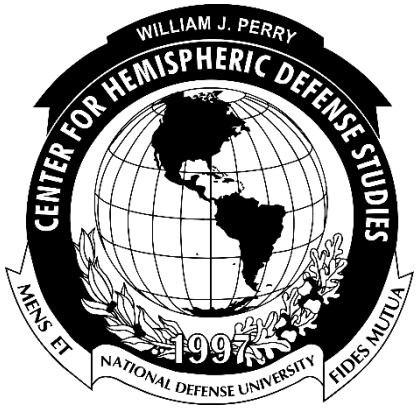
# WEBINARS

July 2, 2020 1900-2000 EDT (UTC-4)

## Strategic Concepts in Cyber: A COVID-21 Pivot



# Strategic Concepts in Cyber: A COVID-21 Pivot

**Dr. Boris Saavedra**

***Associate Professor***

**Center of Hemispheric Defense Study**

**National Defense University**

**Washington, DC 20593-0001**

**saavedrab@ndu.edu**

**202-685-2213**

**FAX 202-685-4675**

# Principle of  Academic freedom

The ideas contained in this presentation are the responsibility of the author, without necessarily reflecting the thinking of the WJPC, NDU, DoD or the US government.

# Agenda

- Objective
- Strategy in Cyberspace
- What is cyber strategy?
- Current global technological context
- Cyber physical systems/Internet of things
- Artificial Intelligence, Machine learning and Quantum Technology
- Conclusions

# Objective

Understand the strategic concepts
for the prospective analysis of cyberspace
in order to design the policy
and establish the strategy
for a possible pandemic situation in 2021.

# Strategy in Cyberspace

- **What is strategy?**

It is a dialectic of opposing wills, a set of ideas on how to use instruments of power to obtain influence through coercion. An inherent element of state policy at all times.

- **What is cyber strategy?**

Modern variant of coercive diplomacy that sits on an escalation ladder between economic coercion and the use of physical force.

# What is a cyber strategy?

- Cyber strategy is a form of political warfare optimized for the 21st century.

- Cyber strategy logics:
  - **Disruption:** is a low-cost, low-payoff form of cyber strategy to shape the larger bargaining context.
  - **Espionage:** focuses on altering the balance of information to achieve a position of advantage.
  - Degradation-coercive designated to sabotage the enemy target's networks, operations or systems-is more likely to have a compellent effect than disruption or espionage.

# Current global technological context

- Accelerated exponential technology ⟶ disruptive innovation

- the conversion of these new accelerated technologies
  - Artificial intelligence
  - Virtual and augmented reality
  - 3 D printing
  - Blockchain
  - Material science and nanotechnology
  - Biotechnology

# Cyber Physical System(CPS) and Internet of Things (IoT) a dependent relationship

- Why it is important?
- What level of understanding is needed at policy and strategic level?
- IoT: Massive connectivity in expansion of physical devices that communicate through a large system. (connectivity)
- CPS: highly integrated computational network, closed loops, and physical processes with high degree of automation and capabilities (knowledge)

Cyber Physical Systems The Coming Singularity. Dr. Marty Trevino
https://www.ndu.edu/News/Article-View/Article/2079817/prism-vol-8-no-3-january-2020/

# Artificial intelligence, machine learning and quantum technology

- **AI:** "Any artificial system that performs tasks that are normally performed by the human being such as: perception, cognition, planning, learning, human-like communication, or physical action."
- **ML:** "Machine learning (ML) is a form of AI that allows a system to learn from data rather than through explicit programming."
- **QT:** "The technology that works using the principles of quantum mechanics (the physics of subatomic particles), including quantum entanglement and quantum superposition."

Cyber Physical Systems The Coming Singularity. Dr. Marty Trevino
https://www.ndu.edu/News/Article-View/Article/2079817/prism-vol-8-no-3-january-2020/

# Conclusions

- Exponential accelerated technology is any technology that doubles its power and reduces cost on a regular basis.
- Technological convergence is the process by which independent technologies converge with each other and accelerate exponentially.
- Cyberphysical systems generate "knowledge" Internet of things is connectivity.
- Artificial intelligence, automation and 5G telecommunications could be further accelerated, particularly in the area such as artificial intelligence, biotechnology, materials development, among others.

https://advisor.thedialogue.org/wp-content/uploads/2020/04/LAA200416.pdf

# Assessing Cyber Capabilities in a Changing Environment

A DECONSTRUCTIVST APPROACH TO DEVELOPING AND MANAGING CYBER CAPABILITIES

Dr. Marty Trevino Jr.

CREATED FOR THE NATIONAL DEFENSE UNIVERSITY

JUNE 2020

The world of Cyber is constantly changing, COVID-19 is one example of an unexpected event that has altered the Cyber Ecosystem.

Challenges for Cyber Leaders:

1. A New Domain
2. Rapidly and Unexpected Changing Environment

The only effective model for dealing with this complexity is through Capabilities. One's Own evolving Capabilities vs. Threats and Actors.

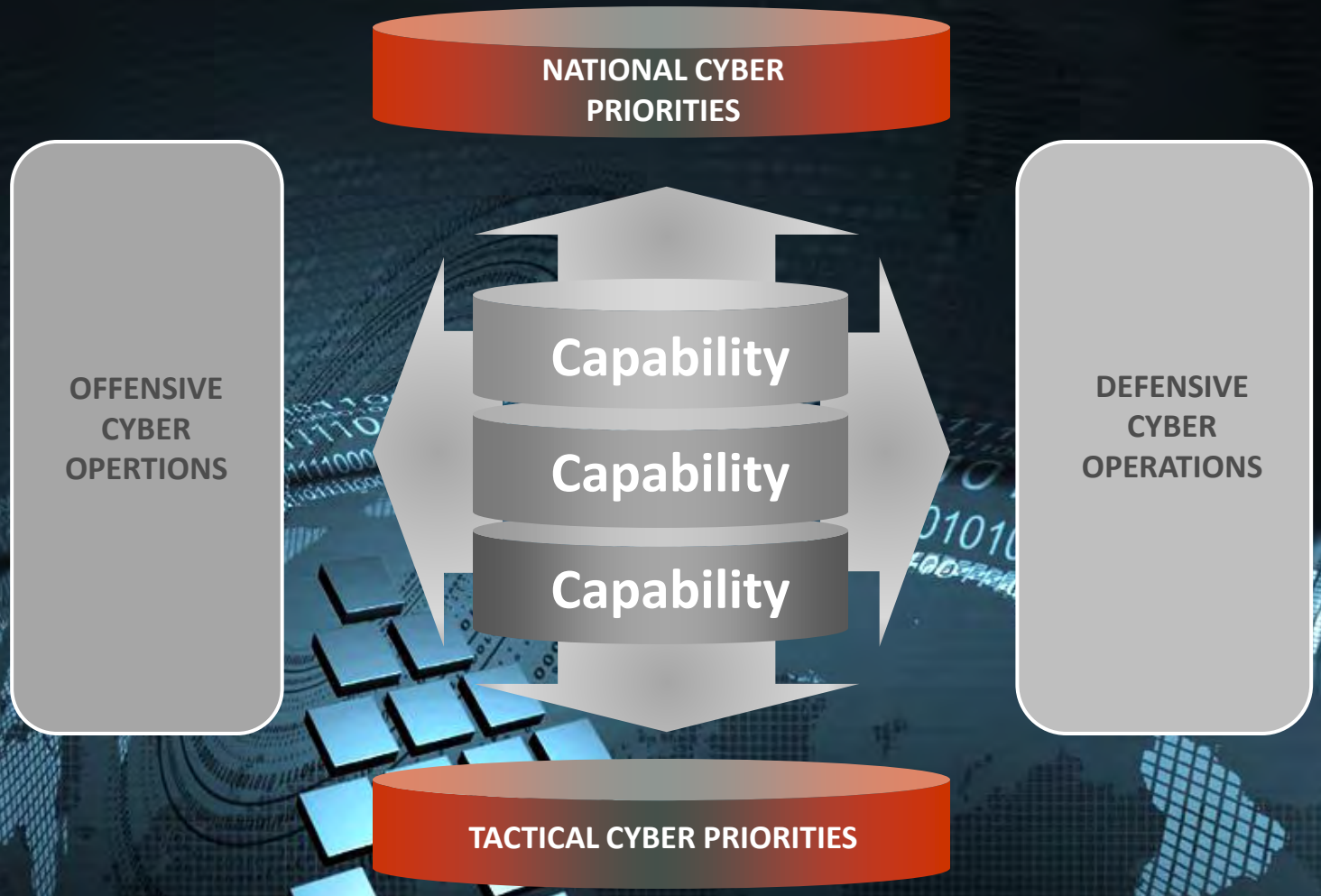
The Question is "How"?

# CAPABILITY MODELING

Military Organizations have used Capability Models to Develop and Maintain Kinetic Force to Great Effectiveness.

Capability Models Apply to Cyber and can be among the Most Effective Tools in a Cyber Leader's Arsenal.

# Cyber Capability Models



# NATION STATE CAPABILITIES

## SED UT LOREM NATUS ERROR SIT LOREM

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Mauris massa erat, semper ut suscipit id, bibendum sed mi. Vestibulum venenatis enim id urna rhoncus imperdiet, porttitor ligula adipiscing.

# NATION STATE CYBER CAPABILITIES

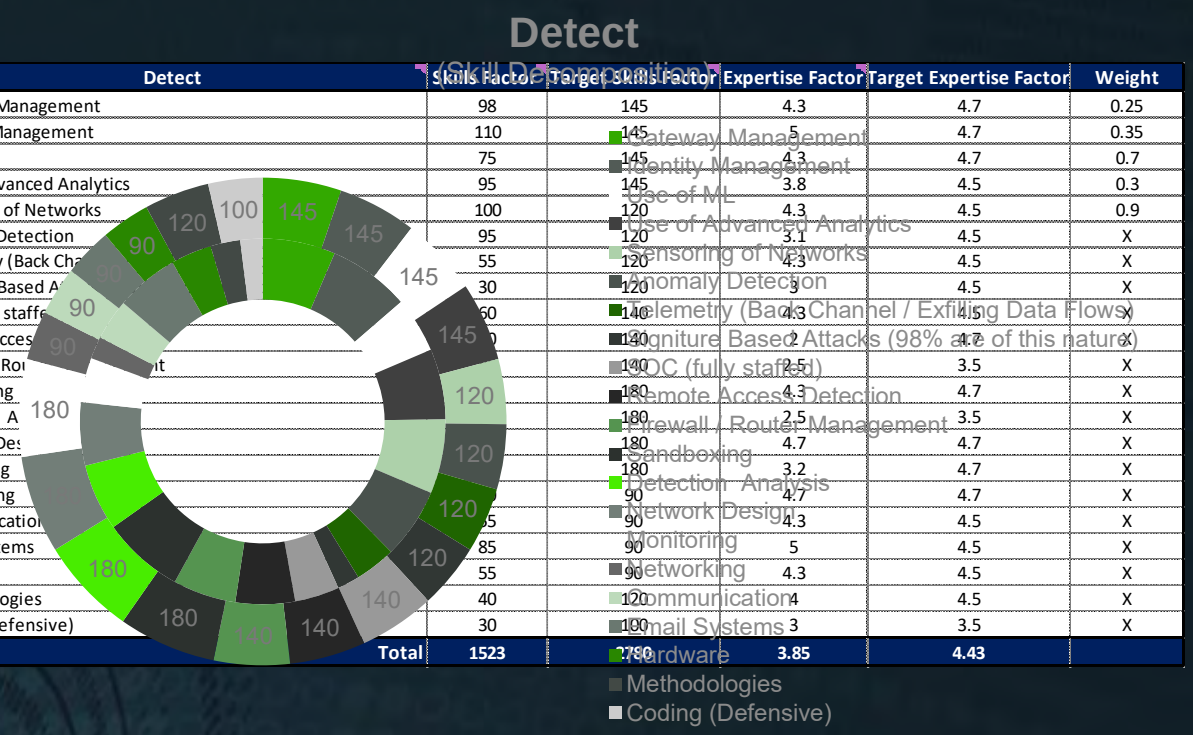
DETECT

HARDEN

# NATION STATE CYBER CAPABILITIES

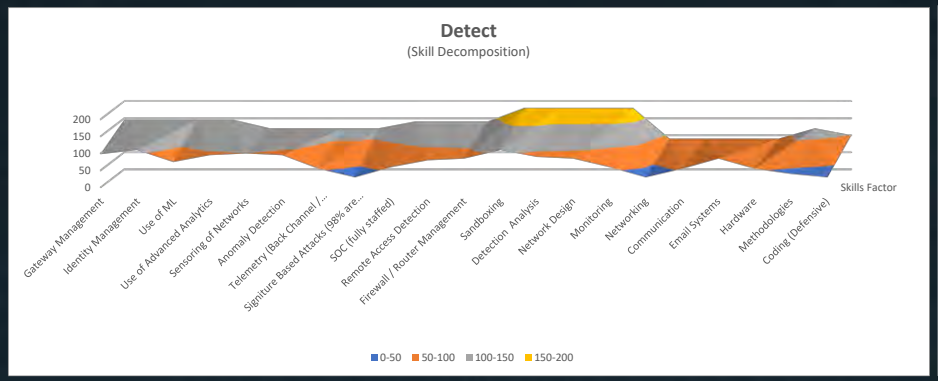
## DETECT - DECOMPOSITION

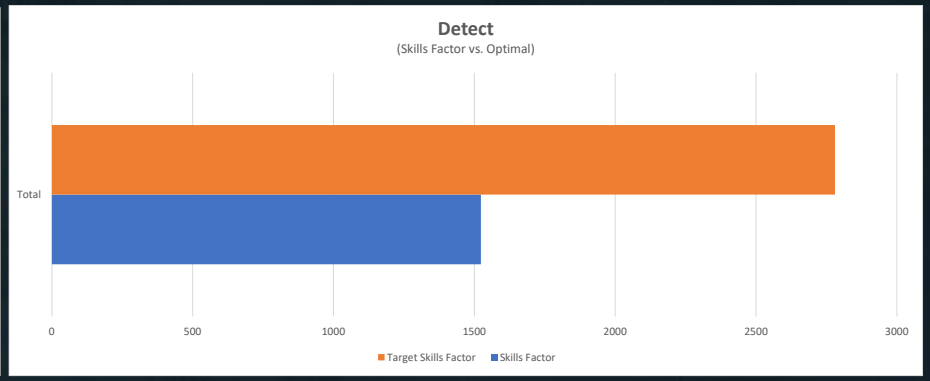
| | Detect | Skills Factor | Target Skills Factor | Expertise Factor | Target Expertise Factor | Weight |
|---|---|---|---|---|---|---|
| 1 | Gateway Management | 98 | 145 | 4.3 | 4.7 | 0.25 |
| 2 | Identity Management | 110 | 145 | 5 | 4.7 | 0.35 |
| 3 | Use of ML | 75 | 145 | 4.3 | 4.7 | 0.7 |
| 4 | Use of Advanced Analytics | 95 | 145 | 3.8 | 4.5 | 0.3 |
| 5 | Sensoring of Networks | 100 | 120 | 4.3 | 4.5 | 0.9 |
| 6 | Anomaly Detection | 95 | 120 | 3.1 | 4.5 | X |
| 7 | Telemetry (Back Cha | 55 | 120 | 4.3 | 4.5 | X |
| 8 | Signiture Based A | 30 | 120 | 3 | 4.5 | X |
| 9 | SOC (fully staffe | 60 | 140 | 4.3 | 4.5 | X |
| 10 | Remote Acces | 0 | 140 | 2 | 4.7 | X |
| 11 | Firewall / Rou | nt | 140 | 2.5 | 3.5 | X |
| 12 | Sandboxing | | 180 | 4.3 | 4.7 | X |
| 13 | Detection A | | 180 | 2.5 | 3.5 | X |
| 14 | Network Des | | 180 | 4.7 | 4.7 | X |
| 15 | Monitoring | | 180 | 3.2 | 4.7 | X |
| 16 | Networking | | 90 | 4.7 | 4.7 | X |
| 17 | Communicatio | 5 | 90 | 4.3 | 4.5 | X |
| 18 | Email Systems | 85 | 90 | 5 | 4.5 | X |
| 19 | Hardware | 55 | 90 | 4.3 | 4.5 | X |
| 20 | Methodologies | 40 | 120 | 4 | 4.5 | X |
| 21 | Coding (Defensive) | 30 | 100 | 3 | 3.5 | X |
| | Total | 1523 | 2780 | 3.85 | 4.43 | |

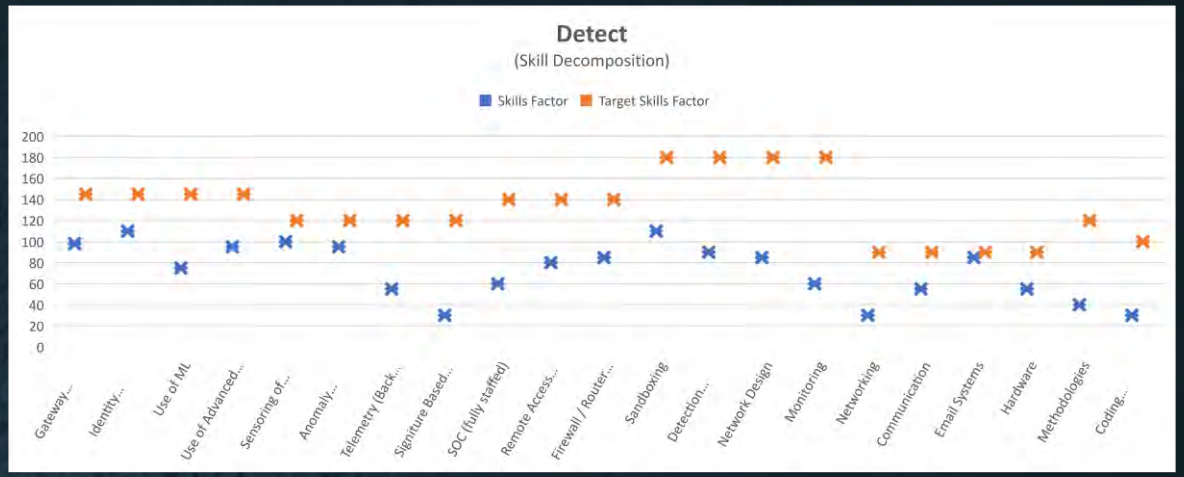


# NATION STATE CYBER CAPABILITIES

## DETECT - DECOMPOSITION



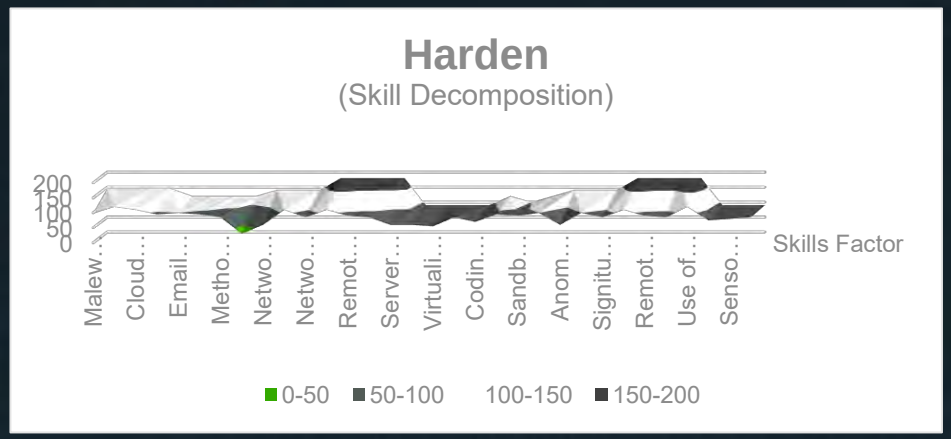
# NATION STATE CYBER CAPABILITIES

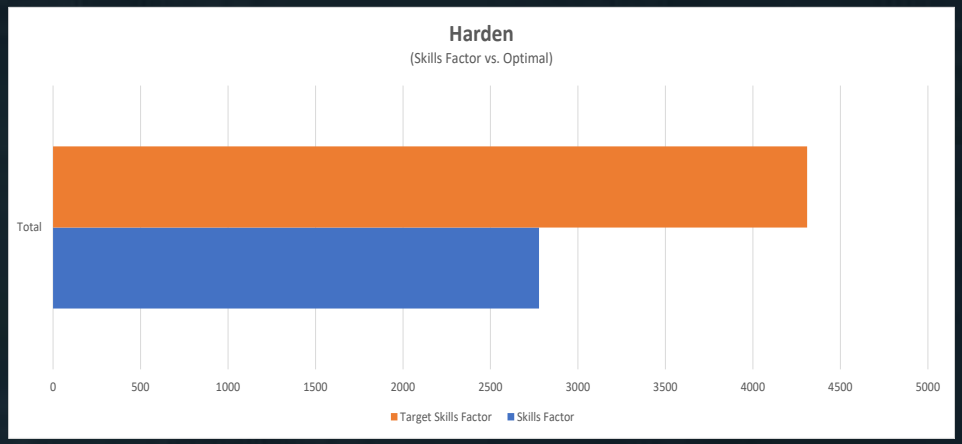
## HARDEN - DECOMPOSITION

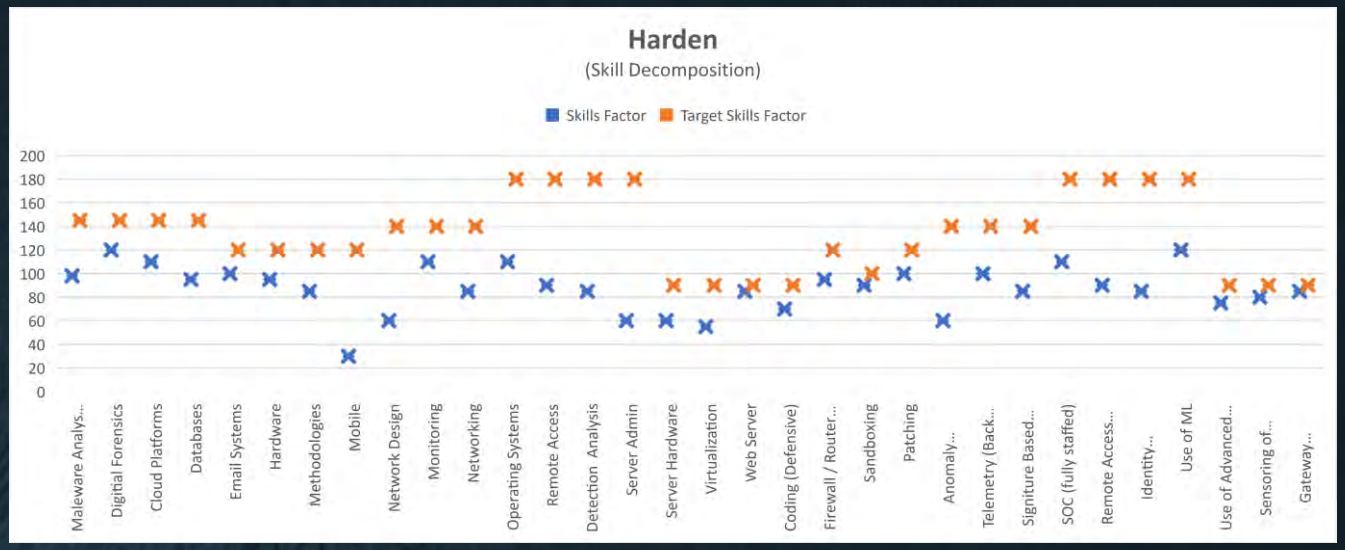
| | Harden | Skills Factor | Target Skills Factor | Expertise Factor | Target Expertise Factor | Weight |
|---|---|---|---|---|---|---|
| 1 | Maleware Analysis & Reversal | 98 | 145 | 4.3 | 4.7 | 0.6 |
| 2 | Digitial Forensics | 120 | 145 | 5 | 4.7 | 0.5 |
| 3 | Cloud Platforms | 110 | 145 | 4.3 | 4.7 | 0.4 |
| 4 | Databases | 95 | 145 | 3.8 | 4.5 | 0.3 |
| 5 | Email Systems | 100 | 120 | 4.3 | 4.5 | X |
| 6 | Hardware | 95 | 120 | 3.1 | 4.5 | X |
| 7 | Methodologies | 85 | 120 | 4.3 | 4.5 | X |
| 8 | Mobile | 30 | 120 | 3 | 4.5 | X |
| 9 | Network Design | 60 | 140 | 4.3 | 4.5 | X |
| 10 | Monitoring | 110 | 140 | 2 | 4.7 | X |
| 11 | Networking | 85 | 140 | 2.5 | 3.5 | X |
| 12 | Operating Systems | 110 | 180 | 4.3 | 4.7 | X |
| 13 | Remote Access | 90 | 180 | 2.5 | 3.5 | X |
| 14 | Detection  Analysis | 85 | 180 | 4.7 | 4.7 | X |
| 15 | Server Admin | 60 | 180 | 3.2 | 4.7 | X |
| 16 | Server Hardware | 60 | 90 | 4.7 | 4.7 | X |
| 17 | Virtualization | 55 | 90 | 4.3 | 4.5 | X |
| 18 | Web Server | 85 | 90 | 5 | 4.5 | X |
| 19 | Coding (Defensive) | 70 | 90 | 4.3 | 4.5 | X |
| 20 | Firewall / Router Management | 95 | 120 | 4 | 4.5 | X |
| 21 | Sandboxing | 90 | 100 | 3 | 3.5 | X |
| 22 | Patching | 100 | 120 | 3 | 4.5 | X |
| 23 | Anomaly Detection | 60 | 140 | 4.3 | 4.5 | X |
| 24 | Telemetry (Back Channel / Exfilling Data Flows) | 100 | 140 | 2 | 4.7 | X |
| 25 | Signiture Based Attacks (98% are of this nature) | 85 | 140 | 2.5 | 3.5 | X |
| 26 | SOC (fully staffed) | 110 | 180 | 4.3 | 4.7 | X |
| 27 | Remote Access Detection | 90 | 180 | 2.5 | 3.5 | X |
| 28 | Identity Management | 85 | 180 | 4.7 | 4.7 | X |
| 29 | Use of ML | 120 | 180 | 3.2 | 4.7 | X |
| 30 | Use of Advanced Analytics | 75 | 90 | 4.7 | 4.7 | X |
| 31 | Sensoring of Networks | 80 | 90 | 4.3 | 4.5 | X |
| 32 | Gateway Management | 85 | 90 | 5 | 4.5 | X |
| | **Total** | **2778** | **4310** | **3.79** | **4.43** | |

# NATION STATE CYBER CAPABILITIES

## DETECT - DECOMPOSITION



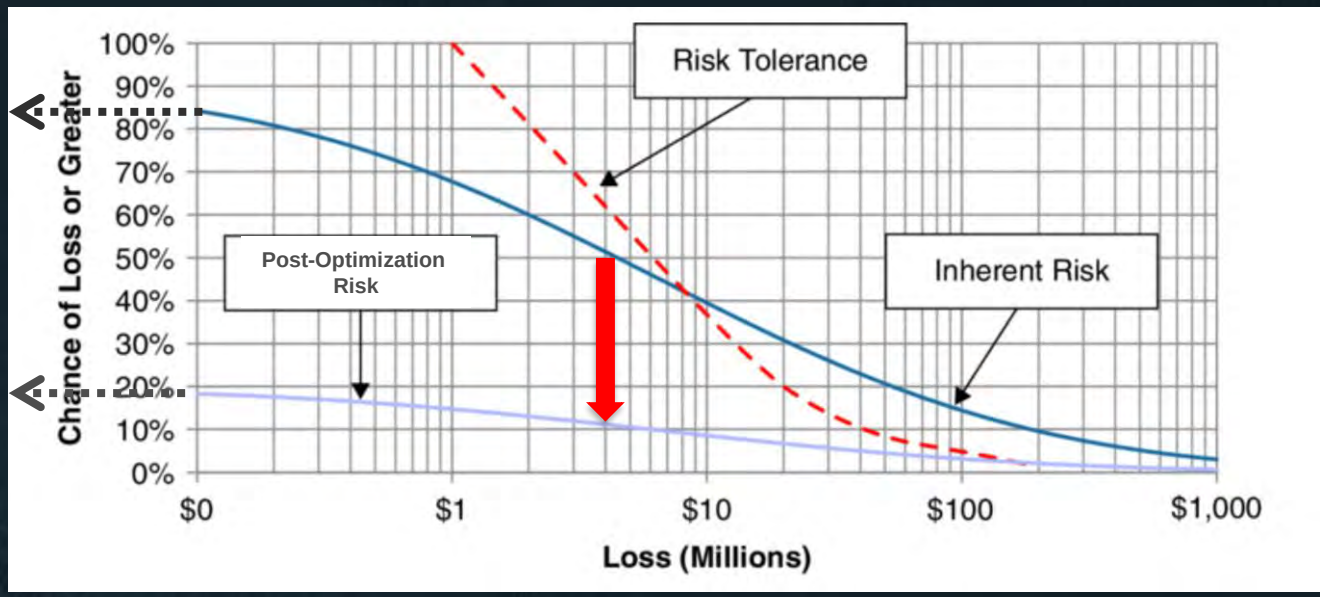
# LOSS EXCEEDANCE CURVES

EXPECTED LOSS

(A)$K

EXPECTED LOSS

(B)$K



# LOSS EXCEEDANCE CURVES

| List of adverse outcomes for use in risk model (Listing the top 20% that have 80% impact) | Probability of outcome | Likely $ impact (90% CI) |
|---|---|---|
| 1. Data breach resulting from Spam | 1. 0.14 | 1. $100,000 to $5,000,000 |
| 2. Data breach resulting from Ransomware | 2. 0.14 | 2. $100,000 to $5,000,000 |
| 3. Data breach resulting from Malware | 3. 0.14 | 3. $100,000 to $5,000,000 |
| 4. Data breach resulting from Social Engineering | 4. 0.14 | 4. $100,000 to $5,000,000 |
| 5. Data breach resulting from Phishing | 5. 0.14 | 5. $100,000 to $5,000,000 |
| 6. Data breach resulting from SQL injection | 6. 0.14 | 6. $100,000 to $5,000,000 |
| 7. Data breach resulting from Zero-day attacks | 7. 0.14 | 7. $100,000 to $5,000,000 |
| 8. Data breach resulting from Virus | 8. 0.14 | 8. $100,000 to $5,000,000 |
| 9. Downtime resulting from Spam | 9. 0.14 | 9. $100,000 to $5,000,000 |
| 10.Downtime resulting from Ransomware | 10.0.14 | 10.$100,000 to $5,000,000 |
| 11.Downtime resulting from Malware | 11.0.14 | 11.$100,000 to $5,000,000 |
| 12.Downtime resulting from Social Engineering | 12.0.14 | 12.$100,000 to $5,000,000 |
| 13.Downtime resulting from Phishing | 13.0.14 | 13.$100,000 to $5,000,000 |
| 14.Downtime resulting from SQL injection | 14.0.14 | 14.$100,000 to $5,000,000 |
| 15.Downtime resulting from Denial of Service attack | 15.0.14 | 15.$100,000 to $5,000,000 |
| 16.Downtime resulting from Zero-day attacks | 16.0.14 | 16.$100,000 to $5,000,000 |
| 17.Downtime resulting from Virus | 17.0.14 | 17.$100,000 to $5,000,000 |
| 18…. (more can be added based on customer's unique situations) | … | … |
| … | … | … |
| 50 | 50. 0.14 | 50. $100,000 to $5,000,000 |

# NATION STATE CYBER CAPABILITIES

NATIONAL CYBER PRIORITIES

TACTICAL CYBER PRIORITIES

ORGANIZATION

DETECT
DEFEND
HARDEN
RECOVER
RESPOND
HUNT

ADVERSARIES / ACTORS

MISSION PRIORITIES

THREATS TO ASSESTS (CI)

(MALWARE, ETC.)

RESOURCING DECISIONS

# END PRESENTATION