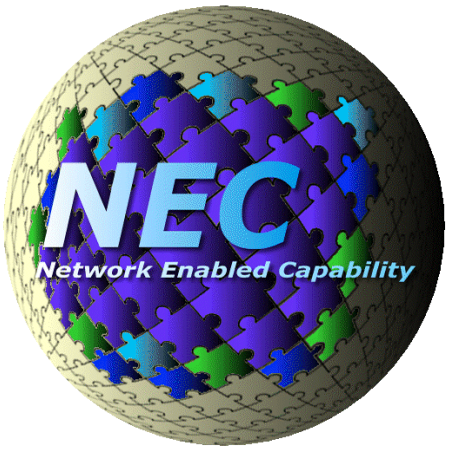
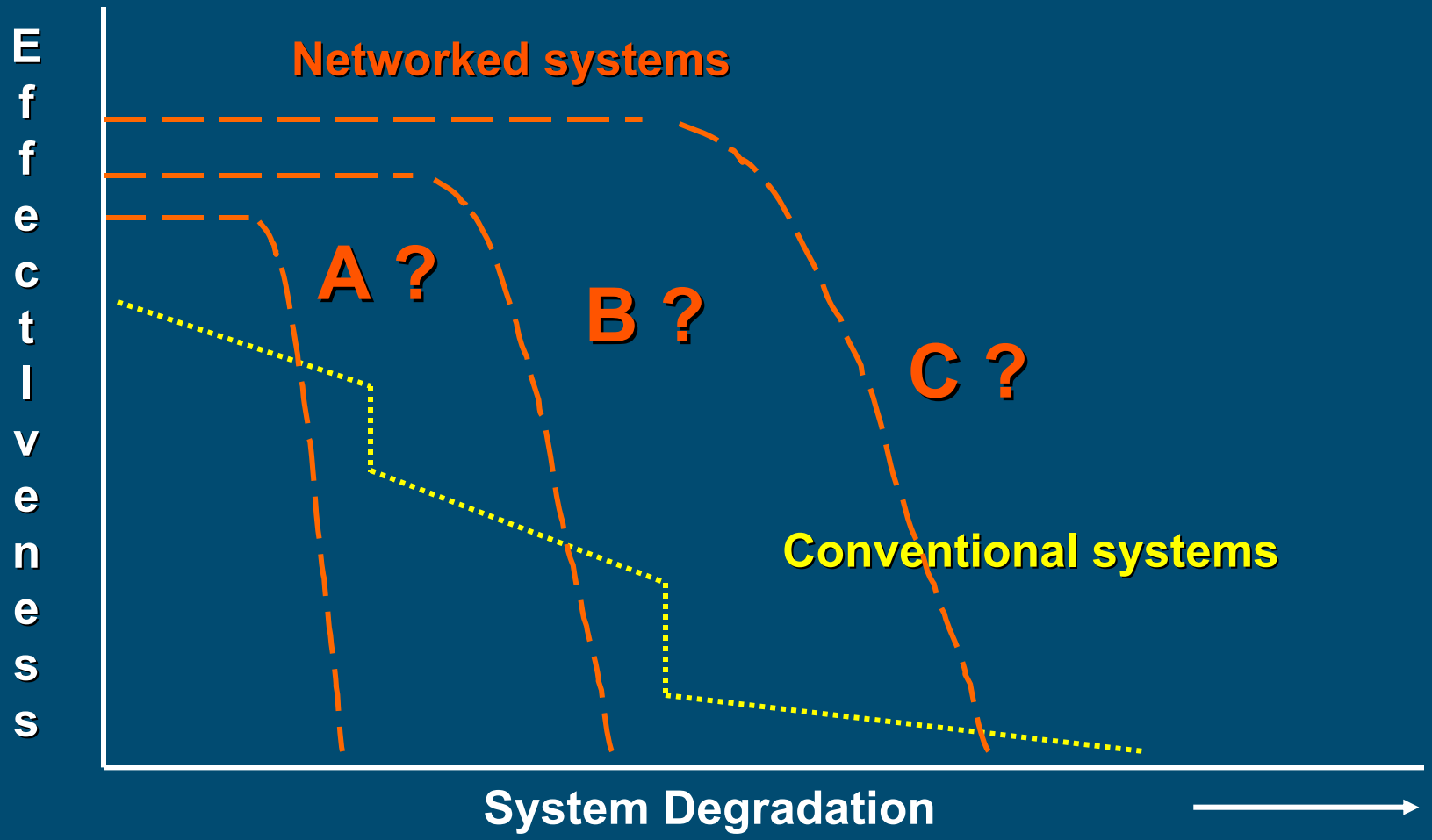
NEC Concepts - Risks and Vulnerabilities

Peter Houghton

9th ICCRTS, Copenhagen
14 September 2004



NEC - another proposition



NEC - Order of Magnitude changes?

- We tend to focus on the positive aspects of new initiatives
  - We forget that our opponents will continue to find ways to exploit weaknesses in any new approaches we develop *(they will specifically avoid playing to our strengths)*
- A warning from Scherrer[1]:
  - ""We must use all types, forms, and methods of force, and especially make more use of non-linear warfare and many types of information warfare methods which combine native and Western elements to use our strengths in order to attack the enemy's weaknesses, avoid being reactive, and strive for being active. In this way, it will be entirely possible for China to achieve comprehensive victory over the enemy even under the conditions of inferiority in information technology." - General Wang Pufeng, Chinese Red Army

Scherrer, J.H., Risks and Vulnerabilities of Network-Centric Forces: Insights from the Science of Complexity, Feb 2003.

Why consider NEC risks and vulnerabilities?

- Focus to date has been on promoting the concept, combined with advancing ideas and understanding
  - Arguably NEC concept is now sufficiently established
- Thus prudent to consider potential negative consequences of such an *approach*
- First we have to accept that such weaknesses exist and commit to dealing with them
  - Our opponents will not stand still - specifically they will avoid our strengths and target our weaknesses
  - Sceptics accept the potential benefits of IS technologies but contend that a more scientific foundation is needed for remainder
- Requires investment of a proportionate degree of effort

Scope

- Not technical vulnerabilities related to equipment
- Focuses on understanding the wider systems problems and concerns
  - Potential weaknesses in our approaches
  - How opposing forces might exploit such weaknesses
  - How those weaknesses may make us vulnerable to self-inflicted damage
  - Ways to reduce our weaknesses or to limit the ability of our opponents to exploit them
- Snapshot only

Other challenges

- Technical challenges
  - Inherent vulnerabilities in technologies
  - Inability of bureaucratic and slowly adapting defence organisations to acquire, assimilate, manage and use complex technology
- Challenges to maintain a ‘scientific’ approach to NEC development
  - Danger of focussing on evidence that supports our hypotheses of NEC benefits and discounting that which does not
  - Should be seeking with equal vigour and effort evidence that disproves our hypotheses
  - Otherwise we will not understand the limitations, risks and dangers in our proposed approaches

Understanding Weaknesses

- Requires us to take seriously criticisms levelled at NCW

  "Network-centric warfare (NCW) increasingly is becoming a new orthodoxy - a set of beliefs that cannot be seriously challenged. Its disadvantages or critical vulnerabilities are not publicly discussed or are grudgingly admitted…The enemy rarely is mentioned, and he seems to be incapable of frustrating our plans and actions."

  Dr. Milan Vego

- Time to:
  - Move away from beliefs or tenets to hypotheses that can be challenged
  - Publicly expose and discuss important vulnerabilities
  - Think more about how the enemy will exploit NEC/NCW weaknesses

Risk issues

- Risks and vulnerabilities arising from:
  1. Complex adaptive behaviour
  2. Technology imbalances
  3. Network reinforcing introversion
  4. Conflict between trend for platform sophistication and network resilience based on low value and ubiquity
  5. New information environment and pressures to respond
  6. Information processing
  7. Information operations including deception
  8. Effects on command
  9. Information risks

Note: Following slides are intentionally not a complete set due to need to keep within time bounds

3. Network Reinforces Introversion

- Information superiority may disable wider communication
  - NCW intent is to gain information superiority
  - Danger is greater focus on *internal* networking ("locking out" opponents - and potentially allies)
- Risks exposed - mainly in non-attritional conflict
  - Impair conflict resolution
    - Military need to be providing others with awareness and clarity of situations (calming rather than de-stabilising effect)
    - Attacks/degradation of opponents IS can both deny calming messages and inflame situations
  - Disabling an opponents information infrastructure can make it more difficult to discern opponents intent and actions

3. Network Reinforces Introversion

For example:

- Shock and Awe
  - Or ‘closing down your opponents ability to know what is happening’
  - May be generating entrained responses, doctrine that are the exact opposite of what is required
- Self Synchronisation
  - Largely, intended to exploit SA to better control tempo
  - Emphasis has to be on internal co-ordination (self!)
  - In future operations a measured approach is needed to decision making and action which include allies, and external non-military stakeholders
  - ‘Self’ synchronisation could be wholly inappropriate in these circumstances
  - Must be cognisant that we do not inadvertently develop a design, training and culture orientated to internal (only) working

4. Platform sophistication vs ubiquity

- NCW at odds with current trends in platform numbers and value
  - Platform numbers decline and ‘value’ increases
  - Opponents likely to be asymmetric with more platforms of lesser value
- Risks exposed
  - Need to protect platforms and possibly keep out of harm’s way
- Exploitation approach
  - Opponents use numerical advantage to persuade high value platforms to retreat out of area
  - If high value platforms are also key infrastructure nodes - result is a simultaneous loss of capability and credibility

5. New Info env't & pressure to respond

- Increasing change in environment
  - Drive for increased tempo (to gain advantage)
  - Increasing amount of information collected (again to gain advantage)
- Risks exposed
  - Network architecture can provide advantage in speed and processing of data, hence:
    - could find ourselves responding to events so quickly - responding essentially to our *own stimuli*
    - may inadvertently take precipitative action and drive operation into more dangerous and precarious states

6. Information Processing

- Over-reliance on COP - an erroneous abstract picture that is neither truly shared or sufficiently representative?
  - Temptation for Command teams to be presented with “clean”, processed and filtered data
- Information management and processing could add new uncertainties
  - Little knowledge of the data sources and subsequent processing
- Risks exposed
  - Consumers have little idea what data has gone into ‘picture’, how reliable it is, what has been fused, what types of math’ processing conducted, what data may have been discarded
  - Uncertainty is shifted from operational situation to the data itself

7. Information Operations

- To counter capable forces with technology and firepower advantages opponents increasingly employ asymmetric approaches
  - (To avoid firepower) including targetting of our infrastructure
- Risks exposed by opponents' asymmetric approaches
  - NEC concepts rely on connectivity - over-reliance on infrastructure, lack of 'reversionary' modes
  - Opponents introduce random failures e.g. via hacking
- Exploitation approach
  - Aim of opponents is to prolong conflict and increase cost e.g expend blue force time, intelligence and weapons on false targets

9. General Information Risks

- Network could reduce personal sharing and loss of required *context*
  - Network allows much greater sharing of information
  - Presently data is frequently shared during interpersonal communication
    - This ensures context is shared and gradually built up and data is more likely to be correctly interpreted and errors quickly detected
- Risks exposed
  - In networked environment - impersonal sharing may lead to loss of important context
  - Significant increased risk of data misinterpretation - especially in coalitions
    - Error detection processes reduced

Conclusions

- Network-centric approaches have the potential to provide significant advantages
- However, there are also serious potential ‘downsides’
  - Challenges from systems, technical and science perspectives
- We ignore these risks, challenges and vulnerabilities at our peril
  - We need to understand the nature and severity of these risks and the conditions under which they become activated
    - Their likelihood, impact and importance has yet to be substantially investigated
  - We need to accept that such vulnerabilities exist, develop and test approaches to eliminate them or at least reduce their impact

Future Research

- There is a need to:
  - Identify more comprehensively system-level risks and vulnerabilities
  - Understand relationship to NEC implementation decisions and feed the warnings into the appropriate decision making processes - including links with experimentation
  - Understand what preventative or mitigating measures are necessary and ensure that appropriate advice is provided to the NEC delivery process
- Previous focus on system-level
  - Need to consider more technical, component level issues
  - Determine whether these have localised or system-wide effects e.g. compromise of communications affecting trust in info source

Important Issues

- To resolve vulnerabilities and risks will require co-ordinated effort across all Lines of Development
  - e.g. password - technical solution to social engineering
- Will require a continuous “learning from experience” process
  - Understand from practice as well as analysis which are the important ones to focus on
  - Understand whether mitigating measures work effectively
  - Look out for indicators of previously unrecognised vulnerabilities
- What are the different types of asymmetry that might be employed against us?
  - Does this generate new vulnerabilities or change our view on current ones?

Questions?

Candidate Research Questions (1)

- 1. Does complexity science provide us with insights into potential vulnerabilities?
- 2. Is it possible to develop an ‘integrated’ force where components have different degrees of net-centricity?
- 3. Is it possible to exploit information superiority without reducing the effectiveness of our external communication?
- 4. How do we deal with the trend towards reduced platform numbers and the networked ideal of greater numbers?
- 5. How do we ensure that networked forces select appropriate tempo, do not get driven by own stimulus, and spend sufficient time making sense of greater input volume?
- 6. How do we ensure that our ‘information improvements’ do not simply increase stress, workload and uncertainty for command?

Candidate Research Questions (2)

- 7. What are the best approaches for protection against IO - not just against technology attacks?
- 8. How do we ensure that the network does not amplify damaging effects of poor command?
- 9. How do we ensure that greater use of automation for information sharing does not lead to damaging loss of necessary context?
- 10. What training do we provide operational and support staffs to avoid the NCW hazards?