber security is needed. It starts with research.

While much attention has being given to the development of cyber security products, increasing efforts in "upstream" research can help predict anomalies and intrusions and thus better support the product developers who are building the next great "firewalls" and "encryption devices".

Academia Panel: Research Transforming Cyber T&E

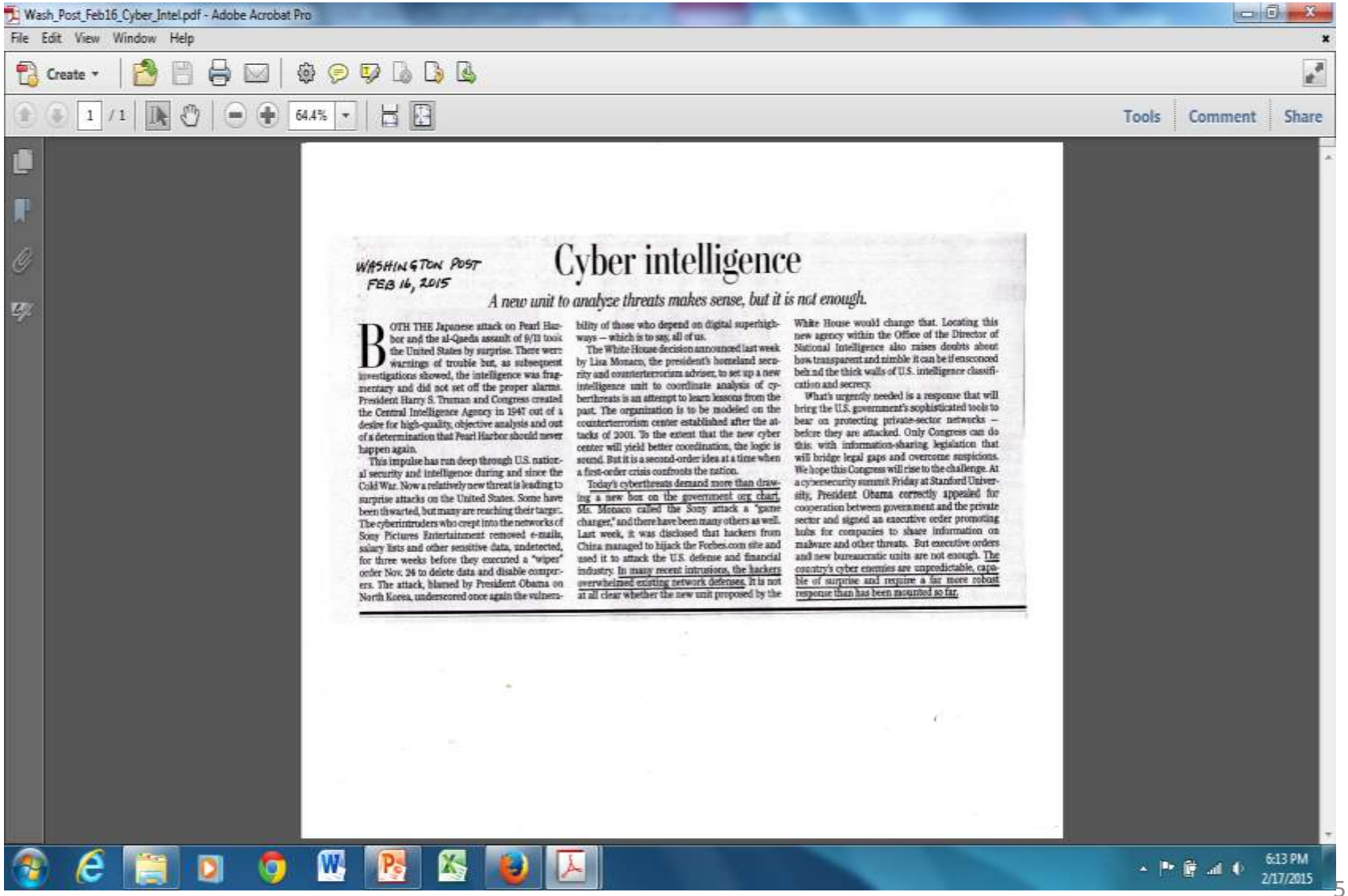
In order to better understand and forecast the behavior of systems under intrusion and attack, discussion will be centered around the following topics:

- ***What are some of the recent and ongoing academic/research study efforts, including math and S&T models and tools?***

- ***What are the current research areas, and what are some examples of ongoing research and concept development?***

- ***What are some of the challenges regarding the "downstream" impacts of research on cyber security product development, including impacts on test infrastructure, test methods and procedures, evaluation metrics and criteria development, and product evaluation?***

Academia Panel: Research Transforming Cyber T&E



Academia Panel: Research Transforming Cyber T&E

Washington Post: February 16, 2015:
Quotes from the *Cyber Intelligence* article:

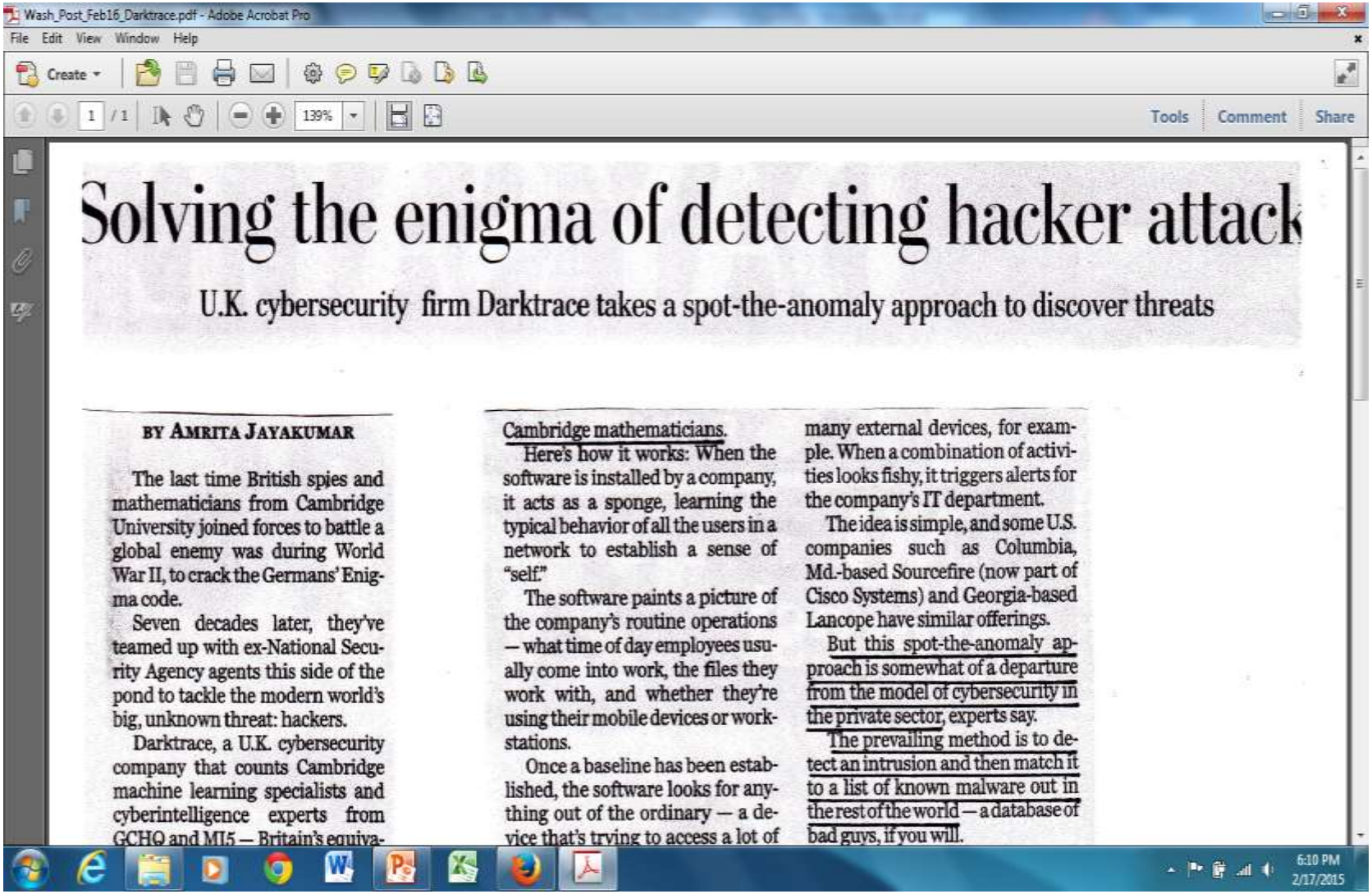
"But it (new cyber center) is a second order idea at a time when a first-order crisis confronts the nation."

"Today's cyber threats demand more than drawing a new box on the government org chart."

"In many recent intrusions, the hackers overwhelmed existing network defenses."

"Bring tools to bear on protecting private-sector networks – before they are attacked".

Academia Panel: Research Transforming Cyber T&E



Academia Panel: Research Transforming Cyber T&E

Washington Post, February 16, 2015:
Quotes from the *Darktrace* article:

"The last time British spies and mathematicians from Cambridge University joined forces to battle a global enemy was during World War II, to crack the Germans' Enigma code."

"The company's software was designed to get ahead of an attack instead of cleaning up quickly after the fact."

"Darktrace's flagship product is the Enterprise Immune System, so named because it mimics the behavior of the human immune system using algorithms developed by Cambridge mathematicians."

"But this spot-the-anomaly approach is somewhat of a departure from the model of cyber security in the private sector… The prevailing method is to detect an intrusion and then match it to a list of known malware……"

"Companies are still a long way off from being proactive about cyber security…"

Academia Panel: Research Transforming Cyber T&E

A number of college/universities offering degrees and certificates in Cyber Security, Cyber Security Policy, and similar fields require minimal formal prerequisite coursework in Mathematics/Operations Research.

In many instances, the only prerequisite is Intermediate Algebra.

Current academic research areas include:

- ***Cyber-attack/anomaly detection for computers and network systems***
- ***Projecting Cyber-attacks***
- ***Pattern recognition and behavior detection***
- ***Forecasting distributed denial of service (DDOS) attacks***

Academia Panel: Research Transforming Cyber T&E

Research regarding cyber security issues is actually a special case of the larger field of Risk Assessment and Decision Analysis; that is, how one analyzes a problem, determines the risks involved for a variety of potential courses of action, and chooses an appropriate (i.e., "optimal") decision.

For malicious attacks on computers and computer networks, one needs to understand and recognize the causes behind the behavior patterns of such attacks, enabling the formulation of a mathematical models to predict the likelihood (and success) of certain responses to the attacks.

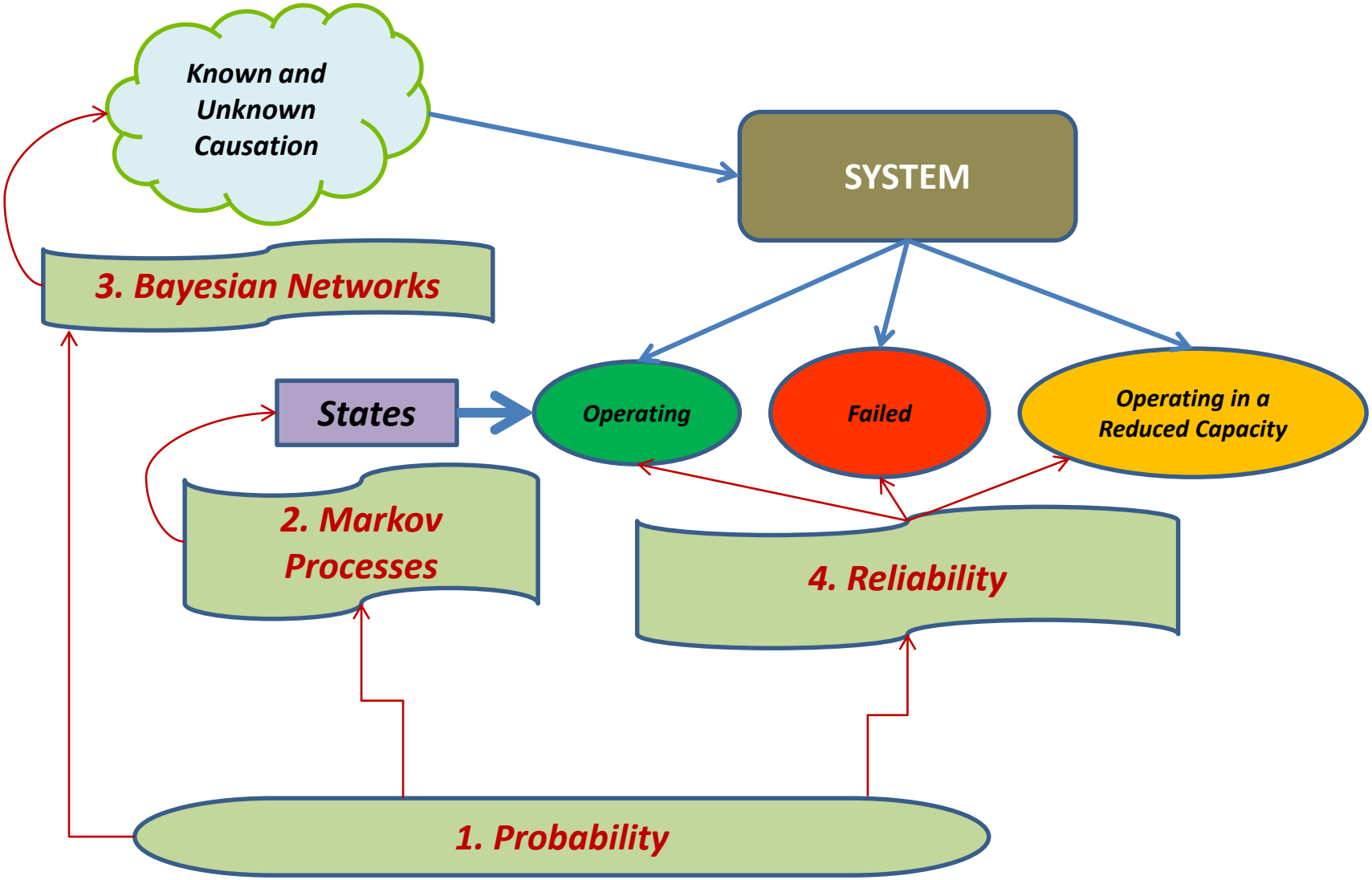
Academia Panel: Research Transforming Cyber T&E

Whether it's dealing with malicious attacks of computers or computer networks; understanding and controlling the spread of diseases, or managing investments of a major financial institution, the foundations of understanding these problems and formulating procedures for dealing with them require a strong mathematical foundation.

These include:

- ***Understanding the likelihood of future events (Probability Theory);***
- ***Understanding the causes and effects of system behavior (Markov Processes and Bayesian Networks);***
- ***Understanding and predicting the operation (or failure) of systems (Reliability Theory).***

Elements of Risk Assessment for Decision Analysis



Academia Panel: Research Transforming Cyber T&E

The following charts contain a sample of some the more recent research papers in the field of Cyber Security. The purpose is to illustrate that much of the current research involves the topics mentioned on the previous chart.

"Projecting Cyber-attacks Through Variable-Length Markov Models"; Daniel S. Fava, Stephen R. Byers, Student Member, IEEE, and Shanchieh Jay Yang, Member, IEEE (IEEE Transactions on Information Forensics and Security, September 2008)

- ***Presents a VLMM that captures the sequential properties of attack tracks, allowing for the prediction of likely future actions on ongoing attacks; it is able to adapt to newly observed attack sequences without requiring specific network information.***

"Robustness of the Markov-Chain Model for Cyber-Attack Detection"; Nong Ye, Senior Member, IEEE, Yebin Zhang, and Connie M. Borror (IEEE Transactions on Reliability, March 2004)

- ***Presents a cyber-attack detection technique through anomaly-detection, and discusses the robustness of the modeling technique employed. In this technique, a Markov-chain model represents a profile of computer-event transitions in a normal/usual operating condition of a computer and network system (a norm profile).***

Academia Panel: Research Transforming Cyber T&E

"Behavior Detection Using Confidence Intervals of Hidden Markov Models"; Richard R. Brooks, Senior Member, IEEE, Jason M. Schwier, and Christopher Griffin, Member, IEEE (IEEE Transactions on Systems, Part B: Cybernetics, December, 2009)

- ***Uses confidence intervals for HMM analysis; enables consideration of the number of data samples available when comparing an HMM model with a sensor data stream; uses a novel approach in applying receiver operating characteristic (ROC) curves to find detection thresholds when confidence intervals are used.***

"An Introduction to Hidden Markov Models and Bayesian Networks"; Zoubin Ghahramani, Gatsby Computational Neuroscience Unit, University College London, London, England (2001, International Journal of Pattern Recognition and Artificial Intelligence.)

- ***Shows that Hidden Markov Models (HMMs) are a special case of Bayesian Networks, thus relating them to more complex and interesting models and thus discuss general solutions to the problems of approximate inference, parameter learning, and model selection.***

Academia Panel: Research Transforming Cyber T&E

Bottom Line:

Much of the current academic research in the area of cyber security involves the basic ingredients of risk assessment:

- ***Probability Theory***
- ***Markov Processes***
- ***Bayesian Networks***
- ***Reliability Theory***

Undergraduate/graduate curricula in support of programs aiming towards Cyber Security degrees or certificates should include exposure to Operations Research-type courses such as these four mentioned above.