

# **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

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE <b>07 NOV 2011</b>		2. REPORT TYPE		3. DATES COVERED <b>00-00-2011 to 00-00-2011</b>	
4. TITLE AND SUBTITLE <b>Scalable Cyber Deception</b>				5a. CONTRACT NUMBER	
				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) <b>Defense Advanced Research Projects Agency (DARPA), Information Innovation Office, 3701 North Fairfax Drive, Arlington, VA, 22203-1714</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
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 <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES <b>Presented at the Colloquium on Future Directions in Cyber Security on November 7, 2011, Arlington, VA.</b>					
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			
<b>unclassified</b>	<b>unclassified</b>	<b>unclassified</b>	<b>Same as Report (SAR)</b>	<b>7</b>	



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

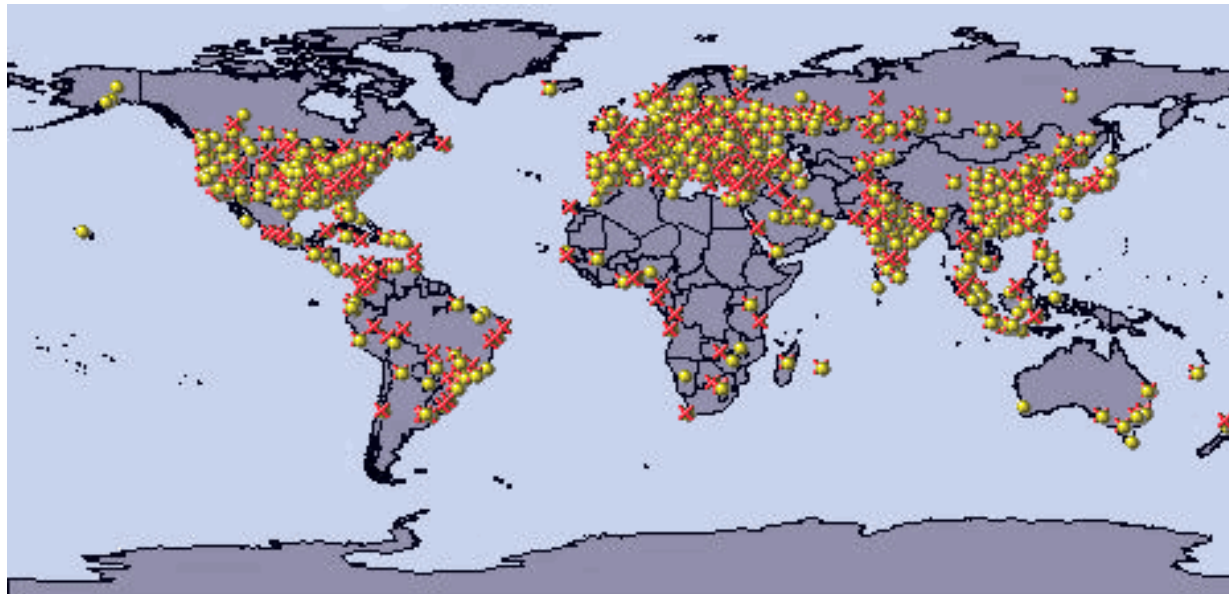
“All warfare is based on deception...” Sun Tzu

Deception: A direct counter to asymmetrical threats



## Intrusion attempts on a Government agency

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



 **Monitored Scanner**

 **Blocked Scanner**

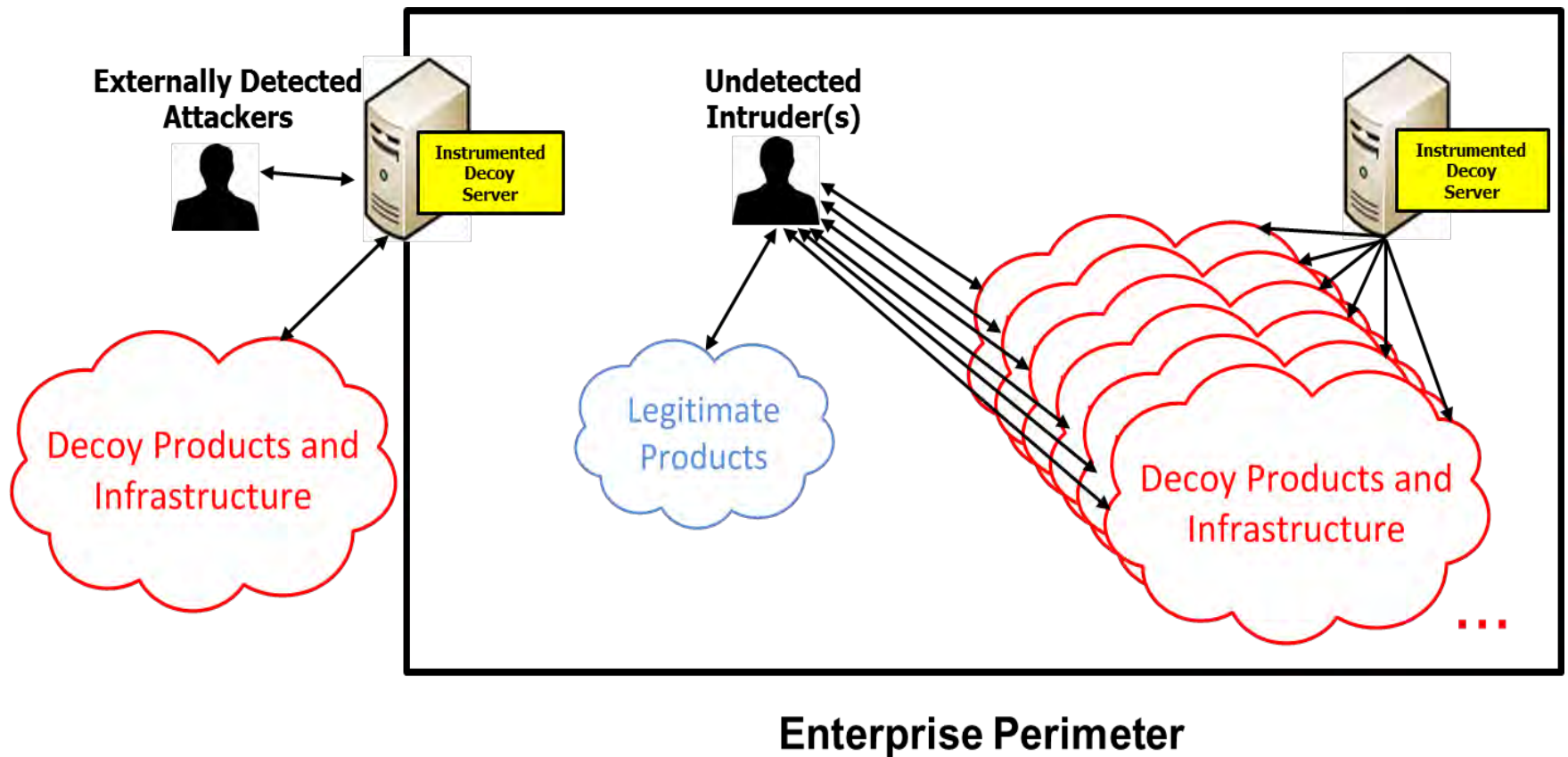
 **Monitored Attacker**

 **Blocked Attacker**

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...



# Scalable and Tailorable Cyber Deception

---

**Please send input to:**

[Daniel.Ragsdale@darpa.mil](mailto:Daniel.Ragsdale@darpa.mil)