How to Quantify Cyber-Resilience?
A Managerial Framework
Ranjan Pal
Talk Outline

I. Conceptual Definition and Metrification

II. Fitting Cyber-Resilience Metrics to Dimensions

III. A Systematic Cyber-Resilience Quantification Framework
I. Conceptual Definition and Metrification
How Can We Define the Cyber-Resilience Concept?

The ability for an enterprise to anticipate, absorb, adapt, and recover under cyber-threat environments

Conceptual Definition $\neq$ Metric Definition

How many of you adhere to this definition in your organization?
Let’s Illustrate the Concept Through a Figurative Example

e.g., # ‘Up’-Servers

What is an enterprise’s ability to **anticipate**, **absorb**, **adapt**, and **recover** to given ‘y’-axis demands?
Let’s Illustrate the Concept Through Another Figurative Example

e.g., Battery Power

What is an enterprise’s ability to anticipate, absorb, adapt, and recover to given ‘y’-axis demands?
An Example Purpose of a Cyber-Resilience Metric

A cyber-resilience (CR) metric will drive enterprise/organization goals

Examples of Enterprise Management Goals

Achieve and sustain acceptable levels of (critical) mission function performance
- e.g., the number of UP-servers should always be greater than $K$

Achieve acceptable levels of cyber-security
- e.g., the number of financial impact causing cyber-incidents within time $[T1, T2]$ should be less than $A$

‘Minimize’ adverse financial impact upon a cyber-attack
- e.g., the monetary value of multi-party loss incurred due to business disruption should be less than $X$

‘Constrain’ time to system recovery upon a cyber-attack
- e.g., the time duration a (sub-)system is ‘down’ due to a cyber-incident should be less than $T$

How many of you have a cyber-resilience metric in your organization?
Many enterprises have cyber-resilience metrics mapping to multiple dimensions. These dimensions fit the quantification framework we have developed in our research.
II. Mapping Cyber-Resilience Metrics to Dimensions
Dimensions that Cyber-Resilience Metrics Map To

Identified five dimensions to view a cyber-resilience metric

I. Management rank
   (e.g., board/C-suite, technical lead)

II. Enterprise system complexity
   (e.g., one component (server), network of components)

III. Network communication type
   (e.g., physical, process, social)

IV. Enterprise type
   (e.g., critical infrastructure, commercial business)

V. Manager risk tolerance
   (e.g., low tolerance, high tolerance)

Listed dimensions based on a survey of approximately 50 research articles in engineering/social science/business, and 20 public website articles
Example Metrics in the ‘Management Rank’ Dimension

Source: Library of Cyber-Resilience Metrics (Lagarde et.al.)

The ability to handle cyber-incidents
(anticipate, adapt/absorb, recover)

- malware
- social engineering
- DDoS

Performance Measure (Tech Lead): #up-servers, #non-compromised sensors
Performance Measure (C-suite): financial impact upon a cyber-incident

High risk-tolerant manager - will quantify ability to maximize mean performance per time interval
Low risk-tolerant manager - will quantify ability to minimize #times performance falls below MALC
III. Our Cyber-Resilience Quantification Framework
The SIMPLEX Cyber-Resilience (CR) Quantification Framework

Communication Type (CT)

Rank

Enterprise Type

System Complexity

The FIVE dimensions in a simplex

A ‘toolbox’ of situational CR metrics

We adopt the term ‘simplex’ as a mashup between the ‘simplicity’ of our quantification framework and the simplex mathematical object.
Let Us Work Through One Dimension Mapping Example

We need to quantify the metric: the **ability** to handle DDoS attacks

### Dimension Configuration #1

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Rank</td>
<td>Technical Lead</td>
</tr>
<tr>
<td>System Complexity</td>
<td>One Server</td>
</tr>
<tr>
<td>Communication Type</td>
<td>Process</td>
</tr>
<tr>
<td>Enterprise Type</td>
<td>Commercial</td>
</tr>
<tr>
<td>Risk Tolerance</td>
<td>H(green), L(blue)</td>
</tr>
</tbody>
</table>

### Performance Metric

- **# Requests/Second**

### CR Score

- **Anticipation Ability**
  - NIST – I,P,D
  - X
- **Adapt & Absorb Ability**
  - NIST - Respond
  - X
- **Recovering Ability**
  - NIST - Recover

<table>
<thead>
<tr>
<th>Desired X-axis values</th>
<th>Desired Y-axis values</th>
</tr>
</thead>
<tbody>
<tr>
<td>CR Score</td>
<td></td>
</tr>
</tbody>
</table>
Dragos’s CR Equation is an Instance of SIMPLEX Quantification

\[ \text{Cyber-Resilience} = \text{Consequence} \times (\text{Threat} \times \text{Vulnerability}) \times (\text{Cyber-Risk})^{-1} \]

\[ RF(\vec{T} = [t_d, t'_d, t_\delta, t_r]) \times \frac{P_r}{P_0} \]

\[ CR = R \times RF(\hat{T} = [t_d, t'_d, t_\delta, t_r]) \times \frac{P^*_r P_d}{P_0 P_0} \]
Key Takeaways from the Discussion

Many enterprises have cyber-resilience metrics

These metrics map to multiple dimensions

Enterprises often do not account for these dimensions to quantify cyber-resilience metrics

We developed a quantification framework where the dimensions fit a quantified metric

ranjanp@mit.edu