Examining Cooperative Strategies through Cyber Exercises

Presented to
March Technical Colloquium
Forum for Incident Response and Security Teams (FIRST)

Ernest W. Drew, III
March 26,2008
Tokyo, Japan

Norwich University Applied Research Institutes (NUARI) 57 Old Freight Yard, PO Box 30, Northfield, VT 05663-0030 +1 802 485 2755

Cyber Conflict – A Difficult Problem for Nations and Enterprises

The conduct of large scale, politically motivated conflict based on the use of offensive and defensive capabilities to disrupt digital systems, networks, and infrastructures, including the use of cyberbased weapons or tools by nonstate/ transnational actors in conjunction with other forces for political ends

Definition adopted by the Cyber Conflict Studies Association
www.cyberconflict.org

Mulvenon, James "Toward a Cyberconflict Studies Research Agenda", IEEE SECURITY & PRIVACY JULY/AUGUST 2005

Observations

- **Lack of Cyber Situational Awareness:**
  There does not appear to be an organization at national levels responsible for ***providing*** cyber situational awareness to:
    - Government Agencies
    - Private Sector Enterprises
- **Who is in Charge ?:**
  What National Agency or Private Sector Enterprise is responsible for taking the lead in response to a Cyber Attack?
    - Whose laws apply?
    - Whose regulations apply?
    - Is it just a civilian problem or will militaries become involved?

Roadblocks to Coordination

- Laws restrict what an Enterprise can do to defend against attack
- Privacy concerns limit the sharing of information
- Regulators place constraints on information sharing
- Cooperation among Nations - Treaty requirements
- The problem of Attribution
- The number of devices and the number of human interactions create complex environments

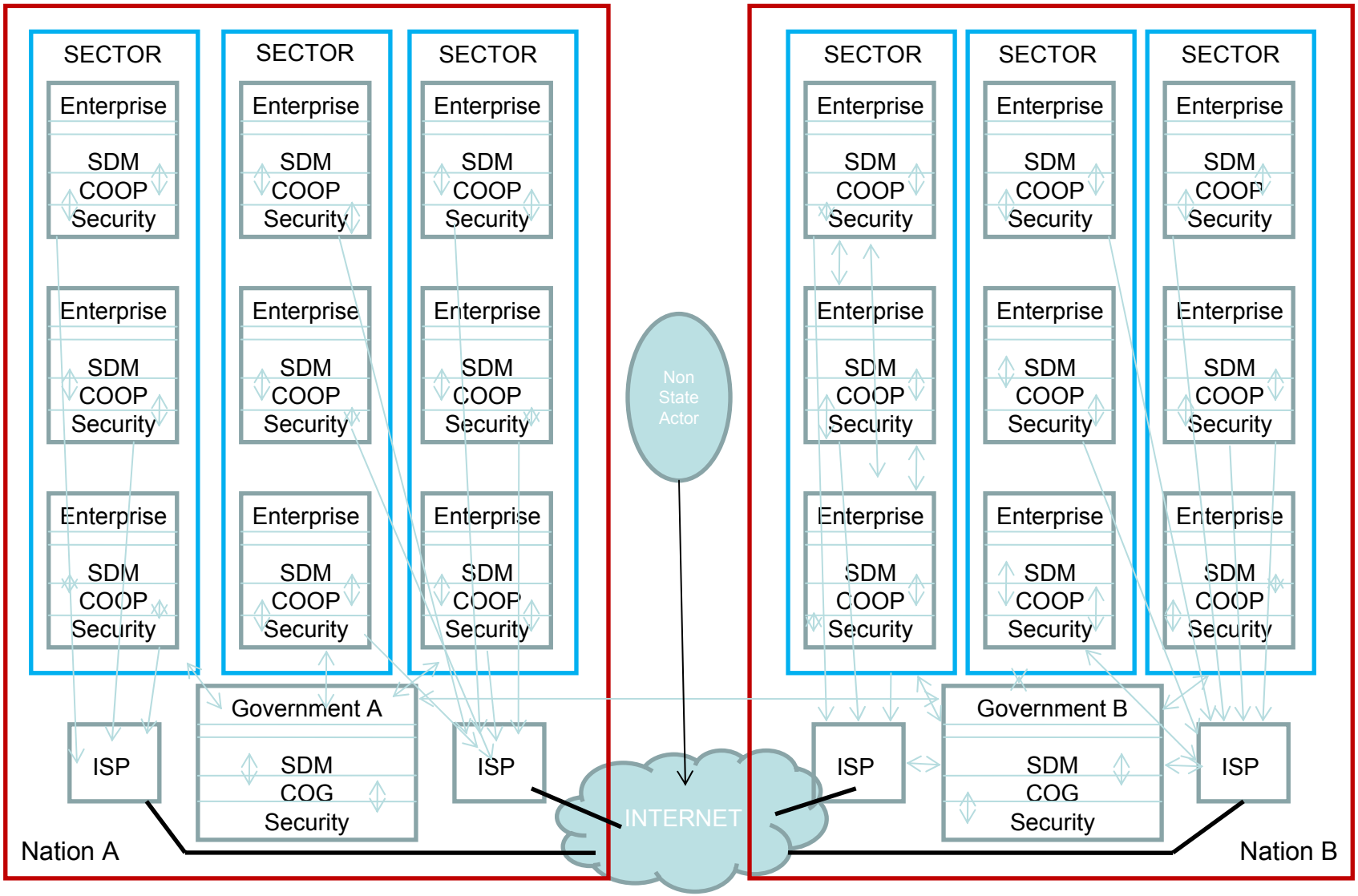
Complexity

- *Structural complexity* is based upon the number of parts in a system. The larger the number of independent parts in a system, the greater its structural complexity.
- *Interactive complexity* is based upon the behavior of the parts and the resulting interactions between them. The greater the freedom of action of each individual part and the more linkages among the components, the greater is the system's interactive complexity.

The U.S. Army Commander's Appreciation and Campaign Design , **TRADOC Pamphlet 525-5-500 , January 2008**

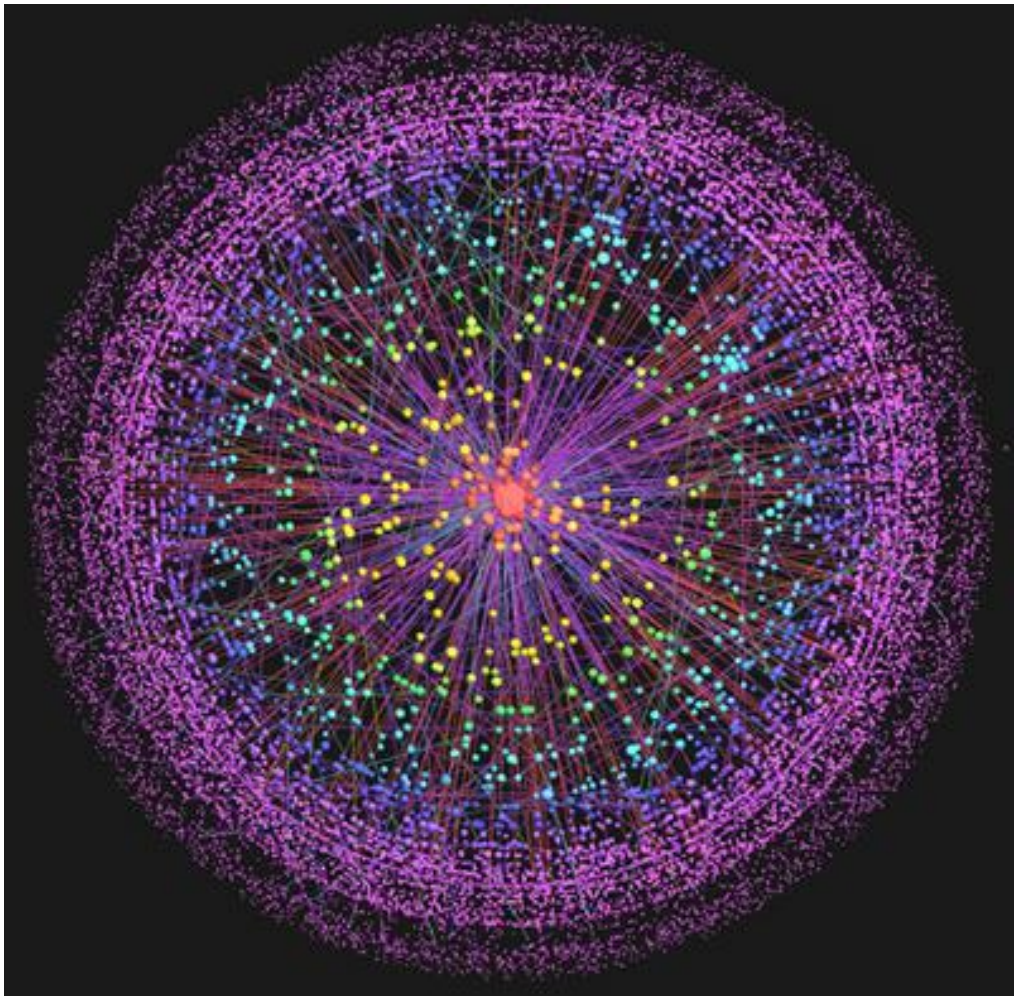
http://www-tradoc.army.mil/tpubs/pams/p525-5-500.pdf

A Simple Complexity Illustration



Norwich University Applied Research Institutes (NUARI) 57 Old Freight Yard, PO Box 30, Northfield, VT 05663-0030 +1 802 485 2755

The Complexity of the Internet



Lanet-vi program of I. Alvarez-Hamelin et al.

Norwich University Applied Research Institutes (NUARI) 57 Old Freight Yard, PO Box 30, Northfield, VT 05663-0030 +1 802 485 2755

Cyber Conflict Response: a "Wicked Problem"

- Horst Rittel, a professor of Design at UC Berkeley, in1972 stated that characteristics of socially complex problems, were as he defined; "Wicked Problems"
  - not wicked in the sense of evil, but rather extremely difficult
- The response to Cyber Conflict, because of its complexity, can be defined as a "Wicked Problem"

Horst W. J. Rittel, "On the Planning Crisis: Systems Analysis of the 'First and Second Generations,'" *Bedriftsøkonomen* 8 (1972), pp. 392-393
http://www.uctc.net/mwebber/Rittel+Webber+Dilemmas+General_Theory_of_Planning.pdf

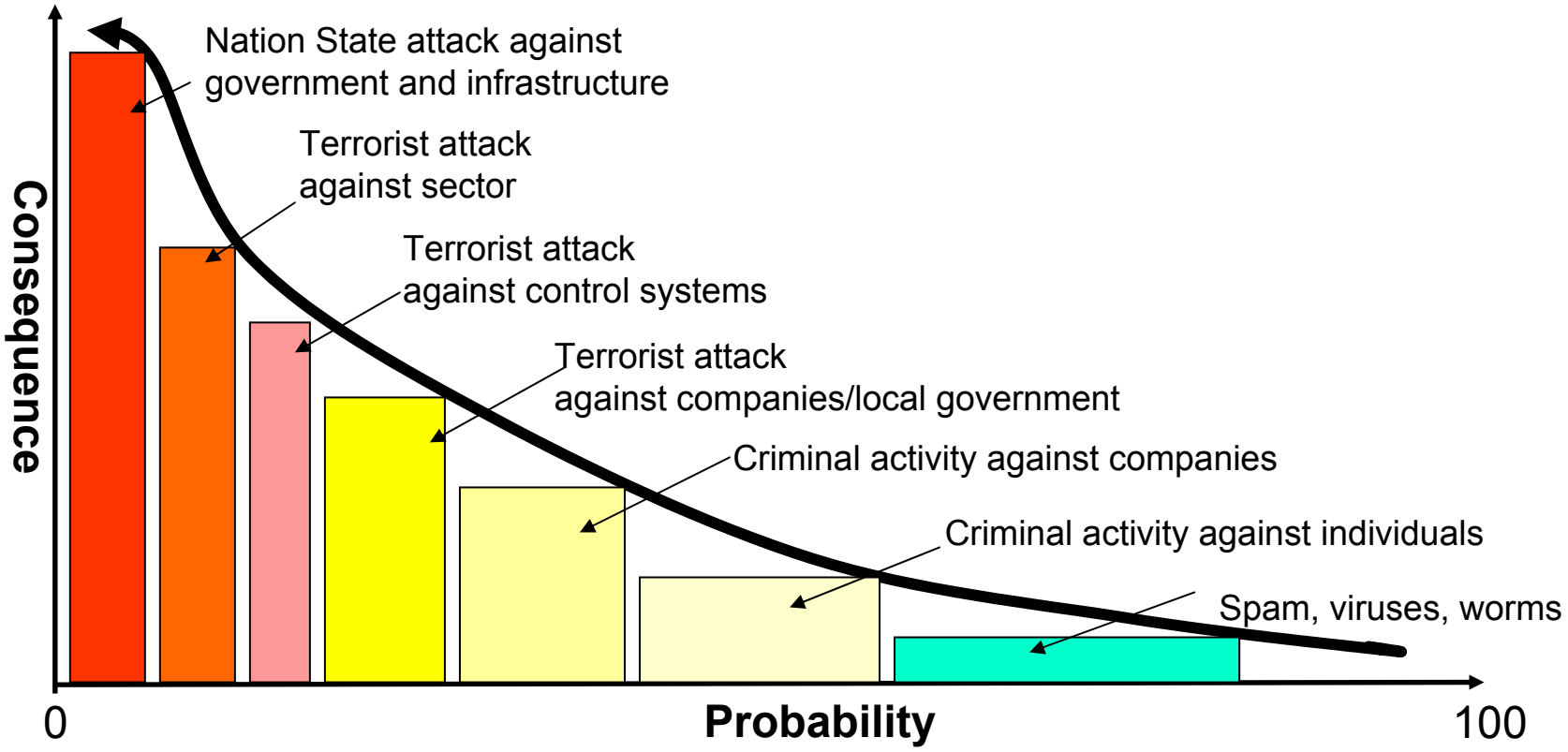
Properties of a “Wicked Problem”

1. There is no definitive formulation of a wicked problem.
2. Wicked problems have no stopping rule.
3. Solutions to wicked problems are not true-or-false, but better or worse.
4. There is no immediate and no ultimate test of a solution to a wicked problem.
5. Every solution to a wicked problem is a "one-shot operation"; because there is no opportunity to learn by trial-and-error, every attempt counts significantly.
6. Wicked problems do not have an enumerable (or an exhaustively describable) set of potential solutions, nor is there a well-described set of permissible operations that may be incorporated into the plan.
7. Every wicked problem is essentially unique.
8. Every wicked problem can be considered to be a symptom of another problem.
9. The existence of a discrepancy representing a wicked problem can be explained in numerous ways. The choice of explanation determines the nature of the problem's resolution.
10. The planner has no right to be wrong (planners are liable for the consequences of the actions they generate).

Horst W. J. Rittel and Melvin M. Webber, “Dilemmas in a General Theory of Planning,” *Policy Sciences* 4 (1973), pp. 155-169. © Elsevier Scientific Publishing Company, Amsterdam

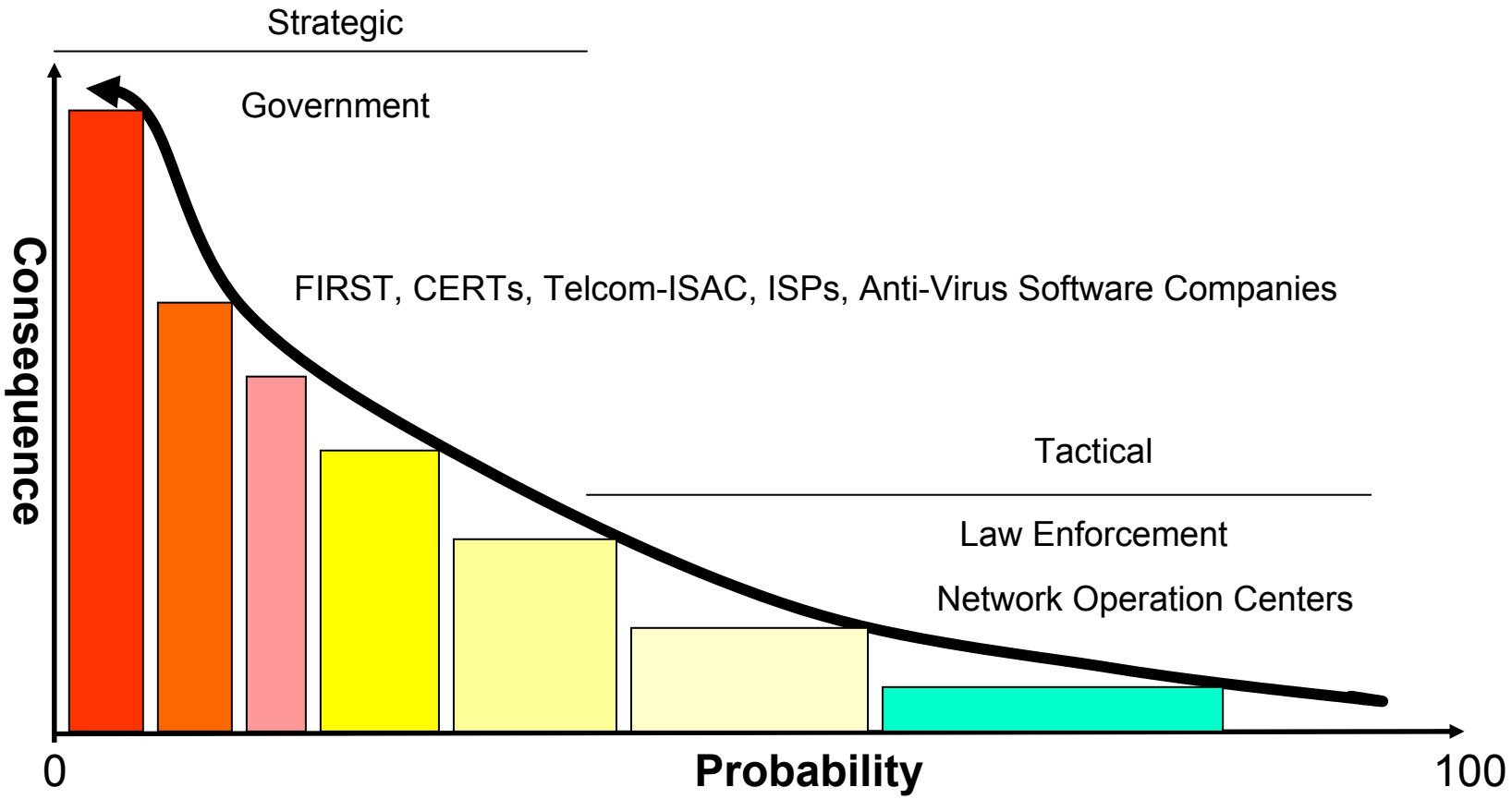
http://www.uctc.net/mwebber/Rittel+Webber+Dilemmas+General_Theory_of_Planning.pdf

Representative Types of Cyber Attacks



Norwich University Applied Research Institutes (NUARI) 57 Old Freight Yard, PO Box 30, Northfield, VT 05663-0030 +1 802 485 2755

Representative Responders for Cyber Attacks



Norwich University Applied Research Institutes (NUARI) 57 Old Freight Yard, PO Box 30, Northfield, VT 05663-0030 +1 802 485 2755

Definition of a Cyber Exercise

An activity that replicates disruption of computers and information systems to stimulate the decision-making processes of participants. The participants make decisions based on their plans, policies and procedures, the decisions will then impact the course of events.

A specialized emergency preparedness exercise designed to look at emergencies caused by disruption of the IP infrastructure. These disruptions can be man-made, the result of a natural disaster, or the infrastructure coming under attack by hackers, criminals, terrorists, or other governments

Cyber Storm – Findings 1 of 4

• **Finding 1: Interagency Coordination.** While the Interagency Incident Management Group (IIMG)*1* and National Cyber Response Coordination Group (NCRCG) activated and interacted constructively during the exercise, further refinement is needed for operations and coordination procedures. Broader understanding, both within government and in the private sector, of the thresholds and ramifications of activation of these bodies will also improve interagency coordination. Specifically the cyber community needs to better understand the readiness and security postures to be considered based on such activations, as well as the level of Federal engagement they imply.

http://www.dhs.gov/xlibrary/assets/prep_cyberstormreport_sep06.pdf

Cyber Storm – Findings 2 of 4

• **Finding 2: Contingency Planning, Risk Assessment, and Roles and Responsibilities.** Formal contingency planning, risk assessment, and definition of roles and responsibilities across the entire cyber incident response community must continue to be solidified. Responses were timely and well coordinated where existing process procedures were clear and fully understood by players.

• **Finding 3: Correlation of Multiple Incidents between Public and Private Sectors.** Correlation of multiple incidents across multiple infrastructures and between the public and private sectors remains a major challenge. The cyber incident response community was generally effective in addressing single threats/attacks, and to some extent multiple threats/attack. However, most incidents were treated as individual and discrete events. Players were challenged when attempting to develop an integrated situational awareness picture and cohesive impact assessment across sectors and attack vectors.

Cyber Storm – Findings 3 of 4

• **Finding 4: Training and Exercise Program.** An established training and exercise program will strengthen awareness of organizational cyber incident response, roles, policies, and procedures.

• **Finding 5: Coordination Between Entities of Cyber Incidents**. Response coordination became more challenging as the number of cyber events increased, highlighting the importance of cooperation and communication across the community.

• **Finding 6: Common Framework for Response and Information Access.** A synchronized, continuous flow of information available to cyber incident stakeholders created a common framework for response, impact development, and discussions. Early and ongoing information access strengthened the information-sharing relationship between domestic and international cyber response communities.

Cyber Storm – Findings 4 of 4

• **Finding 7: Strategic Communications and Public Relations Plan**. Public messaging must be an integral part of a collaborated contingency plan and incident response to provide critical information to the response community and empower the public to take appropriate individual protective or response actions consistent with the situation.

• **Finding 8: Improvement of Processes, Tools and Technology.** Improved processes, tools, and training—focused on the analysis and prioritization of physical, economic, and national security impacts of cyber attack scenarios—would enhance the quality, speed, and coordination of response. This is particularly true in the case of integrated or cascading attacks or consequences.

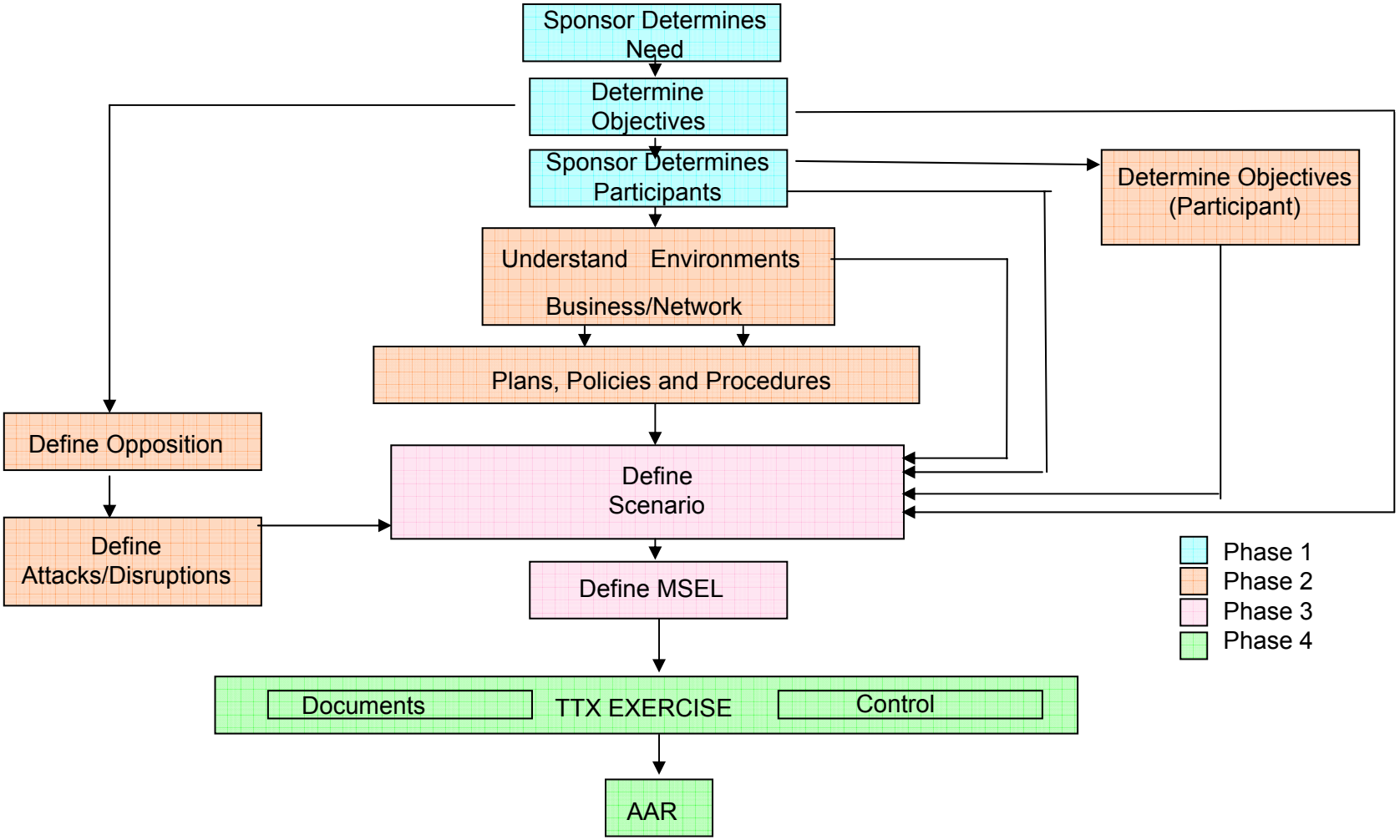
Cyber Exercise - Outcomes

Outcomes may include strategies and planning frameworks to:

- Coordinate responses and consequence management to cyber-attacks among:
  - Governments
  - Organizations
  - Enterprises
- Maintain continuity of operations within participating organizations – COOP and COG
- Sustain confidence in government information networks during a cyber-attack and, if necessary, regain public confidence.

Backup Slides

Design Requirements for Cyber Exercises



Norwich University Applied Research Institutes (NUARI) 57 Old Freight Yard, PO Box 30, Northfield, VT 05663-0030 +1 802 485 2755

Types of Cyber Exercises

- Tabletop Exercises
  - Tabletop Exercises involve senior staff and other key personnel in an informal setting to discuss simulated situations. This type of exercise is intended to stimulate discussion of various issues regarding a hypothetical situation. It can be used to assess plans, policies, and procedures.
- Functional Exercises
  - The Functional Exercise (FE) is designed to test and evaluate individual capabilities, multiple functions or activities within a function, or interdependent groups of functions….. The objective of the FE is to execute specific plans and procedures and apply established policies, plans, and procedures under crisis conditions, within or by a particular function team(s).
- Full-Scale Exercises
  - In a Full-Scale Exercise (FSE), prevention and response elements are required to mobilize and deploy to a designated site or locale in response to a simulated attack, generally for an extended period. It involves testing a major portion of Operations Plans and organizations under field conditions

Homeland Security Exercise and Evaluation Program Volume I: Overview and Doctrine
http://www.crcpd.org/Homeland_Security/HSEEPv1.pdf

Participants

- In a Cyber Exercise players come from many organizations. They are usually representatives who have active roles in the daily management, operations, and security of their information networks, systems, and infrastructure.
- These participants play key roles in responding and managing the consequences of the significant cyber disruption presented in the scenario injects.
- Participation is usually voluntary, however depending on the objectives of the exercise, it may be necessary to make participation mandatory for designated personnel.
- The exercise may have Private Sector enterprises, ISP's, Managed Security Providers, law enforcement, regulatory agencies, and governments both local and national.

Role of Opposition Team

An opposition team should develop their assumptions, determine their resources, and planned their specific attacks

The opposition team is normally an extension of control and should take into account the objectives of the sponsor in order that specific attacks will stimulate a response that can be tied back to an objective