Industrial Security, Preparedness and Mobilization

Thinking the Thinkable
Data as a Strategic Asset

Dan Green, Research Associate
Naval Innovation Advisory Council
12-14 July 2016
Superiority in technology did not just happen.

There have been more than two centuries of collaboration and experimentation among people in and out of uniform, in government and industry, redefining what is possible.

In so many cases, we have taken seemingly impossible ideas and made them real.

Ray Mabus, Secretary of the Navy
April 15, 2015
• Assessing and Forecasting Industrial Security and Preparedness

• The health and resilience of the United States industrial sector are leading indicators of economic security.

• Implications of big data methodologies for assessing and forecasting industrial preparedness in the context of factors such as globalized supply chains, multi-national corporate relationships and cybersecurity vulnerabilities.

• Analysis of micro-economic factors may improve the planning and could help shape domestic for critical sectors will be discussed.

• Risk as a function of the tradeoffs between domestic production, ownership and trade dependencies will also be a theme.
Decision Challenges: Define, Measure, Monitor

- What decisions are made in the context of a desired outcome
- What data informs those decisions
- How do I provision the data (channel)
- How do I *dynamically* define the attributes of “right”

Data Valuation: Dynamic Context

Provide the "right" information ...
To the "right" consumer ...
At the "right" time ...
The Generic Graphic in Figure 1 depicts risk as a function of time. The top section represents the *circumstances* of the operating environment, or industry context. The bottom half represents the *operational decision cycle* which is controlled by the organization. Both change dynamically over time. Risk reflects the degree of uncertainty between the past, “prior” outcomes, and possible future outcomes.

As a starting point for conceptualizing Risk, the graphic can then be used to elicit specific factors, attributes, weights and priorities that are unique to that industry. The resulting *risk profile* defines the prudent *operational trade-space* for the company or industry segment. Industry specific cyber security modeling and assessments are elicited from operators in accordance with the September 2012 revision of NIST 800-30 "Guide for Conducting Risk Assessments". The statistical and probabilistic algorithms used to execute the workflow are abstracted away and reside in a cloud-based risk processing engine which is detailed in the next section.
The concept of “Turning Inside the OODA Loop” was defined by James Boyd in the 1950s. As noted above, when events and entities change faster than the Decision Cycle, outcomes become less predictable. From a decision quality perspective, this raises possibility of strategic surprise or Black Swan events.
Enhanced Decision Cycle: OODA + Analytics

**Planning and Processing**

- Risk and Uncertainty
- Preferences and Priorities
- Rules of Decision
- Data Sources
- Mission Data Sets

**Execution**

- Decision Threshold
- Actions
- Mission Outcomes
- Consequences
- ROE

**Enhanced Decision Cycle:**

1. **Observe and Orient**
2. **Planning**
   - Risk and Uncertainty
   - Preferences and Priorities
   - Rules of Decision
   - Data Sources
   - Mission Data Sets
3. **Decide and Act**
   - Actions
   - Mission Outcomes
   - Consequences
   - ROE

**OODA + Analytics**

- **Observe and Orient**
- **Plan**
- **Decide and Act**
- **Execute**
<table>
<thead>
<tr>
<th>Choice Categories</th>
<th>Efficient Frontiers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choice under uncertainty</td>
<td>Loss Function</td>
</tr>
<tr>
<td>Choice over time</td>
<td>– What is the downside</td>
</tr>
<tr>
<td>Multi-person choice</td>
<td>Utility Function</td>
</tr>
<tr>
<td>Complex choice</td>
<td>– How desirable is it</td>
</tr>
<tr>
<td></td>
<td>Risk Function</td>
</tr>
<tr>
<td></td>
<td>– How much don’t I know</td>
</tr>
</tbody>
</table>

Rational Actors?
Challenges: Risk 2016

• Defense industrial baselines have hidden dependencies between elements in the value chains

• The Rate of Change of Industrial Value Chains exceeds collection and reporting frequency

• Complexity of Industrial Value Chains is dynamic

• Availability of physical assets in the Industrial Baseline is tightly coupled to cyber availability (e.g., cyber-physical systems)