Achieving Agility in Cyberspace

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Philip Boxer, Ed Morris,
Bill Anderson (presenter)

24th October 2007

What is Cyberspace?

Cyberspace* is a term used to define the virtual world, built entirely of computers, computer networks, and associated systems around the globe

> “*Although Cyberspace would not exist without physics, it is by no means bounded to the pure physical reality term.*”

Wertheim, M., *De hemelpoort van cyberspace,* Anthos, Amsterdam, 2000.

**The term was coined by William Gibson in his novel Neuromancer*

Cyberspace as a Theater of Engagement

Loss of boundaries

- A threat can arise instantaneously anywhere. (SIPRNet is not immune.)

Fluidity of the environment

- No consistent front or mode of attack

No global visibility

- Large, chaotic, opaque motives, masking identity is easy

Uncertain nature of time

- Not necessarily a relation between the time an attack occurs and the time it was launched

Overlapping and shared jurisdiction

- Involves many parties, many areas have no clear dominion, spillover across jurisdictions is the norm

What are the Military Threats in Cyberspace?*

Limited cyber war: Information infrastructure is the means and target of attack (i.e., low-intensity conflict)

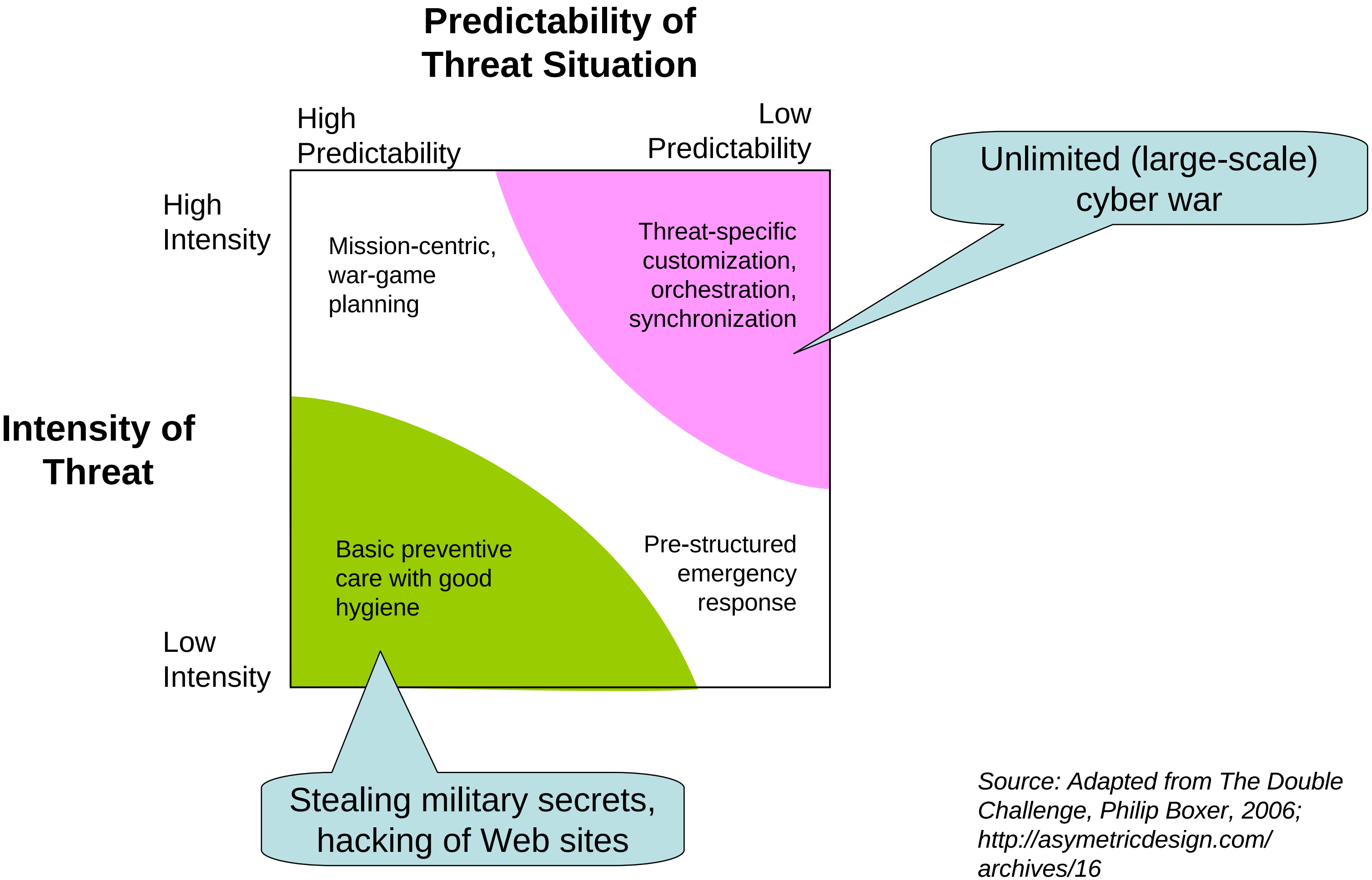
- e.g., denial of service attacks using botnets against Estonia in Spring, 2007

Unlimited cyber war: Comprehensive in scope and target coverage (i.e., high intensity conflict)

- no distinctions between military and civilian targets or between the home front and the fighting front.
- physical consequences and casualties
  - attacks deliberately intended to create mayhem and destruction
- economic and social impact—in addition to the loss of life—could be profound

NATO Review, Vol 49, No 4, Winter 2001

Framing the Cyberspace Theater



Predictability of Threat Situation

High Predictability

Low Predictability

High Intensity

Low Intensity

Intensity of Threat

Mission-centric, war-game planning

Threat-specific customization, orchestration, synchronization

Basic preventive care with good hygiene

Pre-structured emergency response

Unlimited (large-scale) cyber war

Stealing military secrets, hacking of Web sites

Source: Adapted from The Double Challenge, Philip Boxer, 2006; http://asymetricdesign.com/ archives/16

Low-Intensity, High-Predictability Threats

Adversaries threaten (and present opportunities) consistent with plans

- Goal is to develop tactics that counter these predictable threats.
- For the most part, these threats can be addressed by *good hygiene*, such as
  - installing security patches and procedures in a timely way
  - verifying compliance
  - managing passwords and other data securely
  - monitoring attempts to access systems
  - gathering data about the attackers and turning attackers’ actions against them

Low-Intensity, Low-Predictability Threats

Adversaries place unanticipated demands on the organization:

- Malicious agent employs a novel strategy, exploits a new flaw, or targets a new victim.
- Some form of *emergency response* is required.

Activities supporting this function include:

- coordinating the response to counter the threat
- monitoring the frequency/type of events managed by the emergency response capability
- identifying the chain of culpability, where possible
- analyzing patterns of activity in order to understand targets, motivations, strategy, and tactics

High-Intensity, High-Predictability Threats

Adversaries use high-intensity but predictable attacks to achieve large-scale geopolitical or economic gain.

Key to success is to *war-game*—to coordinate relationships with identified partners to meet anticipated threats

To prepare for these threats

- develop scenarios that reflect likely forms of attack
- identify external partners that will be involved and establish coordinated plans for responsibilities
- train personnel on available tools and technologies
- experiment with tools and tactics
- allow sufficient flexibility to allow personnel to adapt to minor variations of known situations

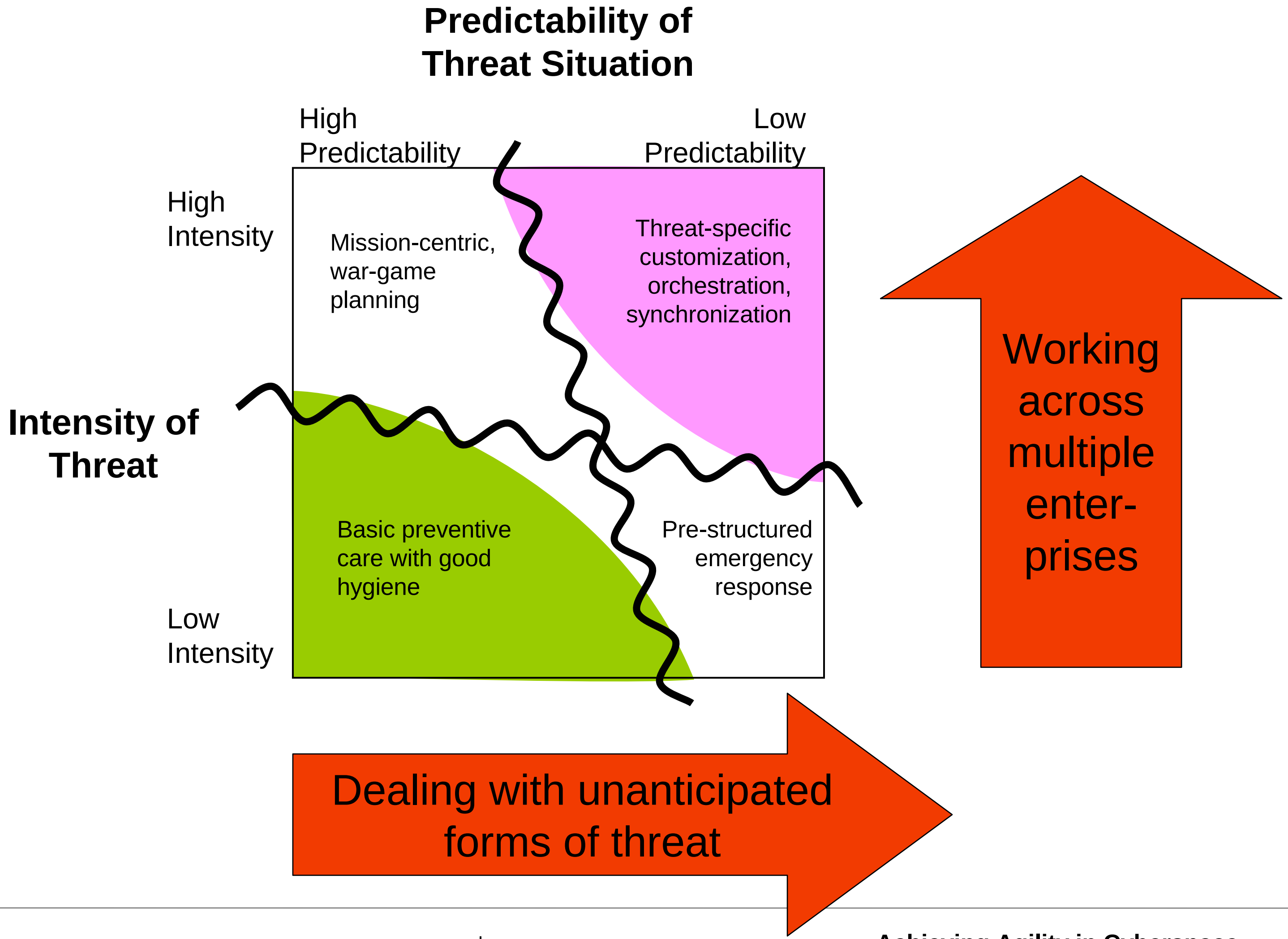
High-Intensity, Low-Predictability Threats

High-intensity and low-predictability conflict implies

- The good hygiene approach (bottom left quadrant) is not sufficient to meet the demand of a rapidly changing threat.
- Emergency response teams (bottom right quadrant) will become overwhelmed as the intensity of the conflict and the stakes involved increase.
- War-gamed responses (top left quadrant) are unlikely to map beyond the opening salvo because the intelligent adversary will continually adapt to the response.

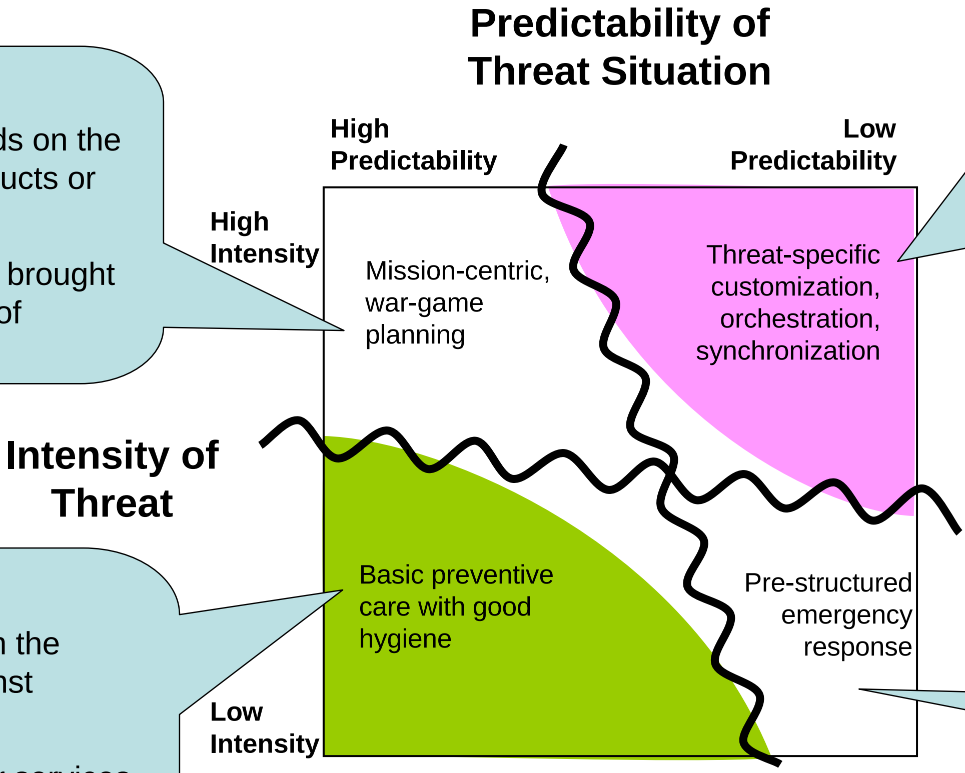
No matter how good the hygiene, emergency response, and war-gaming, intelligent adversaries can drive the situation into the top right quadrant whenever they choose.

The Cyberspace Theater’s Double Challenge



Predictability of Threat Situation
High Predictability
Low Predictability
High Intensity
Intensity of Threat
Low Intensity
Mission-centric, war-game planning
Threat-specific customization, orchestration, synchronization
Basic preventive care with good hygiene
Pre-structured emergency response
Working across multiple enter-prises
Dealing with unanticipated forms of threat

Forms of Agility Required


Predictability of Threat Situation
High Predictability
Low Predictability
Intensity of Threat
High Intensity
Low Intensity
Mission-centric, war-game planning
Threat-specific customization, orchestration, synchronization
Basic preventive care with good hygiene
Pre-structured emergency response

Type II Agility

Anticipate the demands on the mission and how products or services will be used

Multiple organizations brought under a unified chain of command

Type III Agility

Can't anticipate the demands on the mission

Can't anticipate how products or services will be used

Multiple organizations each with its own chain of command

Type I Agility

Anticipate the demands on the mission of defending against intrusion

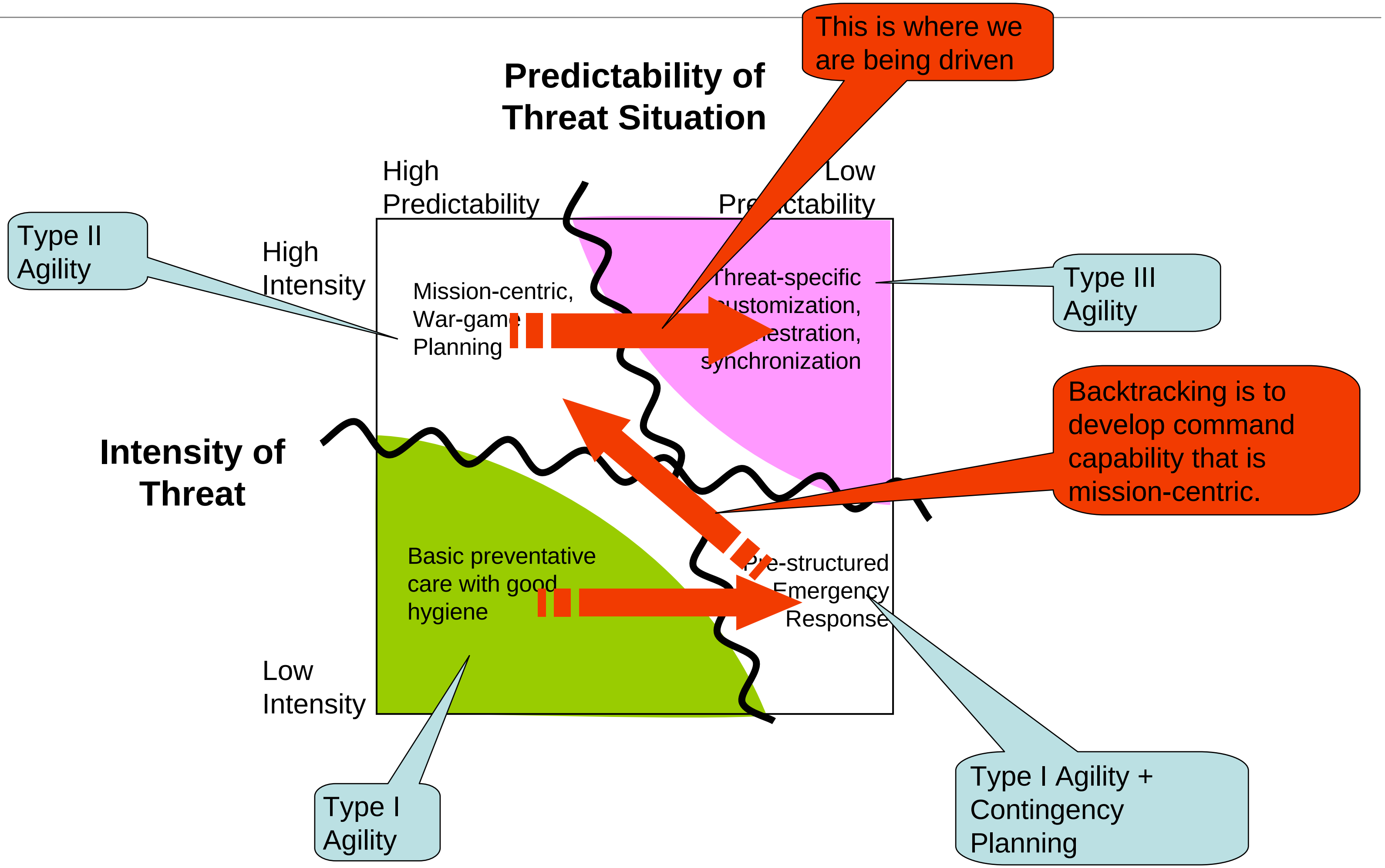
Anticipate how products or services will be used

Ensure that managerial entities apply appropriate commands

Type I Agility + Contingency Planning

Source: The Three Agilities, Philip Boxer & Richard Veryard, 2006; http://asymetricdesign.com/archives/18

An Unfortunate Trend


Predictability of Threat Situation
High Predictability
Low Predictability
Intensity of Threat
High Intensity
Low Intensity
Mission-centric, War-game Planning
Threat-specific customization, orchestration, synchronization
Basic preventative care with good hygiene
Pre-structured Emergency Response
This is where we are being driven
Type II Agility
Type III Agility
Backtracking is to develop command capability that is mission-centric.
Type I Agility
Type I Agility + Contingency Planning

How Does Agility Relate to Command?

Agility Type	Command Governance
Type I ▪ within the enterprise ▪ to predicted threats	**Stretching resources** across the organisation to optimally meet demands (i.e., cost efficiency). **Ensuring** that rules are followed
Type II ▪ across enterprises ▪ to predicted threats	**Leveraging existing** infrastructure and capabilities to address threats **Acting intelligently** by capturing and driving key information and knowledge through the organization **Co-ordinating relationships and processes** between multiple players (i.e., flexibility).
Type III ▪ across enterprises ▪ to unpredictable threats	**Harmonizing competing priorities, multiple strategies, and technologies** across organizations **Sensing and responding across organizations** to new threats and opportunities **Shift** command authority **to the edge**

Distinguishing Forms of Command

The nature of the managerial control is*

- **Directed**
  - Command that can be controlled by a central authority
- **Directed Collaboration**
  - Command that requires collaboration to fulfill an agreed-upon central purpose
- **Distributed Collaboration**
  - Command where there is no centrally agreed-upon purpose (The purpose must be built in response to situations.)

** "Architecting Principles for Systems of Systems," Mark W. Maier.* http://www.infoed.com/open/papers/systems.htm

Mapping Command Types to Agility Types

		Demands/ Purposes	
		Anticipated	Unanticipated
Autonomous Command Entities	Multiple	Directed Collaboration (Type II Agility)	Distributed Collaboration (Type III Agility)
	Single	Directed Composition (Type I Agility)	Directed Composition (Type I Agility + Contingency Plan’g)

Distributed Collaboration, Type III Agility Requires Edge-Synchronization

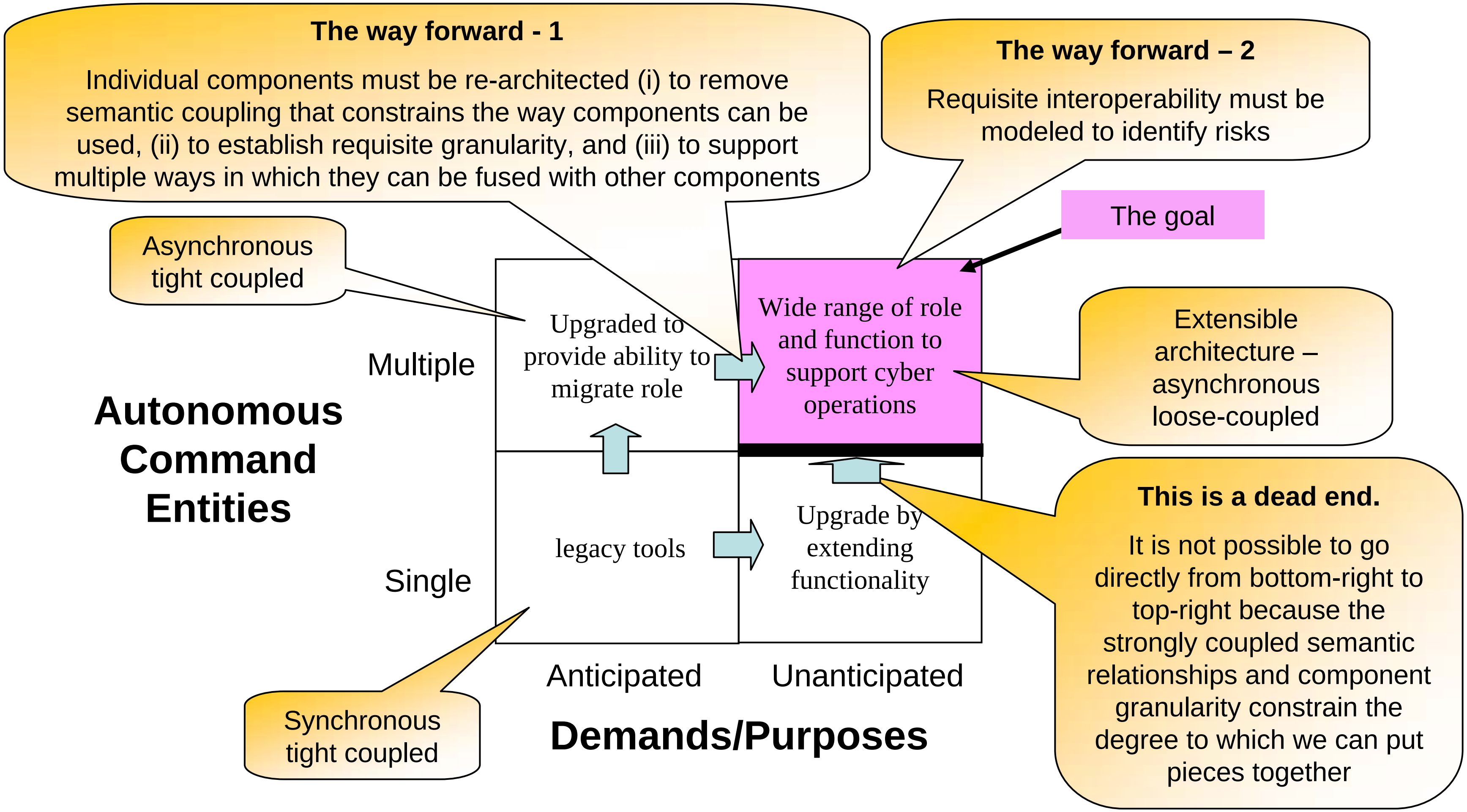
This means

- Missions are defined at the edge where the threat is encountered, rather than at the center.
- The infrastructures have to be “loosely-coupled” and “under-constrained” (i.e., able to be orchestrated and composed at the edge).

This in turn requires us to develop

- command structures that support power-to-the-edge, and
- agile infrastructures—with stratified granularity—that are sufficiently expressive to enable power-at-the-edge.

How do we get there?



The way forward - 1

Individual components must be re-architected (i) to remove semantic coupling that constrains the way components can be used, (ii) to establish requisite granularity, and (iii) to support multiple ways in which they can be fused with other components

The way forward – 2

Requisite interoperability must be modeled to identify risks

The goal

Asynchronous tight coupled

Extensible architecture – asynchronous loose-coupled

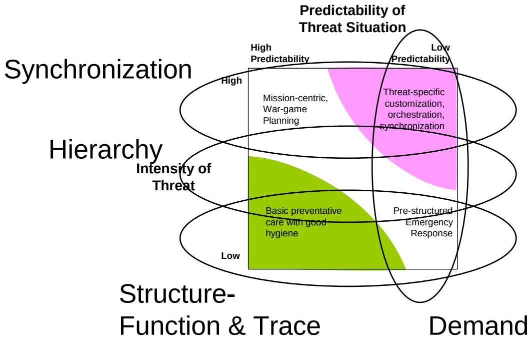
This is a dead end.

It is not possible to go directly from bottom-right to top-right because the strongly coupled semantic relationships and component granularity constrain the degree to which we can put pieces together

Synchronous tight coupled

Autonomous Command Entities
Multiple
Single
Upgraded to provide ability to migrate role
Wide range of role and function to support cyber operations
legacy tools
Upgrade by extending functionality
Anticipated
Unanticipated
Demands/Purposes

Model Interoperability Through the Command Structures and infrastructures in Their Contexts-of-Use


Predictability of Threat Situation
High Predictability
Low Predictability
Synchronization
High
Mission-centric, War-game Planning
Threat-specific customization, orchestration, synchronization
Hierarchy
Intensity of Threat
Basic preventative care with good hygiene
Pre-structured Emergency Response
Low
Structure-Function & Trace
Demand

Model interoperability with 5 layers of analysis:

- **Structure/Function**: The physical structure and functioning of resources and capabilities.
- **Trace**: The digital processes and systems that interact with the physical processes.
- **Hierarchy**: The formal hierarchies under which the uses made of both the physical and the digital are held accountable.
- **Synchronization**: The lateral relations of synchronization and orchestration within and between the organizations providing services "on the ground"
- **Demand**: The nature of the contexts-of-use giving rise to demands on the way the operations are organized to deliver services effectively and timely.

These 5 layers combine to form a model of the operational space as a whole, enabling Cyber Command to analyse the threats associated with orchestrating and synchronizing systems of systems in relation to particular forms of demand.

For More Information

Bill Anderson (presenter)

wba@sei.cmu.edu

Philip Boxer

pboxer@sei.cmu.edu

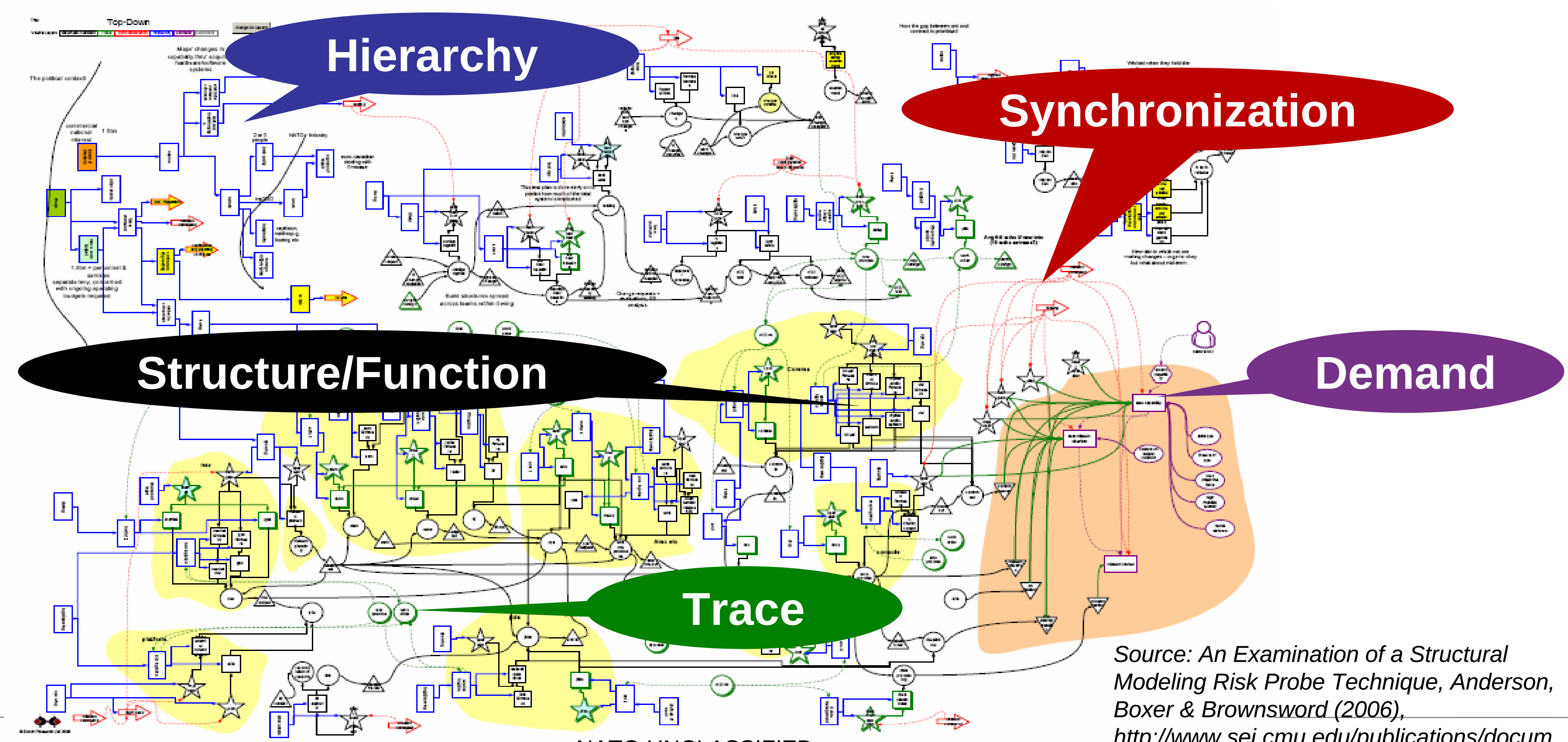
Ed Morris

ejm@sei.cmu.edu

Software Engineering Institute | Carnegie Mellon

Visual PAN—Rapid, Well Structured, Spaghetti

The PAN symbols and their relationship rules generate five interlocking layers in the visual model.



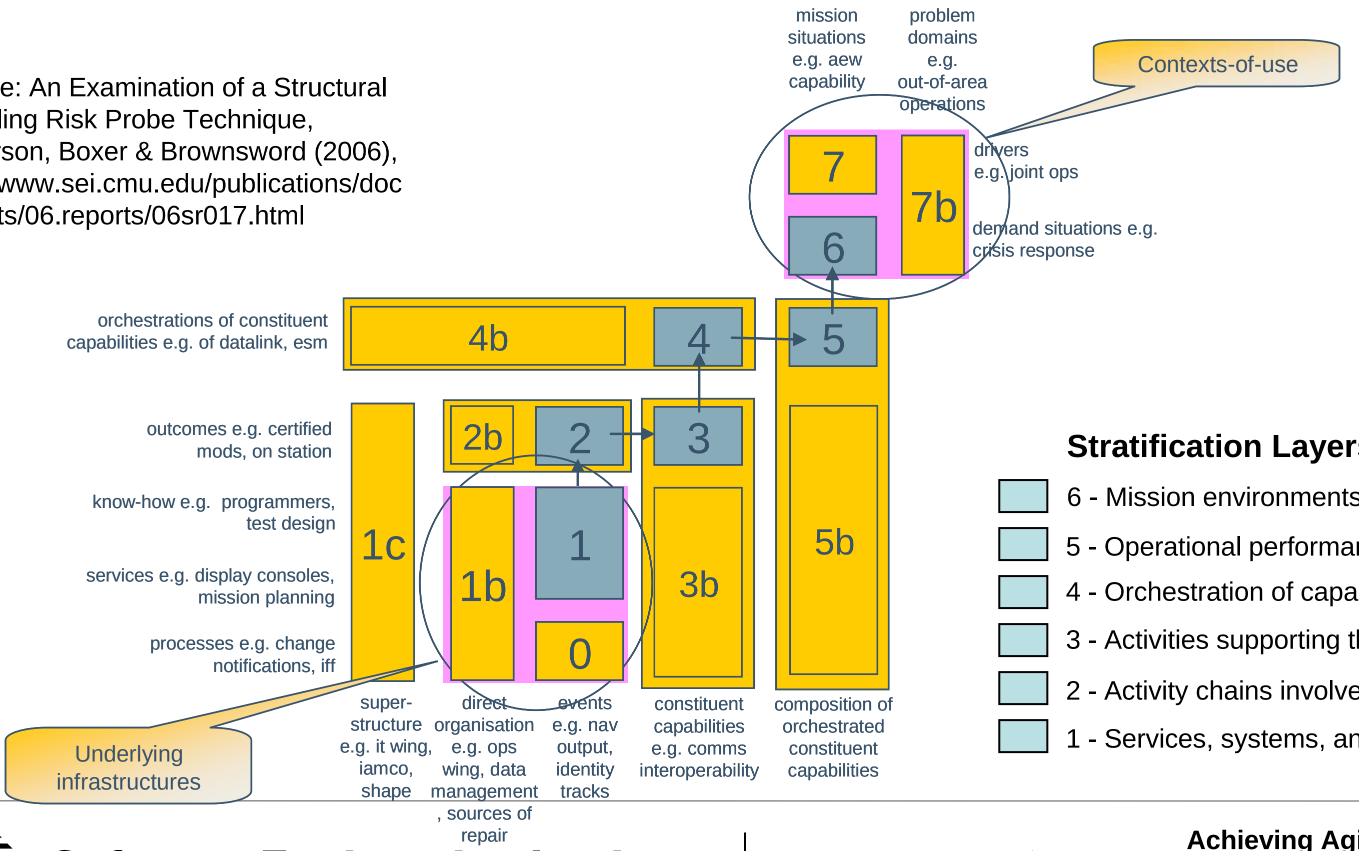
Source: An Examination of a Structural Modeling Risk Probe Technique, Anderson, Boxer & Brownsword (2006), http://www.sei.cmu.edu/publications/documents/06.reports/06sr017.html

NATO UNCLASSIFIED

Stratification Brings Structure to the Spaghetti

A six-layer stratification forms a framework against which the people, processes, and technical structures are analyzed in relation to the demands being placed upon them.

Source: An Examination of a Structural Modeling Risk Probe Technique, Anderson, Boxer & Brownsword (2006), http://www.sei.cmu.edu/publications/documents/06.reports/06sr017.html



mission situations e.g. aew capability
problem domains e.g. out-of-area operations
Contexts-of-use
7
7b
6
drivers e.g. joint ops
demand situations e.g. crisis response
orchestrations of constituent capabilities e.g. of datalink, esm
4b
4
5
outcomes e.g. certified mods, on station
2b
2
3
know-how e.g. programmers, test design
services e.g. display consoles, mission planning
processes e.g. change notifications, iff
1c
1b
1
0
3b
5b
super-structure e.g. it wing, iamco, shape
direct organisation e.g. ops wing, data management, sources of repair
events e.g. nav output, identity tracks
constituent capabilities e.g. comms interoperability
composition of orchestrated constituent capabilities
Underlying infrastructures

Stratification Layers

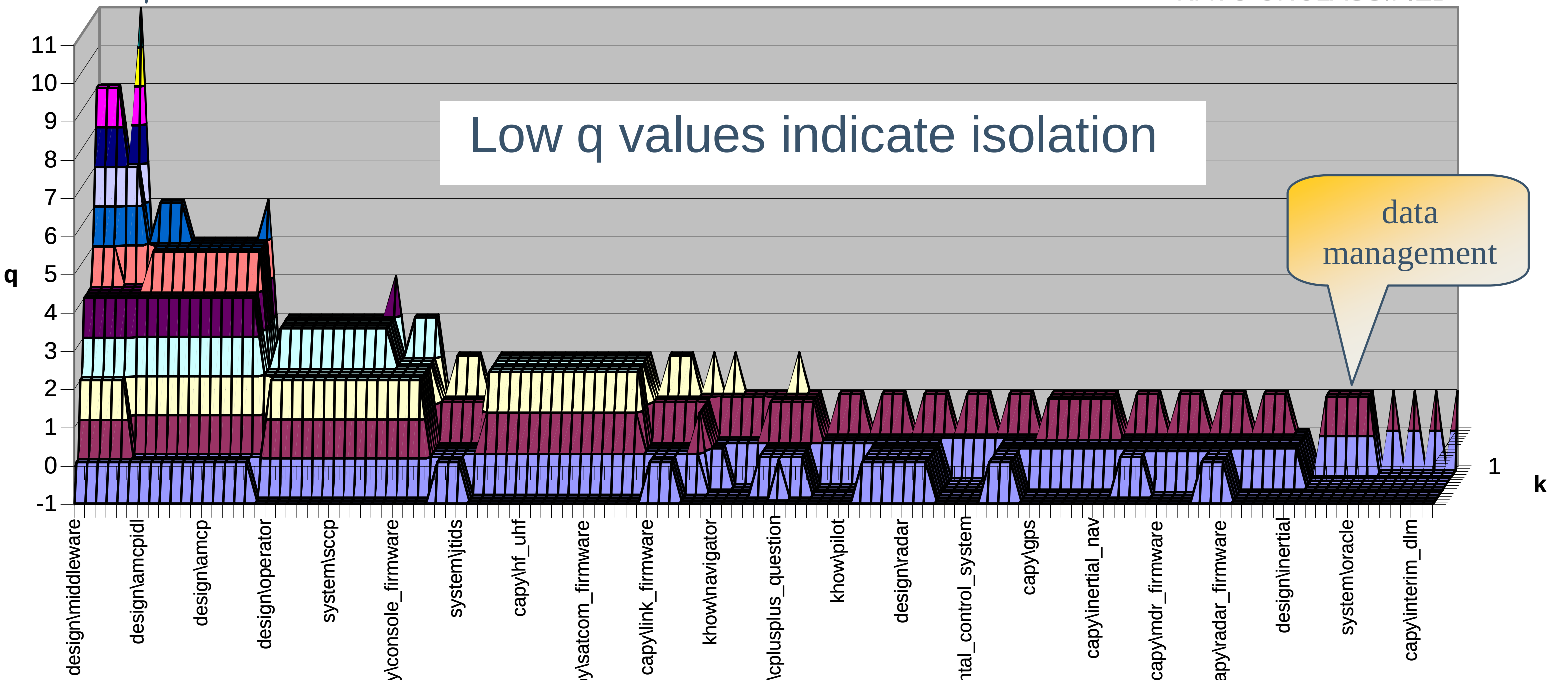
- ▢ 6 - Mission environments
- ▢ 5 - Operational performance of the capability
- ▢ 4 - Orchestration of capabilities by crew and operators
- ▢ 3 - Activities supporting the operational capability
- ▢ 2 - Activity chains involved in integrating components
- ▢ 1 - Services, systems, and know-how

Type 0 - Constructive Risk Landscape

The **Constructive Risk Landscape** reveals the degree of isolation between the many structural entities in this system of systems.

operator

NATO UNCLASSIFIED



Low q values indicate isolation

data management

q = number of events related to service

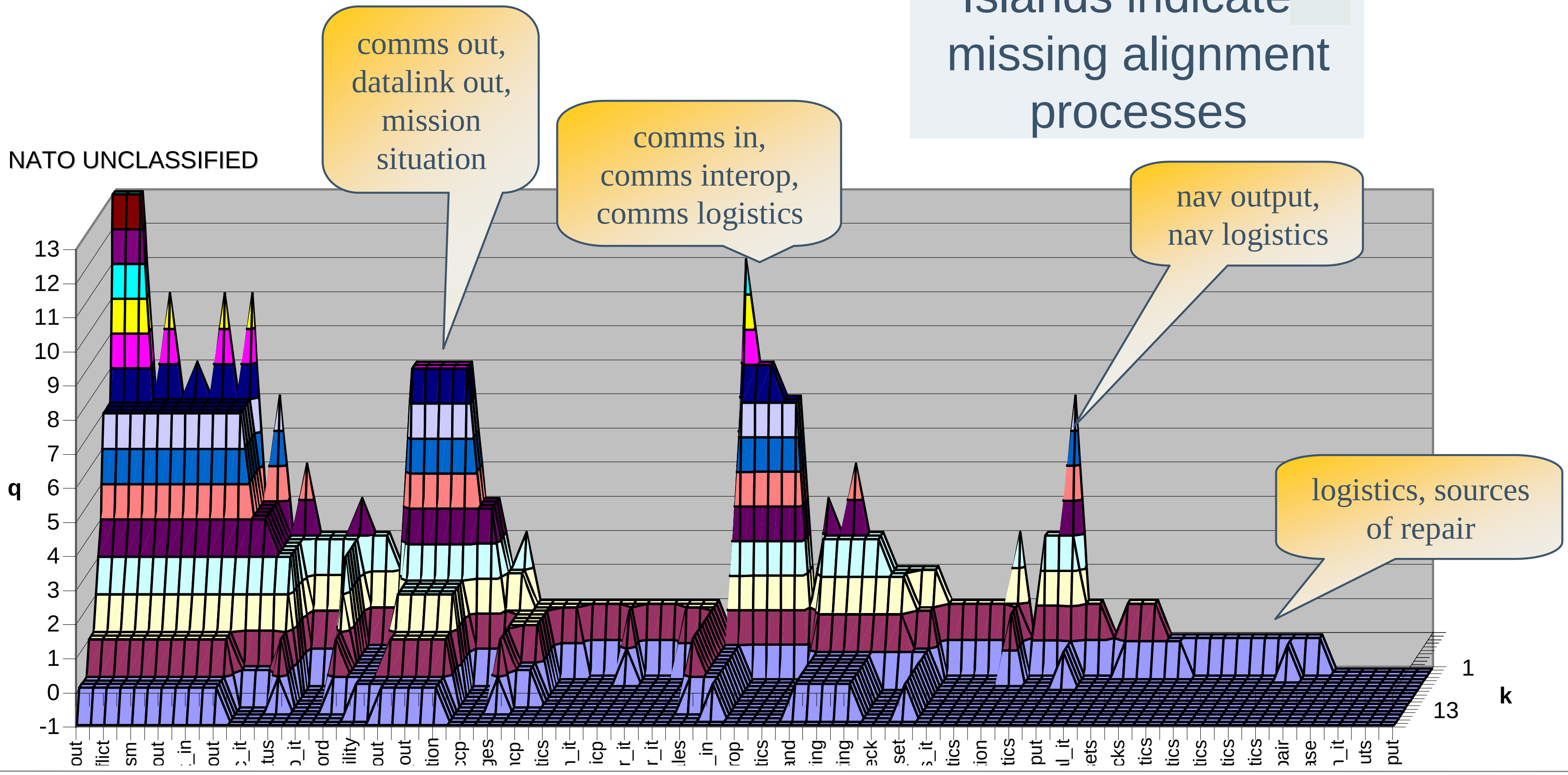
k = number of other services with common events at this level of q

Source: An Examination of a Structural Modeling Risk Probe Technique, Anderson, Boxer & Brownsword (2006). http://www.sei.cmu.edu/publications/documents/06.reports/06sr017.html

Type I - Customization Risk Landscape

The **Customization Landscape** reveals islands of high connectivity with broad regions of separation.

Islands indicate missing alignment processes



comms out, datalink out, mission situation

comms in, comms interop, comms logistics

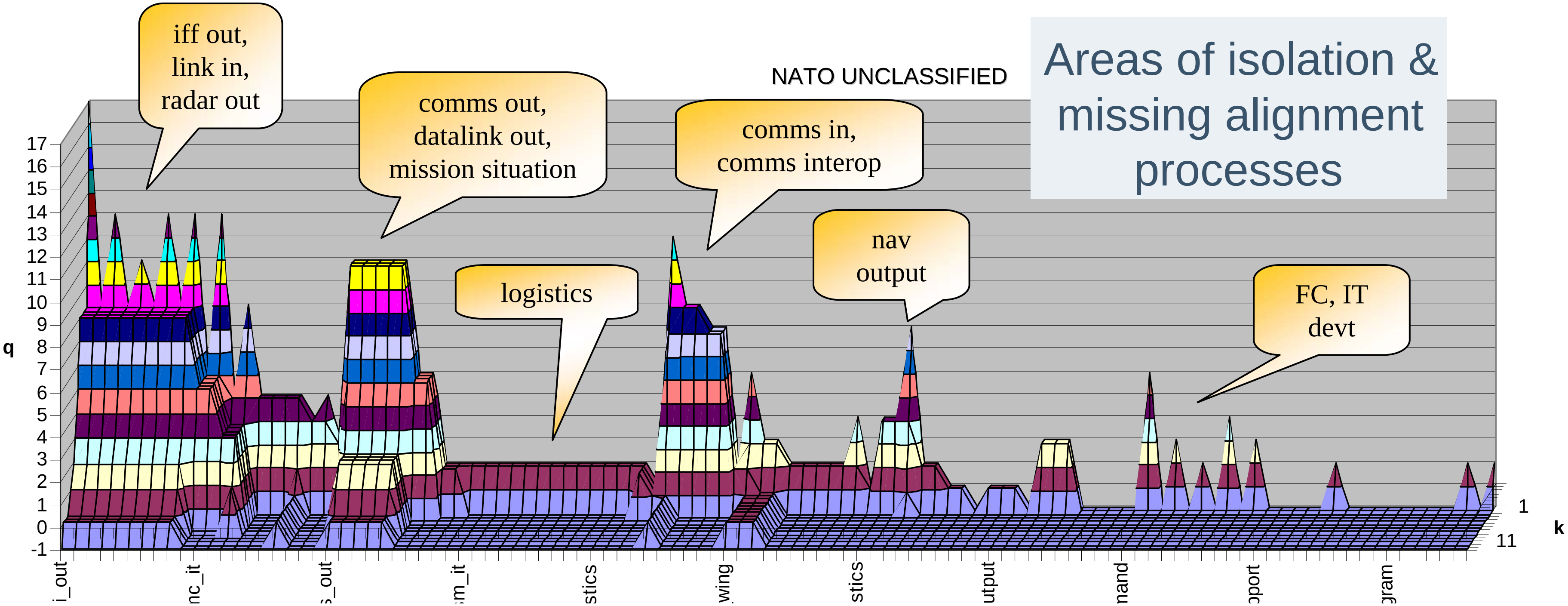
nav output, nav logistics

logistics, sources of repair

Source: An Examination of a Structural Modeling Risk Probe Technique, Anderson, Boxer & Brownsword (2006). http://www.sei.cmu.edu/publications/documents/06.reports/06sr017.html

Type II - Orchestration Risk Landscape

The **Orchestration Landscape** reveals areas of isolation, islands of high connectivity, and broad regions of separation.



iff out, link in, radar out

comms out, datalink out, mission situation

logistics

comms in, comms interop

nav output

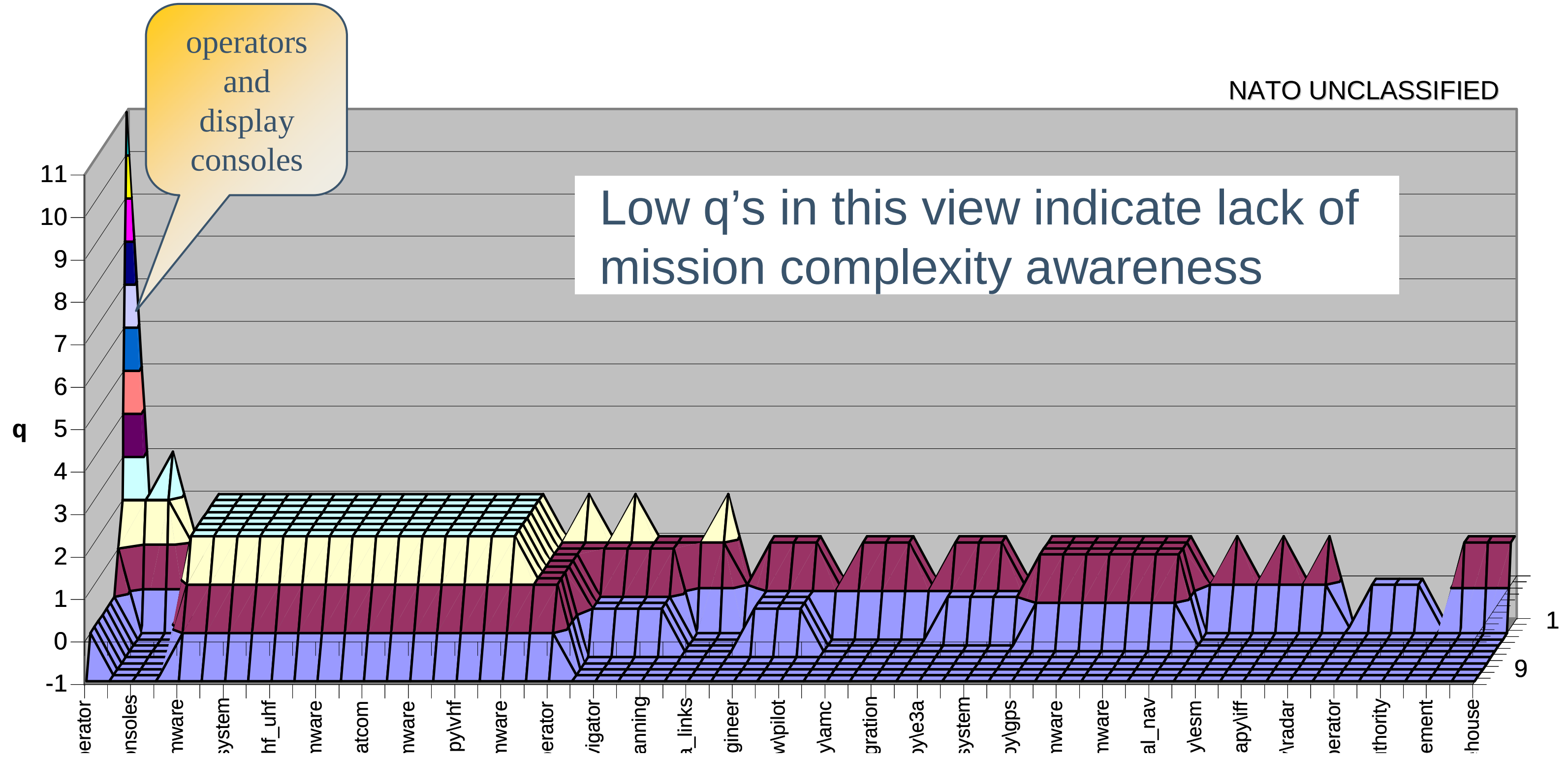
FC, IT devt

Areas of isolation & missing alignment processes

Source: An Examination of a Structural Modeling Risk Probe Technique, Anderson, Boxer & Brownsword (2006), http://www.sei.cmu.edu/publications/documents/06.reports/06sr017.html

Type III - Synchronization Risk Landscape

The **Synchronization Landscape** shows that the predominant mission awareness integration point is the system operator and the operator’s display console.



operators and display consoles

Low q’s in this view indicate lack of mission complexity awareness

Source: An Examination of a Structural Modeling Risk Probe Technique, Anderson, Boxer & Brownsword (2006), http://www.sei.cmu.edu/publications/documents/06.reports/06sr017.html