A Developing Science of Cyber Security – an Opportunity for Model Based Engineering & Design

July 27, 2017

Jerry M. Couretas, PhD
About Me - Cyber Modeling and Simulation

• Editor-in-Chief of the Journal of Defense Modeling and Simulation
  – 7/2017 Cyber M&S Special Issue
  – 1/2018 Cyber Special Issue on Developing Science of Cyber Security

• PhD from Dr. B.P. Zeigler at the University of Arizona’s Artificial Intelligence and Simulation Lab
Hackers Are Targeting Nuclear Plants, U.S. Says

By NICOLE PERLROTH

Since May, hackers have been penetrating the computer networks of companies that operate nuclear power stations and other energy facilities, as well as manufacturing plants in the United States and other countries.

Among the companies targeted was the Wolf Creek Nuclear Operating Corporation, which runs a nuclear power plant near Burlington, Kan., according to security consultants and an urgent joint report issued by the Department of Homeland Security and the Federal Bureau of Investigation last week.

The joint report was obtained by The New York Times and confirmed by security specialists who have been responding to the attacks. It carried an urgent amber warning, the second-highest rating for the severity of the threat.

The report did not indicate whether the cyberattacks were an attempt at espionage — such as stealing industrial secrets — or part of a plan to cause destruction. There is no indication that hackers were able to jump from their victims’ computers into the control systems that operate critical infrastructure.

The Wolf Creek nuclear plant in Kansas in 2000. Its operator was targeted by hackers.

cause of confidentiality agreements.

The origins of the hackers are not known. But the report indicated that an “advanced persistent threat” targeted their victims’ internet traffic through their own machines.

Energy, nuclear and critical manufacturing organizations directed their victims’ internet traffic through their own machines. “We never anticipated that critical infrastructure control systems would be facing advanced levels of malware,” Wellinghoff said.
### Infrastructure Characteristics

<table>
<thead>
<tr>
<th>Complexity</th>
<th>Electricity</th>
<th>Gas</th>
<th>Railways</th>
<th>ICT</th>
<th>Urban Water</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organisational</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Speed of change</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dependence (interconnectedness)</th>
<th>Electricity</th>
<th>Gas</th>
<th>Railways</th>
<th>ICT</th>
<th>Urban Water</th>
</tr>
</thead>
<tbody>
<tr>
<td>On other infrastructures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>For other infrastructures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intra-infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICT control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Electricity</th>
<th>Gas</th>
<th>Railways</th>
<th>ICT</th>
<th>Urban Water</th>
</tr>
</thead>
<tbody>
<tr>
<td>External impact*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical/human failure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber attacks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terrorist target</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Market environment</th>
<th>Electricity</th>
<th>Gas</th>
<th>Railways</th>
<th>ICT</th>
<th>Urban Water</th>
</tr>
</thead>
<tbody>
<tr>
<td>Degree of liberalisation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inadequacy of control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Speed of change</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Degree of Criticality Factors

<table>
<thead>
<tr>
<th>Degree of criticality factors</th>
<th>Scope**</th>
<th>Magnitude</th>
<th>Effects of time</th>
</tr>
</thead>
</table>

### Overall Degree of Criticality
Cyber in the News (Stoplight Charts)

M&S Work

NASA Technological Readiness Levels (TRLs)
Contents

• Science of Cyber Security
• Developing Communities
• Cyber Risk Evaluation & Assessment
• Cyber Model Example
• Current Evaluations
• Developing Work
• Wrap Up
Contents

- Science of Cyber Security
- Developing Communities
- Cyber Risk Evaluation & Assessment
- Cyber Model Example
- Current Evaluations
- Developing Work
- Wrap Up
The Scientific Underpinnings of Cybersecurity

A science of security will develop

– a body of scientific laws

– testable explanations

– confirmation or validation of predicted outcomes

1 https://mail.google.com/mail/u/0/#search/nas/15c758e80b12d023
Scientific Approach to Cybersecurity

There are strong and well-developed bases in the contributing disciplines:

- mathematics and computer science
- human sciences

A scientific approach to cybersecurity challenges expands understanding of

- systems
- defenses
- attacks
- adversaries

National Academy of Science & Cyber Research

Findings included

– Interdisciplinary program examples – U of Bochum

– Questions current research
  • High frequency publishing vs quality
  • Enabling results

– Longer research projects may help

¹ https://mail.google.com/mail/u/0/#search/nas/15c758e80b12d023
Example Transitions from Art to Science

- **Cyber Security Science**
  - 1700s–1960s – complex industrial systems with integrated timing handled by respective operators
  - 1960s–1980s – Systems Theory (e.g., Wymore, Zeigler …) texts introduced
  - 1990s–2000s – micro computers increased number of entities to point where scale and scope of new systems introduce overall security / safety issues
  - Early 2000s–present – “cyber” introduced as topic in security circles
  - Next step?

- **Computer Science**
  - Pre History – 1930s – “computer” was a person who used various devices (e.g., Abacus, analytical engine, etc.)
  - 1930s–1950s – algorithms (e.g., Church-Turing, …), N. Wiener’s “Cybernetics,” identified as independent domain
  - 1950s–1970s – development of computer science curricula and specialized literature (e.g., first PhD ~ 1965)
  - 1970s–present – “Computer Science” with provable hypotheses

- **Material Science**
  - Pre History to 17th Century – Alchemy
  - 17th Century – 1960s – Metallurgy
  - 1960s–present - Material Science
  - Still recipe based
We have built high risk, complex systems, for new domains

Hard Problems are what M&S is For
Contents

• Science of Cyber Security

• Developing Communities

• Cyber Risk Evaluation & Assessment

• Cyber Model Example

• Current Evaluations

• Developing Work

• Wrap Up
Cyber Mission M&S Communities

Mission Operators

Assured Operations

Cyber Professionals

Cyber for Others

Cyber for Cyber
Cyber for Others, C4O

- Recognise cyber attack indicators
- React – call C4C
Cyber for Cyber, C4C

- Block network attacks
- Mitigate network attacks
- Reconstitute networks
Military Activities & Cyber Effects (MACE)¹

<table>
<thead>
<tr>
<th>Cyber Effects (C4C)</th>
<th>Military Effects (C4O)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Deny</td>
</tr>
<tr>
<td>Interruption</td>
<td>✓</td>
</tr>
<tr>
<td>Modification</td>
<td>✓</td>
</tr>
<tr>
<td>Degradation</td>
<td>✗</td>
</tr>
<tr>
<td>Fabrication</td>
<td>✓</td>
</tr>
<tr>
<td>Interception</td>
<td>✗</td>
</tr>
</tbody>
</table>

¹ Bernier, M. (2015). Cyber Effects Categorization - The MACE Taxonomy. DRDC Center for Operational Research and Analysis. TTCP JSA TP3 Cyber Analysis
Example Cyber Mission Use of Standards

• OASIS standards address IA to **protect**
  • CybOX (Cyber Observable eXpression)
    – STIX (Structured Threat Information eXpression)
    – TAXII (Trusted Automated eXchange of Indicator Information)

• **Cyber Range Interoperability Standard (CRIS) for connect different range emulations**¹
  - SISO Training Standards

Contents

• Science of Cyber Security
• Developing Communities
• Cyber Risk Evaluation & Assessment
• Cyber Model Example
• Current Evaluations
• Developing Work
• Wrap Up
2015 Business Blackout

Lloyd’s of London scenario looked at a U.S. power grid failure

… and, while a major cyber attack is unlikely …

Cyber attacks, including against industrial control systems, are a continuing phenomena
Hijo, no todo es mejor con Wireless
Böhme & Schwartz (2010) provide an excellent summary of cyber insurance literature and define a unified model of cyber insurance that consists of 5 components:

- the networked environment
- demand side
- supply side
- information structure
- organizational environment

In addition, the defining characteristics of cyber insurance are

- interdependent security
- correlated failure
- information asymmetry
Example Cyber Measurement Models

• Factor Analysis of Information Risk (FAIR) Model \(^1\)

• “How to Measure Anything in Cyber Security Risk”\(^2\)

1 \(\text{http://www.fairinstitute.org/}\)
2 \(\text{http://www.howtomeasureanything.com/cybersecurity}\)
To ensure that Spain uses Information and Telecommunications Systems securely, by strengthening prevention, defence, detection, analysis, investigation, recovery and response capabilities vis-à-vis cyber attack.

**OVERALL OBJECTIVE**

---

**OBJECTIVE I**

To ensure that the Information and Telecommunications Systems used by the Public Authorities have the appropriate level of cyber security and resilience.

**OBJECTIVE II**

To foster the security and resilience of the Information and Telecommunications Systems used by the business sector in general and operators of Critical Infrastructures in particular.

**OBJECTIVE III**

To enhance prevention, detection, reaction, analysis, recovery, response, investigation and coordination capabilities vis-à-vis terrorist activities and crime in cyberspace.

**OBJECTIVE IV**

To raise the awareness of citizens, professionals, companies and Spanish Public Authorities about the risks derived from cyberspace.

**OBJECTIVE V**

To gain and maintain the knowledge, skills, experience and technological capabilities Spain needs to underpin all the cyber security objectives.

**OBJECTIVE VI**

To contribute to improving cyber security in the international sphere.
Contents

- Science of Cyber Security
- Developing Communities
- Cyber Risk Evaluation & Assessment
- Cyber Model Example
- Current Evaluations
- Developing Work
- Wrap Up
Cyber Model Example - Introduction

• Build Enterprise Description Model

• Use Analytic Model
Enterprise Model

People manage enterprise due to the scope of information

1 http://www.itl.nist.gov/div898/handbook/apr/secUon1/apr161.htm
Enterprise Model Construction & Evaluation

Data Discovery
- Interviews & Surveys
- Network Data
- ...

Structure Data
(e.g., People, Process & Tool domains)

Entity Relation Model of “As Is” Enterprise

Estimate Failure Rates For each Domain

Model with Rates assigned To each Domain

Combine Failure Rates for Overall Vulnerability Estimate

Enterprise Cyber Risk Estimate

Authoritative Data
- 2013 OT&E AR
- Verizon report
- McAfee / Symantec

Data to Rates
- Annual Occurrences

Strategy Alternatives
- Cost
- Timeliness
- Effectiveness

Strategy Evaluation

Policy
Training
Technology

Metrics
- Dollar quantifiable (e.g., Target, Nieman Marcus …)
- Media quantifiable (e.g., Snowden, Manning) – number of articles / exposure
Use the Q&A process to develop an information structure amenable to modeling:

<table>
<thead>
<tr>
<th>People</th>
<th>Processes</th>
<th>Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Who</strong></td>
<td>System Access</td>
<td>User Authentication</td>
</tr>
<tr>
<td><strong>What</strong></td>
<td>Personally Identifiable Information (PII)</td>
<td>Critical Information</td>
</tr>
<tr>
<td></td>
<td>Social Media</td>
<td>High Volume (e.g., manufacturing)</td>
</tr>
<tr>
<td><strong>When</strong></td>
<td>System Access</td>
<td>Maintenance Schedule</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Patch Schedule</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Software Updates</td>
</tr>
<tr>
<td><strong>Where</strong></td>
<td>Fixed Site</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mobile</td>
<td></td>
</tr>
<tr>
<td><strong>Why</strong></td>
<td>Business System access</td>
<td>Secure Sockets Layer (SSL)</td>
</tr>
<tr>
<td></td>
<td>Technology System Access</td>
<td></td>
</tr>
<tr>
<td><strong>How</strong></td>
<td>Recruiting</td>
<td>Security Architecture Level</td>
</tr>
<tr>
<td></td>
<td>Screening</td>
<td>Firewall – monitoring &amp; control</td>
</tr>
</tbody>
</table>
Enterprise Model & Parameterization
(organize respective failure rate estimates)

\[
\lambda_{\text{enterprise vulnerability}} = \lambda_{\text{people}} \text{ AND } \lambda_{\text{process}} \text{ AND } \lambda_{\text{tools}}
\]

- \(\lambda\) is the failure rate for the respective domain (e.g., people, process, tool) or one of its components

- Exponential distribution results in “additive” combination of failure rates over the heterogeneous data for the respective domains
“As Is” Risk Estimation
(Strategy – “Do Nothing”)

Time (months) vs. Mean Time to Exploit (MTTE)
(Strategy: Do Nothing)
## Example Countermeasures as Work Packages

<table>
<thead>
<tr>
<th>Packages / Domain &amp; Work Package</th>
<th>Cyber Enterprise Domain Affected by Work Packages</th>
<th>Work Package Time / Cost Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>People ($λ_{people}$) Process ($λ_{process}$) Tool ($λ_{tool}$)</td>
<td>Implementation Time</td>
</tr>
<tr>
<td><strong>Work Packages</strong></td>
<td></td>
<td>months</td>
</tr>
<tr>
<td>Access</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td>Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Device</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Critical Information</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Phishing</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td><strong>Training</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet Use</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Firewalls</td>
<td>○</td>
<td>●</td>
</tr>
<tr>
<td><strong>Technology</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M&amp;C</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Authentication</td>
<td>●</td>
<td>○</td>
</tr>
</tbody>
</table>

- Work Packages provided as policy / training / technology “fixes” and affect cyber enterprise domains (i.e., people, processes and tools) independently.
- Independent Work Package provision results in ready project plans in terms of time and cost estimates for improving enterprise resilience.
Model Based ↔ Knowledge based

Enterprise
(Information Asset View)

People
- Access to Critical Information
- Mobile Access (e.g., BYOD)
- Recruiting

Processes
- Manufacturing (i.e., value-add)
- Procurement
- Communications

Tools / Technology
- Firewalls (e.g., OSI Layers & Packet Inspection)
- Security Architecture Level
- Authentication System

Contents

• Science of Cyber Security
• Developing Communities
• Cyber Risk Evaluation & Assessment
• Cyber Model Example
• Current Evaluations
• Developing Work
• Wrap Up
Nissan Quest / Ford Villager

- 7 Prototype builds
- 1000s of hours of testing / evaluation

Death Valley Hot Weather Testing

Bemidji MN Cold Weather Testing
Cyber M&S / Test Example

Network Emulation (StealthNet) injection into Network System Under Test (NSUT)

Cyber-Range Event Process Overview

**Plan & Design**
- Event Goals
- Event Scenarios (MSEL)
- Event Environment
- Metrics

**Deploy**
- Cyber Ranges and Capabilities
- Cyber Range Support Tools
- Data Collection Plan

**Execute**
- Logical Range
- Event
- Sites/Participants
- Control Plane
- Instrumentation Plane

**Analyze**
- Collected Event Data
Cyber Operations Architecture Training System (COATS)¹

Inject Cyber Range effects into Command Staff training simulations

“I’m no expert, but I think it’s some kind of cyber attack!”
Contents

• Science of Cyber Security
• Developing Communities
• Cyber Risk Evaluation & Assessment
• Cyber Model Example
• Current Evaluations
• Developing Work
• Wrap Up
Cyber Mission Representation (DoD SBIR Conf – 2013)

Two major subspaces of cyber M&S problems
MITRE & ATT@CK Framework

- ATT@CK provides decomposition of cyber attack cycle
- CARET\(^2\) expands ATT@CK to give more context on tactics, tools and threat groups

1. https://attack.mitre.org/wiki/Main_Page
2. https://car.mitre.org/caret/#/
Security Metrics

Alarm Correlation And Attack Response

Network Hardening

Cauldron
Analyzing Mission Impacts of Cyber Actions (AMICA)\(^1\)\(^2\)

For mission analysts, we seek to answer mission impact questions

For cyber defenders and analysts, we consider security posture

---

\(^1\) 2015 NATO IST 128 Workshop (https://pdfs.semanticscholar.org/ff89/1d6348e2e2f01b3eef52126b45c64110a0a1.pdf)

\(^2\) http://csis.gmu.edu/noel/pubs/2015_AMICA.pdf
Contents

• Science of Cyber Security
• Developing Communities
• Cyber Risk Evaluation & Assessment
• Cyber Model Example
• Current Evaluations
• Developing Work
• Wrap Up
<table>
<thead>
<tr>
<th>Cyber Threads</th>
<th>Examples</th>
</tr>
</thead>
</table>
| People             | • Mission Operators  
                     • Cyber Security Professionals  
                     • M&S Professionals that help design secure cyber systems |
| Process            | • Insurance Evaluation  
                     • Assessment Frameworks  
                     • Knowledge Based Design  
                     • Range Testing  
                     • Modeling Process for Developing Secure Cyber Systems |
| Technology         | • Attack / Dependency Graphs  
                     • Layered Network Simulators  
                     • Threat Frameworks |
5 Step Formula for Cyber M&S Success

1. Use your skills to make a contribution to Cyber Modeling
2. Because we need it
3. I know you can do it
4. Think what you’ve done together before
5. Now let’s go and do it!