Dan “Rags” Ragsdale
Program Manager, Information Innovation Office

Scalable Cyber Deception

DARPA Cyber Colloquium
Arlington, VA

November 7, 2011

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
07 NOV 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Scalable Cyber Deception	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Defense Advanced Research Projects Agency (DARPA),Information Innovation Office,3701 North Fairfax Drive,Arlington,VA,22203-1714	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the Colloquium on Future Directions in Cyber Security on November 7, 2011, Arlington, VA.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**7**	

Deception in Warfare

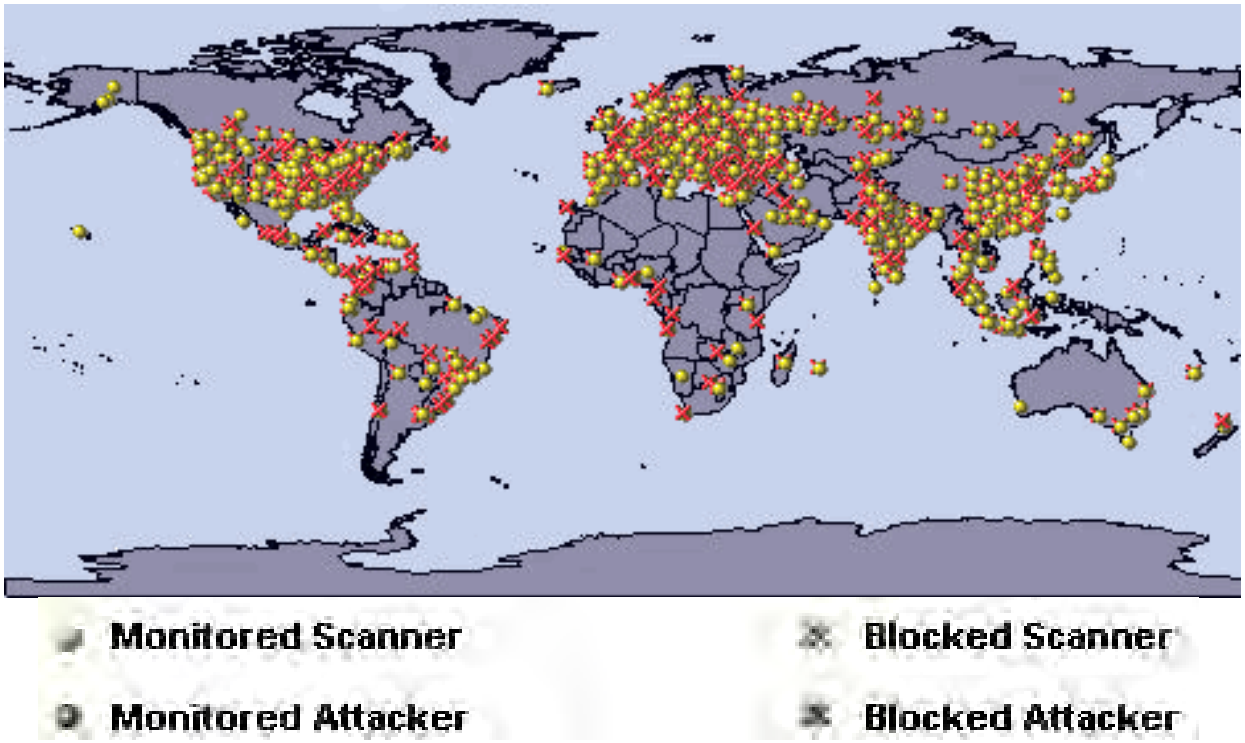
http://www.ng.mil/Images1/today/0501b.jpg

"All warfare is based on deception..." Sun Tzu

Deception: A direct counter to asymmetrical threats

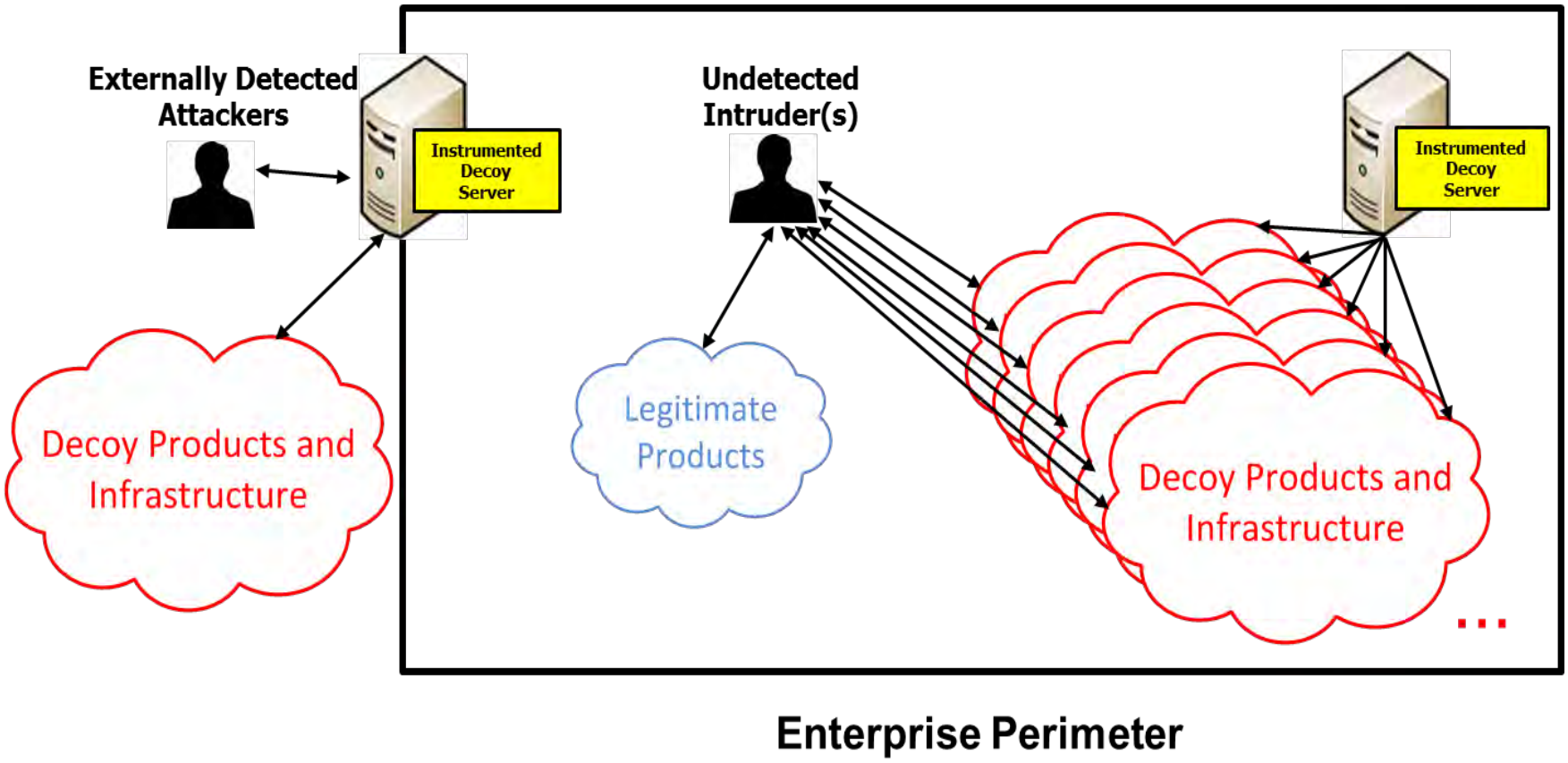
Intrusion attempts on a Government agency

- 40,000 blocked intrusion attempts/week
- World-wide attack sources



An Opportunity?

An Example Architecture for Cyber Deception



Scalable Cyber Deception Issues

Generation and Deployment of both Decoy Products and Infrastructure

- Automated
- Realistic, Credible, Enticing
- Tailorable
- Differentiable / Non-differentiable
- Noninterference

Key Technical Challenge

To significantly increase adversaries' workloads with minimal increase to our own

Promising Applicable Research Areas:

- Natural Language Processing
- Large-scale Virtualization
- Realistic Synthetic Activity Generation
- Protocol Manipulation and Exploitation
- Behavioral Science
- Others...

Please send input to:

Daniel.Ragsdale@darpa.mil