"Gaming versus Exercises: Designing Surprise-resilient Organizations for a Cybered World"

Chris C. Demchak

Professor, United States Naval War College

Co-Director, Center for Cybered Conflict Studies

Strategic Research Department

Newport, Rhode Island, USA 02841

Views expressed are not those of the US Government or the US Navy .

Cyberspace imposes wide range of conceivable forms of nasty surprises to critical Socio-Technical-Economic Systems

- Possible on global scale,
- Including those from unintentional acts or just poorly coded attacks
- Multiplies knowledge and sense-making problems many times over for leaders and institutions ensuring national security

FOUR Layers of Complex Systems Surprise inherent in Global, Open Cyberspace

- **Layer One: LTSs, Largescale Complex Socio-Technical Systems, "Normal accident" in surprise-prone large cybered organizations)**

- **Layer Two (all above plus: CIP, Critical Infrastructure LTSs (protected status, many linked organizational and technical systems)**

- **Layer Three (all above) plus :mass volume Bad Actors (average to good skills, ubiquitous from script kiddies to vast majority of botnet masters, volunteer anarcho-hactivists and less well skilled nation states)**

- **Layer Four (all above) plus: highly skilled low volume Wicked Actors (high threat persistent motivations, exquisite skills, ability to organize, access/evasion expertise, or wide deep harm propagation potential)**

Must to learn to be resilient when embedded and vulnerable to globally complex system

- Resilience to surprise must be developed inside the socio-technical system, especially its security units.
- Need to develop collective sensemaking AND a menu of doable rapid accurate actions under urgent conditions (*)
  - In addition to comprehensive data inside and outside the institution
  - Must have collective trust among those responsive, mitigation or improvisation or innovation knowledge foundations, and holistic understanding of the wider environments involved.

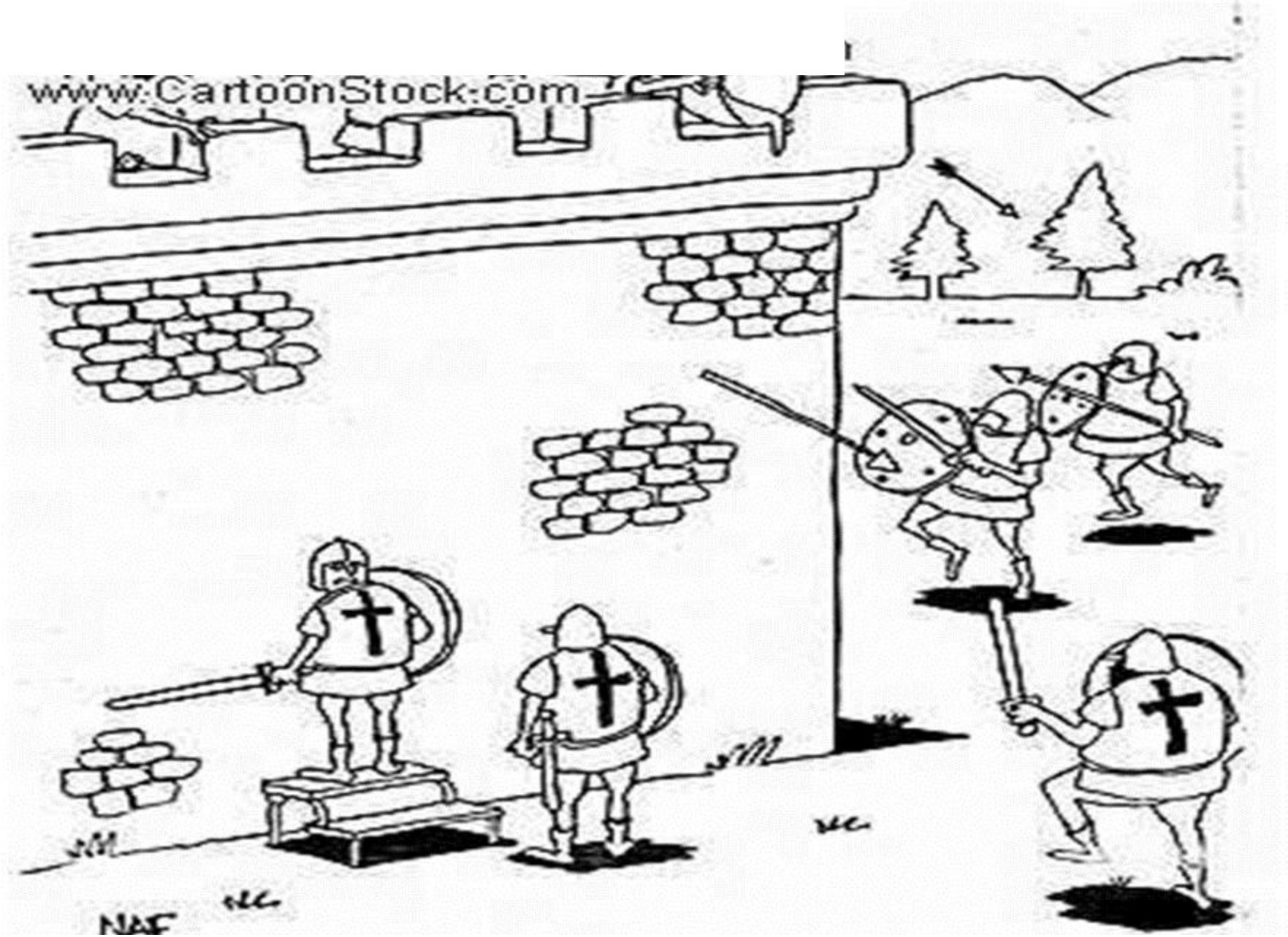
* From L. Comfort, A. Boin, and C. Demchak, eds. 2010. Designing Resilience. U of Pittsburgh Press

Exercises that worked in the past are today need virtual advances for surprises of cybered conflict

- See cyberspace narrowly as “domain” so limit environment
- Construct exercises for known roles and responses
- One-offs, even if annual event
  - No replay on the spot to test alternative hypotheses
- Usually do not play to “break” because want to bound the training or events
  - Reverberations beyond scenario at best second order
- Educates those who design it and those who directly play, few others
- Not widely available for replay, update, dissemination

Exercise Shortcomings in Values

- **do not collect tacit knowledge continuously, develop it, or allow the widespread reuse of this data.**
- **Do not prepare adequate capabilities against surprise across multitude of actors in complex socio-technical systems**
- **Even cyber ranges suffer from narrowness of vision**



"Oh great! We trained only with BIG ladders"

Basic Lessons about Responding to Surprise

from Complexity, LTS and Complex Adaptive Social System Research

Complexity Research Major Lessons

1. ***Only Trends can be forecast*** *with knowable/unknowable unknowns*
2. ***Path Dependence*** *powerful*
3. ***Channeling trends*** *is best possible accommodation option*

Largescale Technical Systems Research Major Lessons

1. ***Trial and Error best*** *to acquire knowable unknowns*
2. ***Tighter coupling increases potential rippling*** *error paths*
3. ***Redundancy and Slack*** *powerful accommodators*
4. ***Knowledge is expensive*** *in time, money, staff attention, implementation*

Complex Adaptive Social Systems Research Major Lessons

1. ***Human buy-in essential*** *for effectiveness (legitimate, useful, doable)*
2. ***Cultural filters powerful*** *(socialization, operationalization hard to control)*
3. ***Largescale socio-technical systems drift readily*** *into unnoticed critical coupling and a lack of urgency to absorb or seek knowledge*

FOUR Types of MultiSource Threat Categories in Increasing Uncertainty and Surprise Potential	Cybered Resilience Action Requirements (including Disruption Supplement)
Complexity in Largescale Complex Socio-Technical Systems, LTSs (basic "normal accident" and cascading surprise-prone large cybered organizations)	
(all above) plus Criticality for Nation CIP, Critical Infrastructure LTSs (protected status), High Reliability Industry, or Operationally Engaged Military	
(all above) plus high volume Bad Actors (average to good skills, ubiquitous from script kiddies to vast majority of botnet masters, volunteer anarcho-hactivists and less well skilled nation states)	
RESILIENCE	
DISRUPTION	
(all above) plus highly skilled low volume Wicked Actors (high threat persistent motivations, exquisite skills, ability to organize, access/evasion expertise, or wide deep harm propagation potential)	

Organizations need to “Play It Through” using advantages of virtual worlds

- Virtual reality simulations, if done correctly, can allow organizational members to play out their experiences and hypotheses with others, developing richer options for response to surprise
- Gathers tacit knowledge in ways that meet the graphical and spatial predilections of humans in easy, useful, and collaborative mechanisms
- Members can develop trust relations with those playing, and engage instinctively in performance assessments
- Can be re-used, replayed, reviewed, analyzed, and reconsulted later – trial-and error learning
- IF co-authored, the tacit knowledge can be provide remarkably informed innovative responses to surprise because they or someone has played through

The Gaming needs to be Fully Embedded in Shared Practices of the Organization

- Knowing when to seek more knowledge is the sense-making of resilience
  - Requires seeking what can be known continuously and keeping that tacit knowledge for ubiquitous operational use
- Embedded organizational high-fidelity, continuously available, co-authored, game-based simulations
  - Daily practice of contributing reinforced by relatively frequent episodes of development of competence under surprising conditions
  - Actors unusually educated about overall system
- Advantages
  - Maintenance of knowledge closely monitored
  - Environmental surprises constantly explored
  - Cognitive resilience encouraged
    - by ability to test ideas for local actions and see how they blend
  - Operational knowledge exchanges practiced broadly with different actors or same ones

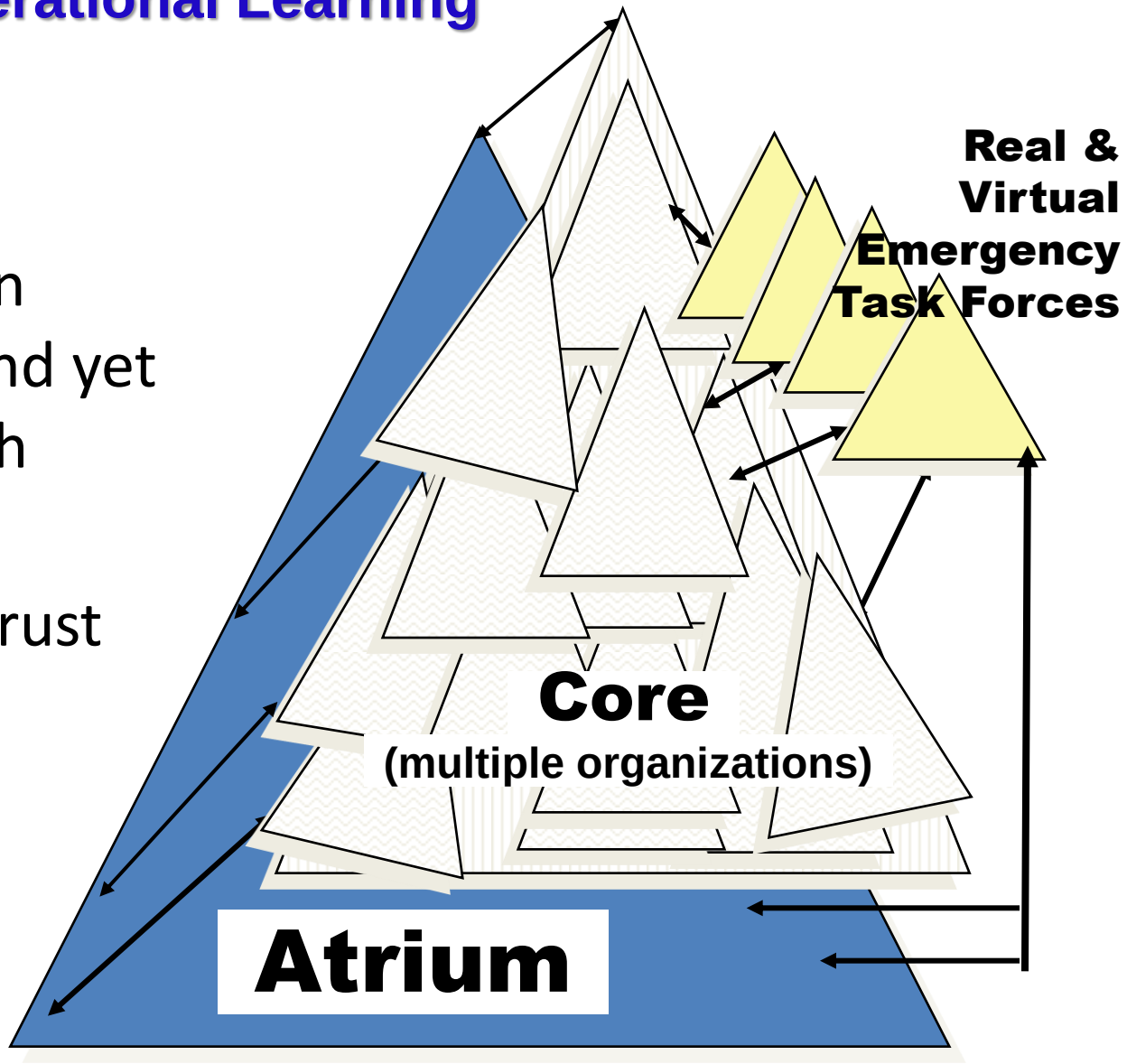
Operationalized real time surprise

Gaming and an Atrium Organization

- Embed operationalized on-call gaming in the organization
- Trial-and-error learning is easy, accessible, and useful
- Key attributes: High fidelity, continuously available, co-authored game-based simulations embedded in shared practices of critical organizations
- Encourages knowledge redundancy, along with novel approaches to slack.

ATRIUM for Cross Organizational Cyber Gamed Operational Learning

- Only possible in cybered world
- Can segregate own sensitive files and yet still play through
- Builds cross organizational trust continuously
- Builds inter-organizational knowledge sets



" Wow! … for a moment there, it all made sense!"

Chris.demchak@usnwc.edu