Achieving Agility in Cyberspace

Dr Philip Boxer

Adapted from NDIA presentation given at NDIA Oct 2007
By Philip Boxer, Ed Morris and Bill Anderson

Boxer Research Ltd

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*

Boxer Research Ltd

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

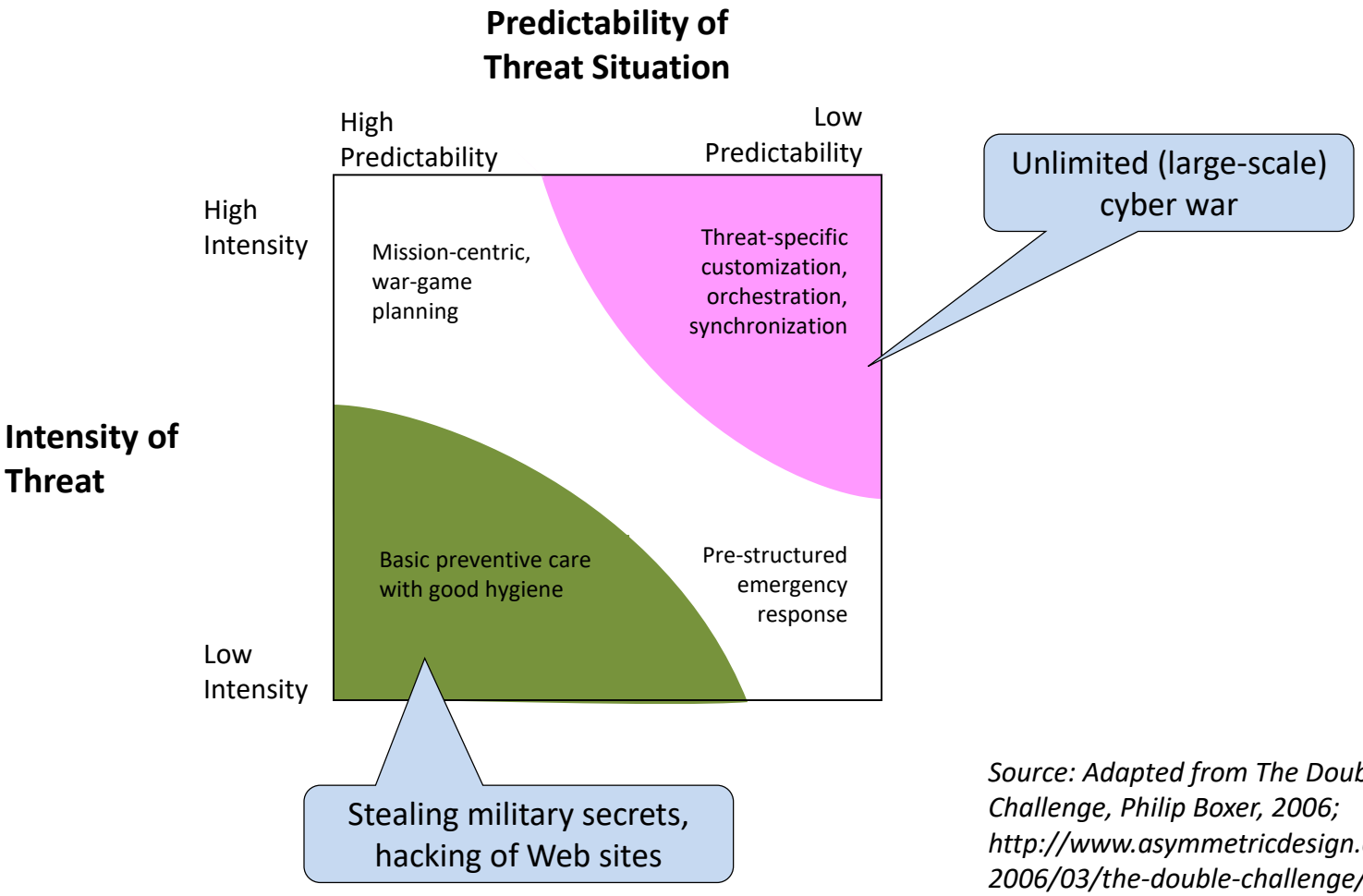
Boxer Research Ltd

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

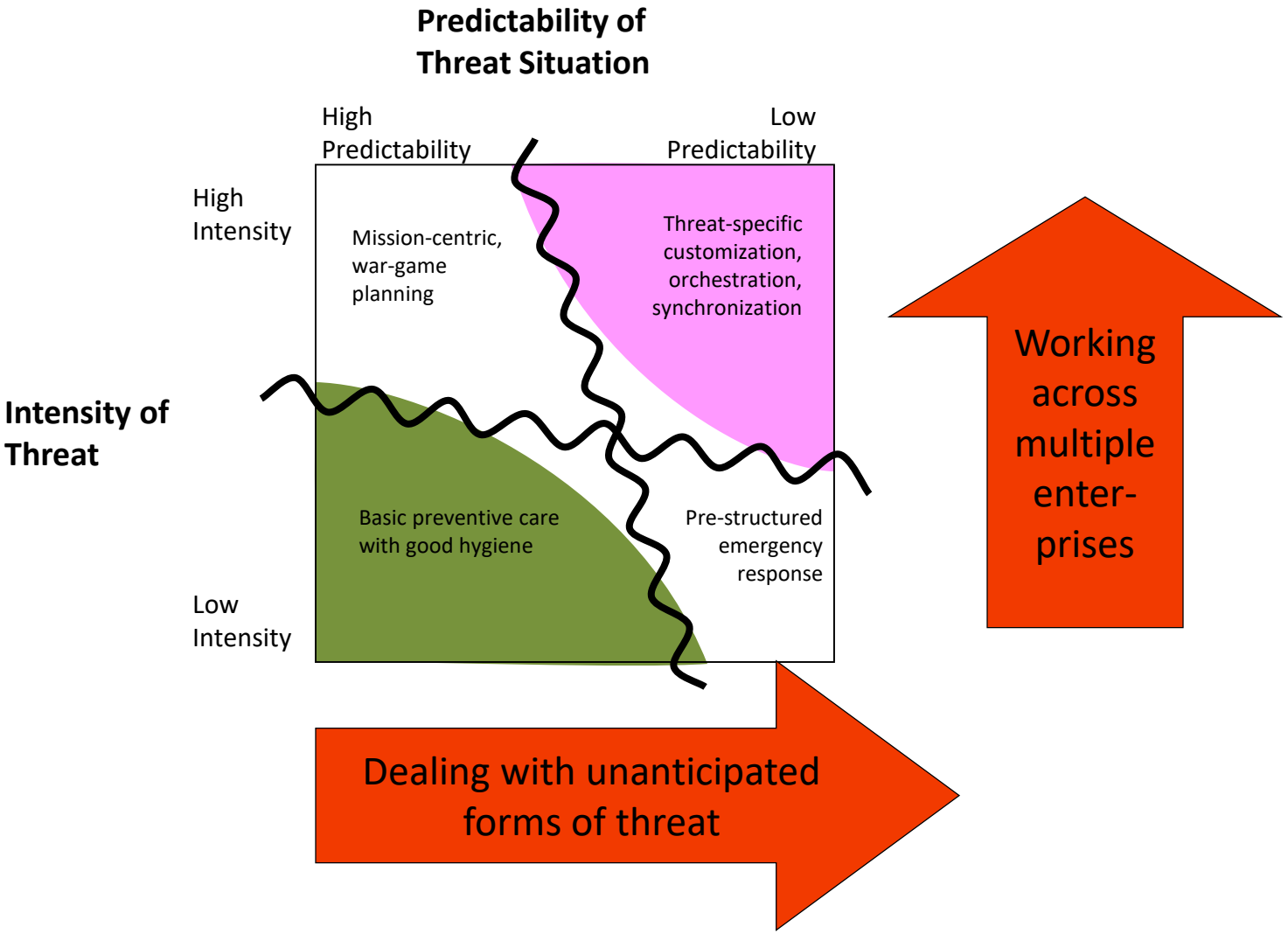
Framing the Cyberspace Theater



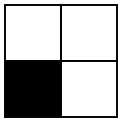
Source: Adapted from The Double Challenge, Philip Boxer, 2006; http://www.asymmetricdesign.com/2006/03/the-double-challenge/

Boxer Research Ltd

The Cyberspace Theater's Double Challenge



Boxer Research Ltd



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

Boxer Research Ltd

Low-Intensity, Low-Predictability Threats

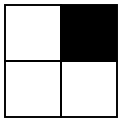
- Adversaries place unanticipated demands on the organization:
  - Malicious agent employs a novel strategy, exploits a new flaw, or targets a new victim.
  - Some form of emergency response is required.
- Activities supporting this function include:
  - coordinating the response to counter the threat
  - 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

Boxer Research Ltd

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

Boxer Research Ltd



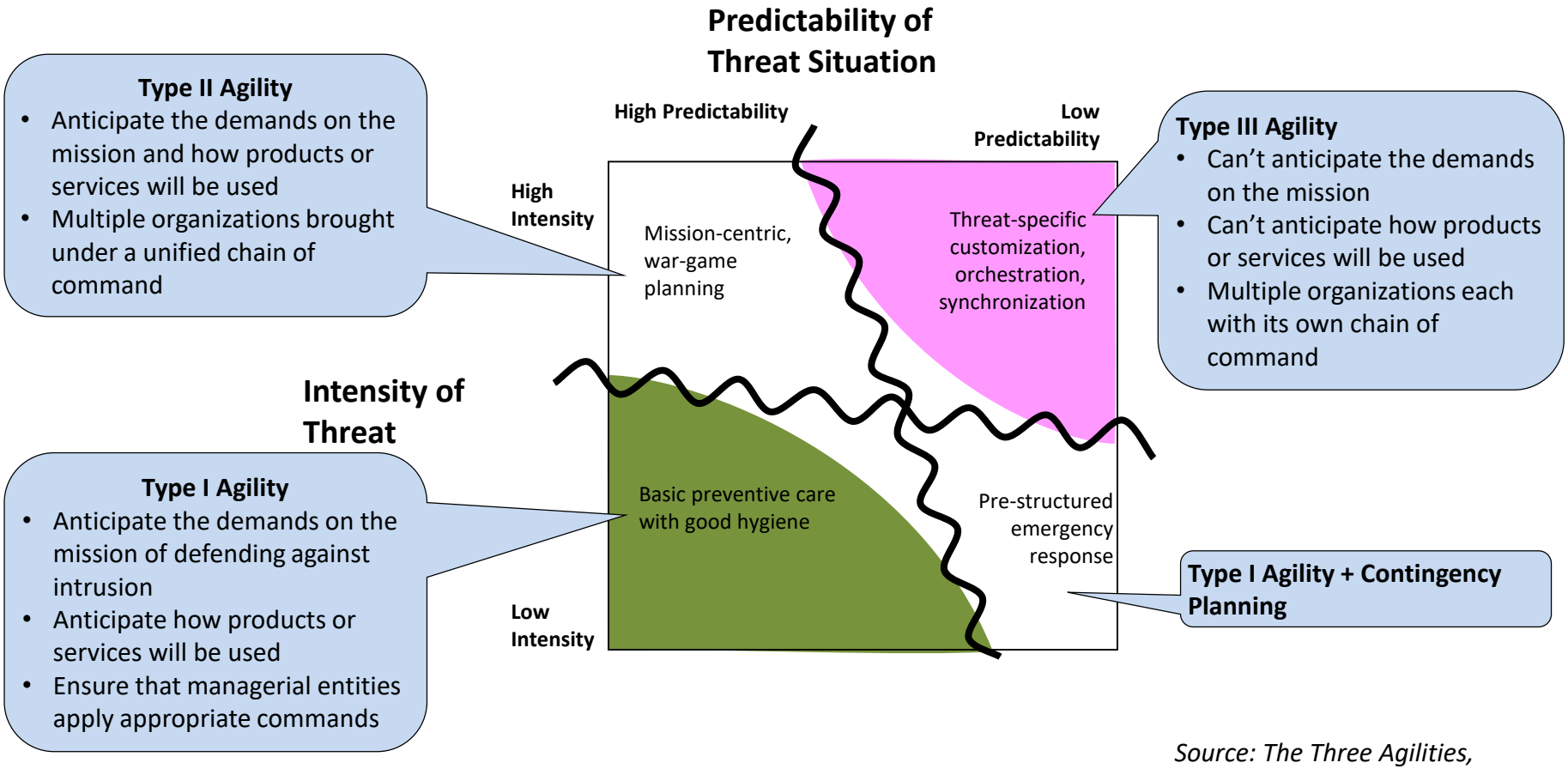
High-Intensity, Low-Predictability Threats

- 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.

Boxer Research Ltd

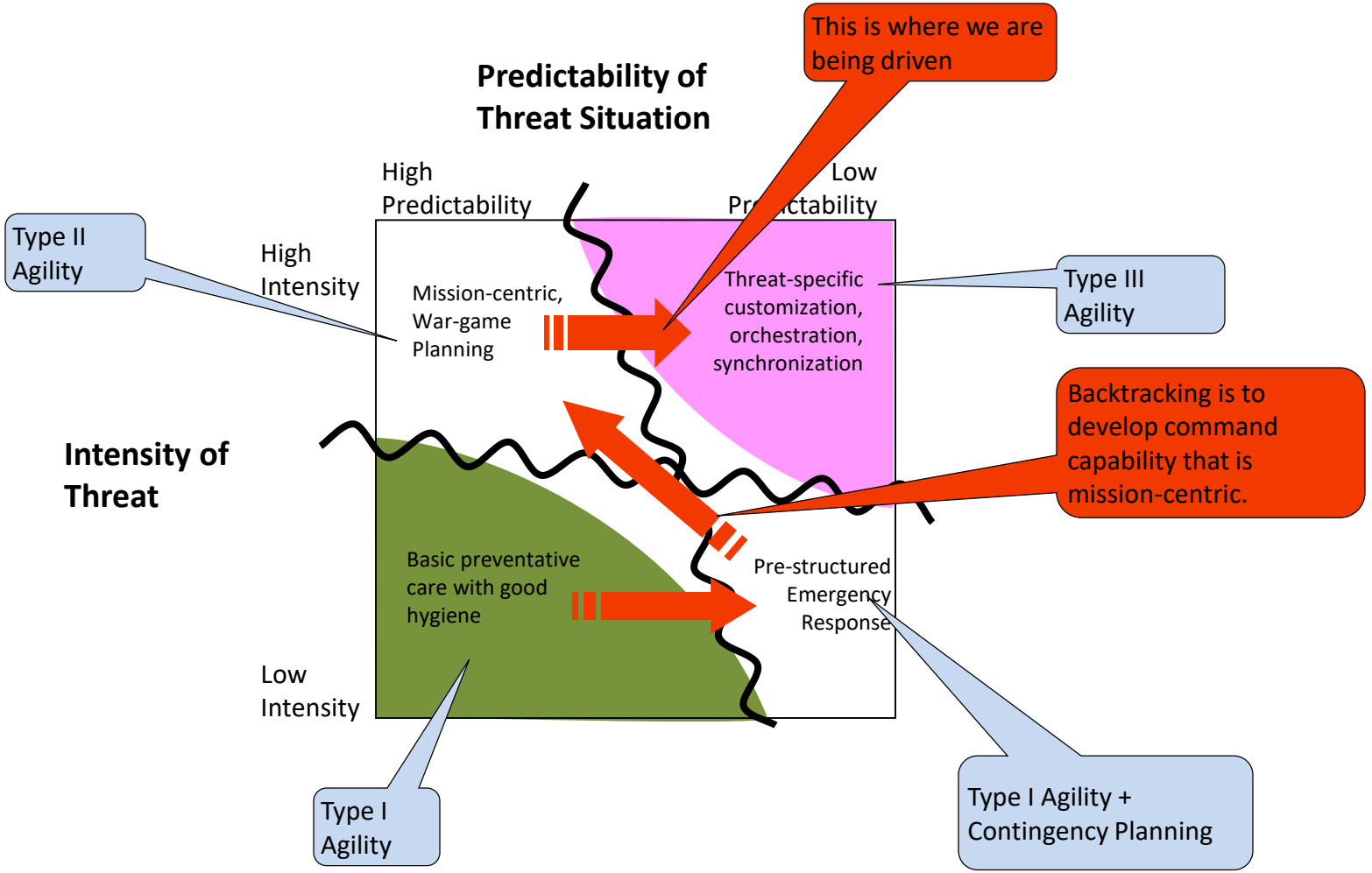
Forms of Agility Required



Source: The Three Agilities, Philip Boxer & Richard Veryard, 2006; http://www.asymmetricdesign.com/2006/01/3-agilities/

Boxer Research Ltd

An Unfortunate Trend



Boxer Research Ltd

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**

Boxer Research Ltd

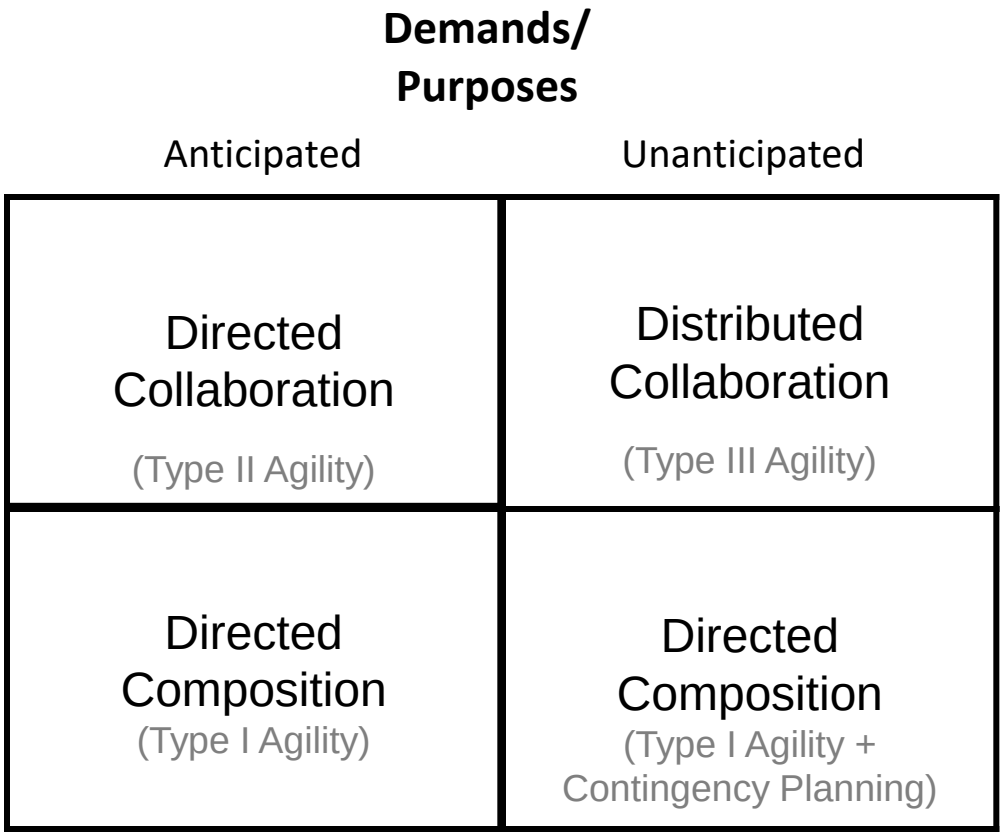
Distinguishing Forms of Command

- 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*

Boxer Research Ltd

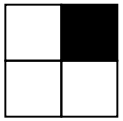
Mapping Command Types to Agility Types



Adapted from : Type III Agility, Philip Boxer, 2006; http://www.asymmetricdesign.com/2006/01/type-iii-agility/

Boxer Research Ltd

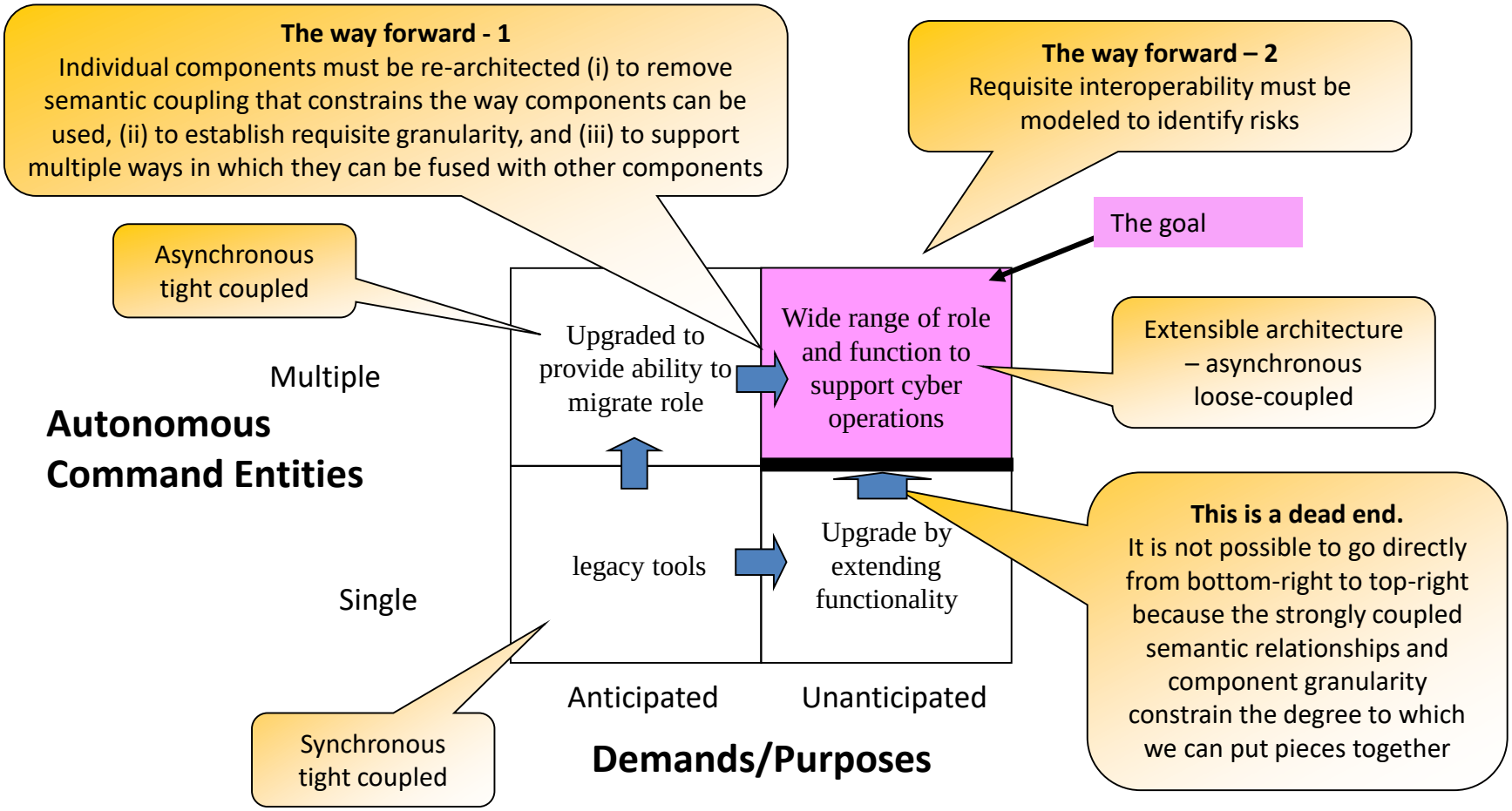
Distributed Collaboration, Type III Agility Requires Edge-Synchronization



- 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.

Boxer Research Ltd

How do we get there?



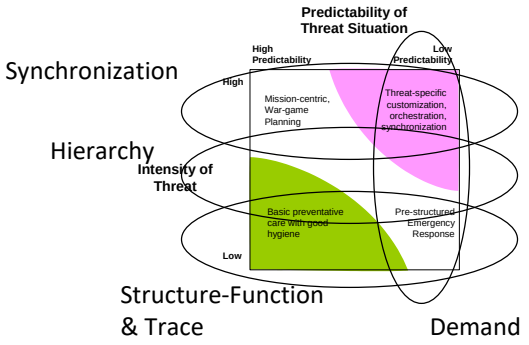
Taken from outputs of project reported in: Anderson, W., P. Boxer, and L. Brownsword, An Examination of a Structural Modeling Risk Probe Technique, 2006, CMU/SEI-2006-SR-017: Pittsburgh.

Boxer Research Ltd

Model interoperability

through command structures/infrastructures within contexts-of-use

- 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.

Approach adapted from: Anderson, W.B. and P. Boxer. Modeling and Analysis of Interoperability in Systems of Systems Environments. in IDGA Systems of Systems Engineering Forum. 2009.

Boxer Research Ltd

For More Information

Dr Philip Boxer

Philip.Boxer@brl.com

Boxer Research Ltd