Dan “Rags” Ragsdale
Program Manager, Information Innovation Office

Scalable Cyber Deception

DARPA Cyber Colloquium
Arlington, VA

November 7, 2011

Deception in Warfare

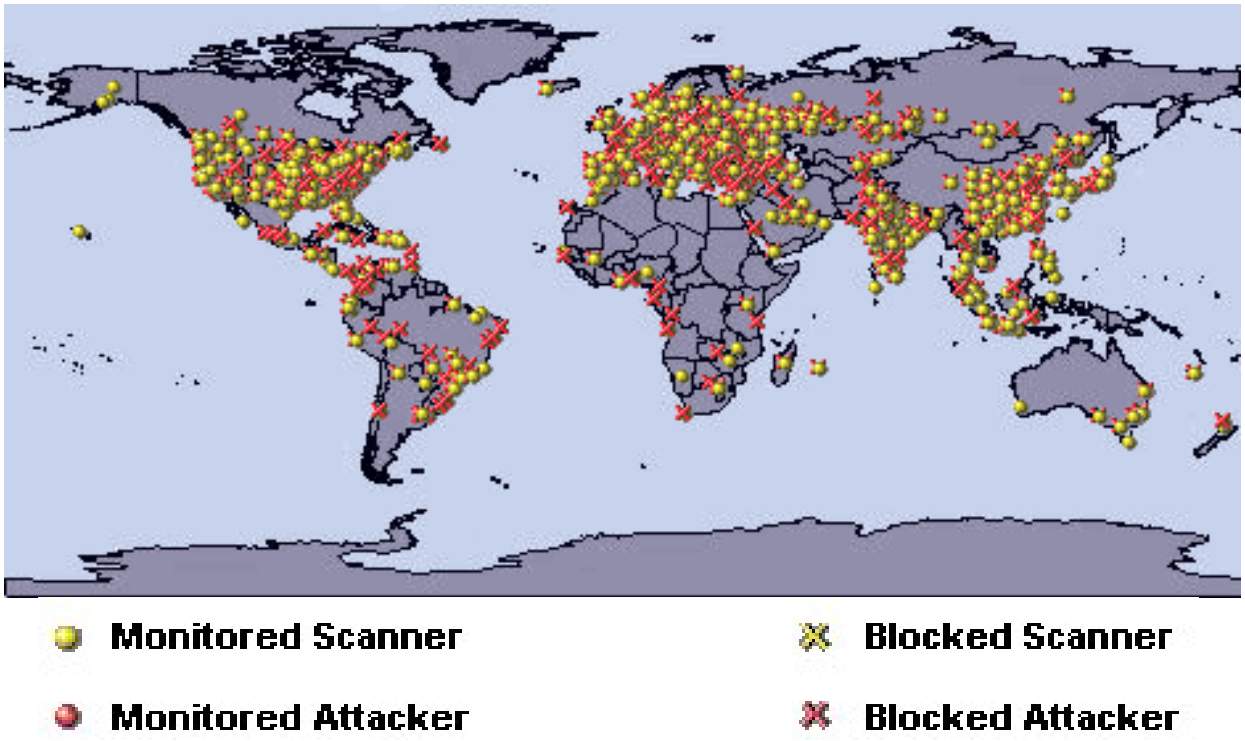
http://www.ng.mil/Images1/today/0501b.jpg

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

Deception: A direct counter to asymmetrical threats

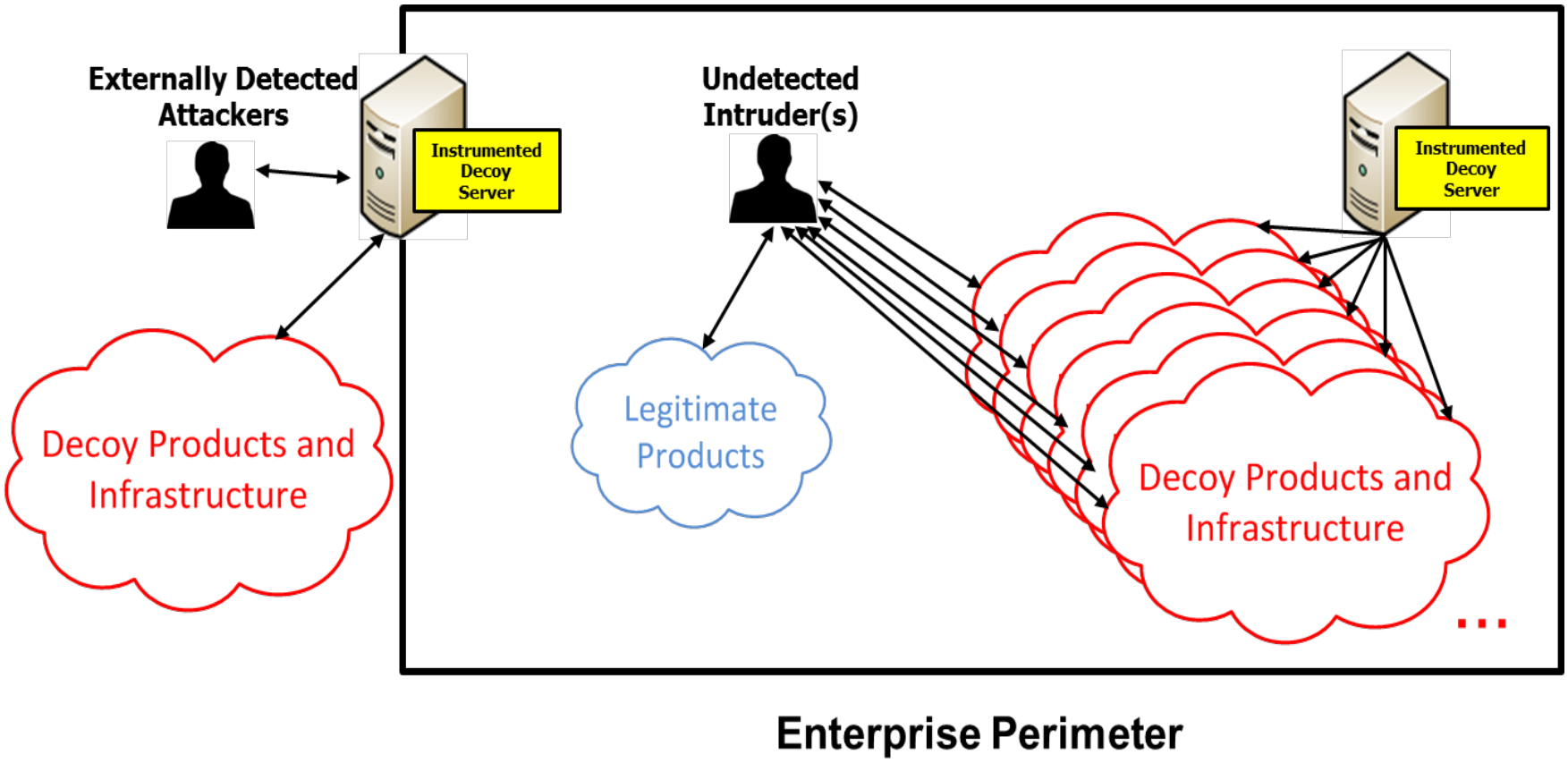
Intrusion attempts on a Government agency

- 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