

SBIR Case Study: Centripetal Networks

Subtitle: How CNI Leveraged DHS S&T SBIR Funding to Launch a Successful Cyber Security Company

Cyber Security Division
2012 Principal Investigators' Meeting
10-October-2012

Sean Moore, PhD
CTO & VP Research
Centripetal Networks, Inc. (CNI)

smoore@centripetalnetworks.com
571-252-5078

Centripetal Networks

- **Vendor of next-generation cyber security products and services. Current products include:**
 - **RuleGate™ packet filtering appliances**
 - **Network Protection System™ (NPS) management software**
 - **Powerful New NETSEC Applications**
 - **Advanced Cyber Threat™ (ACT) subscription service**
 - **Exfiltration Prevention**
 - **DoS Protection**
 - **SDK for integrating cyber threat information feeds**

CNI Timeline

- **Founded:** 2009
- **Goal:** Bring innovative cyber security technologies to market that protect US interests
- **Plan:** Self-fund proofs-of-concept & seek R&D funding for development
- **Spring 2010:** Proof-of-concept packet filter (TRL 4)
- **Summer 2010:** DHS S&T SBIR Phase 1
“Large-Scale Network Survivability, Recovery, & Reconstitution” (NS2R)

Response to a DHS **Grand Challenge Problem:** Protect US Internet infrastructure from extreme attacks (massive flooding DDoS attack)

NS2R Concept

- **Premise:** Must have mission assurance during extreme attacks → Progressively cycle through three (3) phases of network operations:
- **Survive:** Upon attack detection, enforce Internet-wide network security policies that restrict Internet packet transport to communications between highest-priority, mission-critical resources (e.g., critical government organizations and applications such as NGN GETS)
- **Reconstitute:** During a restriction phase, decontaminate by eliminating known pests, repairing compromised hosts, etc.
- **Recover:** After reconstitution, enforce a new (restriction) network security policy that allows communication between high- and medium-priority resources.
- **Repeat:** Reconstitution and Recovery phases until normal network operations are restored.
- **(Note:** This may be viewed as a civilian version of the DoD's INFOCON/CYBERCON framework for operational readiness against cyber threats)

NS2R Program

- **NS2R core enabling technologies:**
 1. Capability to enforce very large (million-rule) network security policies
 2. Capability to instantaneously switch between different, very large policies
- **SBIR Phase 1 Goal:** Develop Capability 2 “Rapid Policy Switching” without any loss-of-service or loss-of-security
- **Spring 2011:** Successful Internet-scale demonstration led to Phase II Award
- **SBIR Phase II Goals:**
 - Develop RuleGate™ and “Rapid Policy Switching” to deployed product (TRL 9)
 - Near-term: Develop tactical NETSEC Apps for ISPs, Carriers, and large Enterprises
- **Beyond:** NS2R-based “Emergency Internet Service” program analogous to current Government Emergency Telecommunications Service (GETS/NGN GETS)

Centripetal Networks Oct-2012

- **Products:** Available as of Oct-2012
 - RuleGate 2100 packet filter for enterprise and ISP edge (>1000X performance)
 - Network Protection System management software
 - Advanced Cyber Threat (ACT) subscription service (>100X protection)
 - Software Development Kit (SDK) with API for integrating cyber threat information feeds provided by partners, customers, 3rd parties

Centripetal Networks Oct-2012

- **Customers:** Multiple customer trials (DoD & Commercial) launched in Oct-2012
- **Partners:** Multiple partners using SDK to integrate cyber threat information feeds

Centripetal Networks Oct-2012

- **Cyber Security Applications:**

- Internet Attacks defense preventing DoS, malware, & hostile governments attacks
- CyberBlock™ federation for protection of university networks
- Exfiltration prevention and Advanced Persistent Threat (APT) Defense
- Cyber Enclaves
- Identity-Based IP (IBIP) networking
- NS2R and INFOCON/CYBERCON

Centripetal Networks Oct-2012

- Questions