

# *Application of DETER in Large-Scale Cyber Security Exercises*

Ron Ostrenga, Sparta Inc.

Paul Walczak, Warrior LLC

# Cyber Storm Objectives - DETER

- Provide Opportunity to Evaluate S&T DETER Investment
- Demonstrate Relevance of DETER Simulation Capability
- Transition DETER Technology
  - Test DETER Ability to Provide Meaningful Feedback to Realistic Operational Situations
  - Explore Limits Related to Interactive Integration of Current DETER Capability
  - Establish Baseline for Future Evolution of DETER Capability
    - Understand Requirements for In-Situ Course of Action Estimation Supporting Cyber Security Decision Making Processes
    - Investigate DETER Potential for Use in Cyber Security War Gaming
- Expand DETER Stakeholder Community

The DETER model represents the interconnected organizations that are participating in Cyber Storm abstracted as an enterprise network.

The topology is logically valid, but without the requisite detailed proprietary information from the participating organizations, is not accurate in depicting the actual connection schema. Much has been simplified so that the model can be presented in a single display.

## Master Scenario Event List (MSEL) – Primary DETER Events

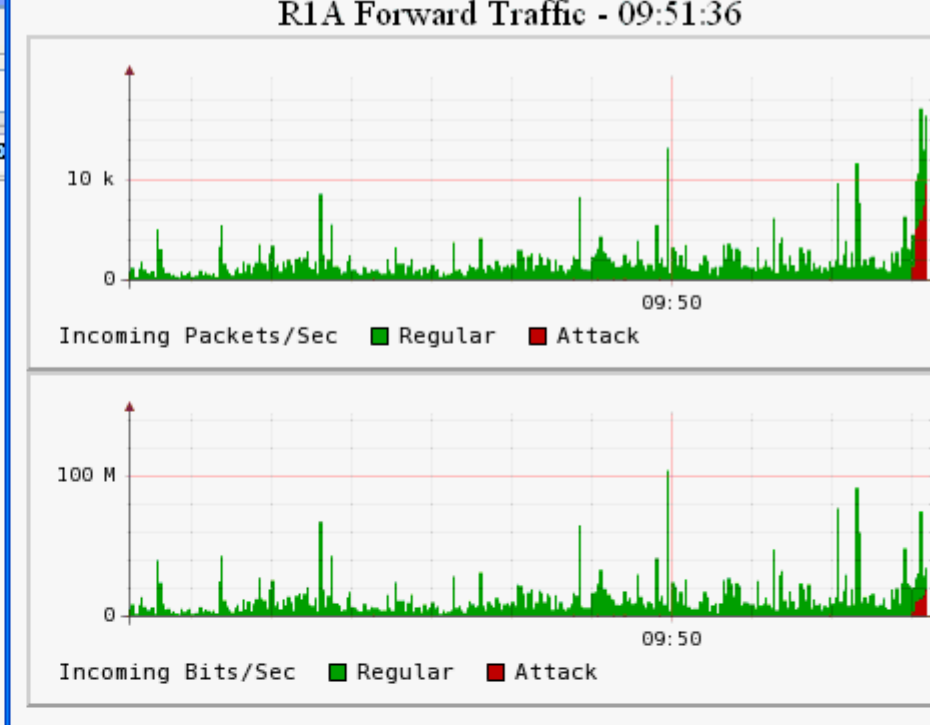
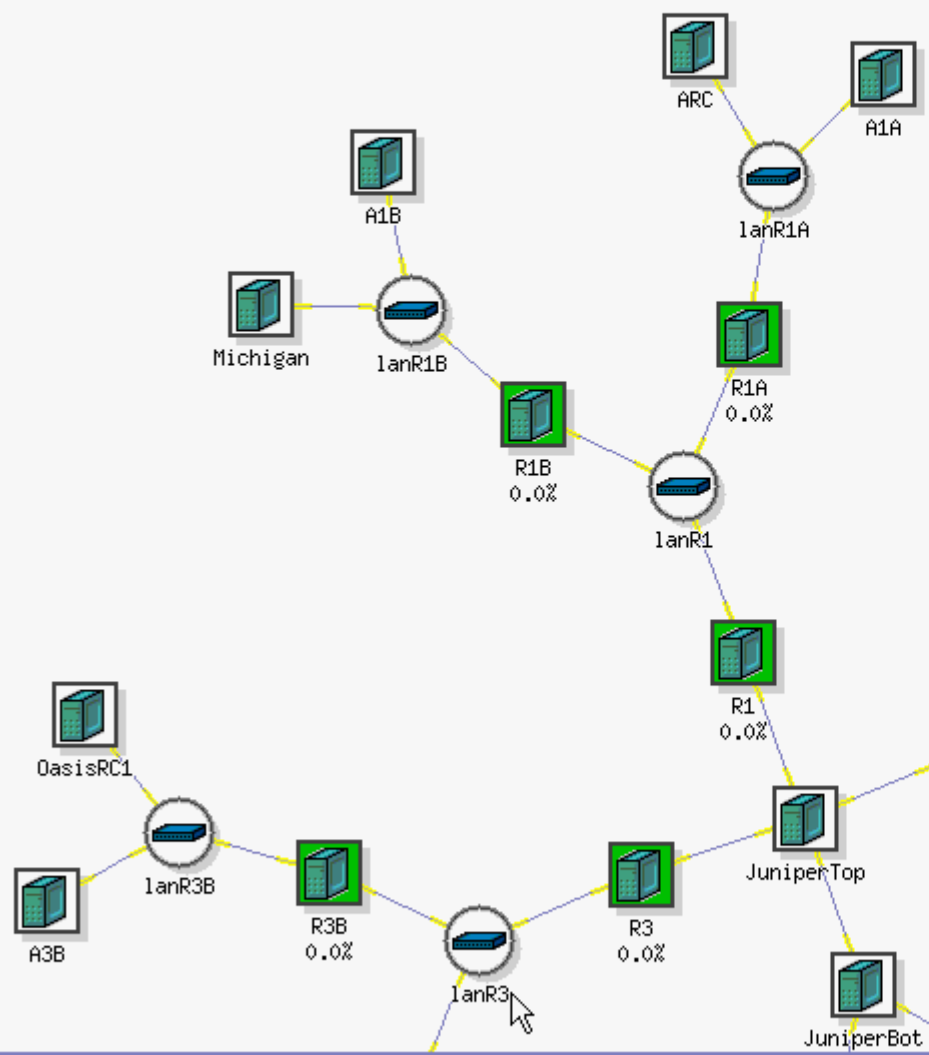
- Red Cross event 4081, 7 Feb (extortion)
  - psychological impact
  - collateral effects
- OASIS (RC2) event 2014, 7 Feb
  - collateral effects
- MI 5203, NY 5313 series, 8 Feb (extortion)
  - collateral effects
  - denial of e-gov services
  - psychological impact, loss of control

# DETER Support to Cyber Storm After Action Review Process

The exercise control summary included DETER output. We produced three animated presentations of DETER output from the primary event threads in which DETER participated. These highlighted the collateral damage associated with a large scale distributed attack, points that supported the exercise's overarching objectives for interconnected consequences / cascading effects. This was the only glimpse into technical realism that was collectively applied to the exercise process, albeit occurring at its culmination. However, this seemed to be an effective use of DETER.

## Red Cross event 4081, 7 Feb (extortion)

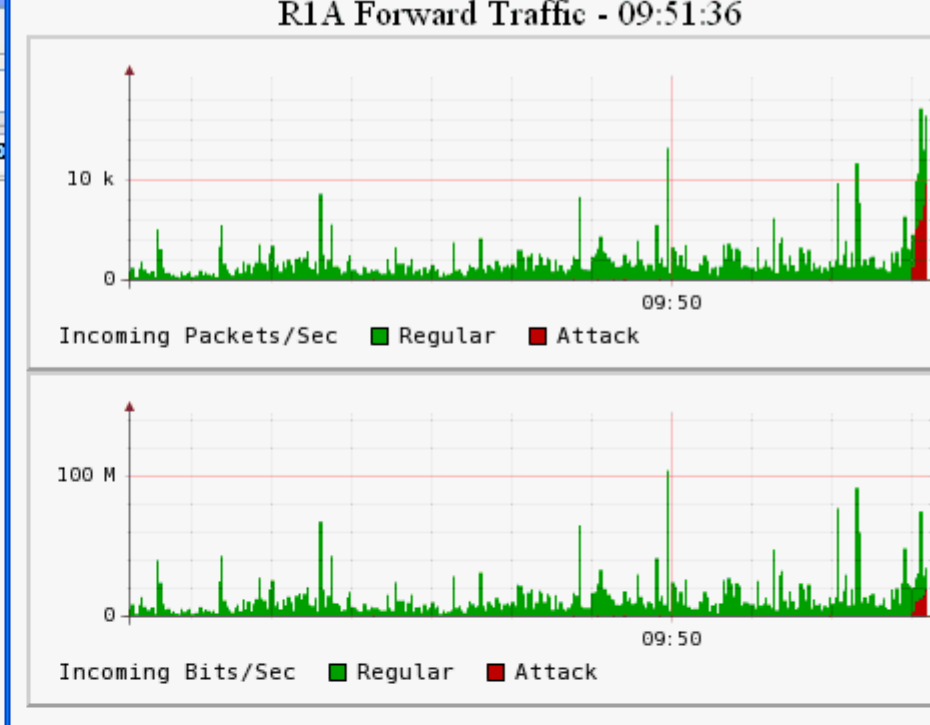
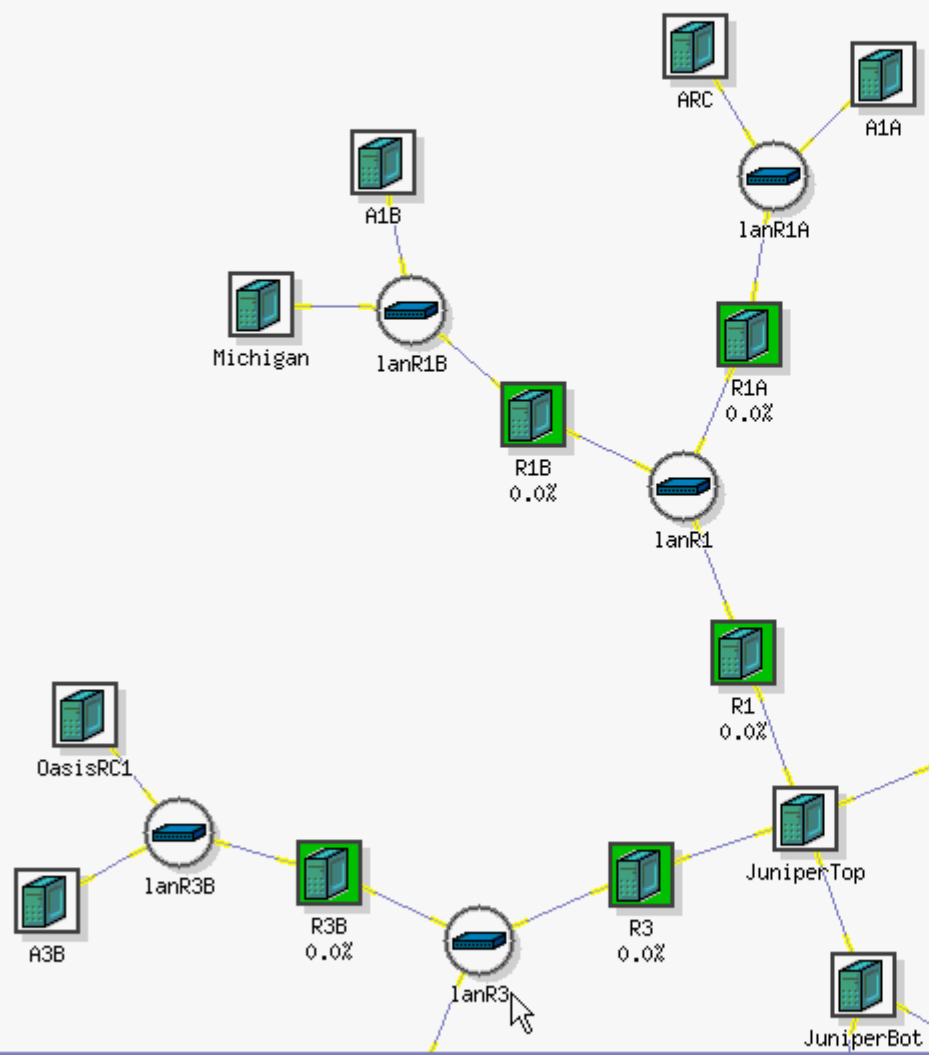
Major Blood Bank (MBB) receives extortion threats that may potentially lead to disruption of services. In order to gauge the degree of loss feasible from the extortion attempt, Red Cross requests that DETER models Red Cross topology to determine the likely impact from anticipated attack classes that may be initiated by the extorting perpetrators.



## **OASIS (RC2) event 2014, 7 Feb**

The OASIS websites for RC2 begins to suffer a denial of service attacks. Since these are the systems that ordinarily provide the data on transmission service availability and on energy prices, shutting these systems down makes it difficult for electric power companies to trade electricity between regions. This threatens to reduce temporarily the flexibility and profitability of the electric power companies affected.

Phone Call: "I notice that your OASIS site is down. Do you know the cause for this? What is the expected return time?"



# MSEL Event 5313 Thread - NY State Extortion

**5313 /-08** 08-0815 EST Feb 2006  
DDoS as part of extortion attempt

The network is still running slow. Many complaints from users. I talked to the folks in the NOC and they said that last night the logs show that the border routers returned to their normal levels at 9 PM. But at 6 AM incoming activity increased and is now at 50 percent capacity.

**5313-01 /09** 08-0825 EST Feb 2006  
Border Routers are now at normal capacity.

**5313-02 / -10** 08-0910 EST Feb 2006  
Border Routers are now saturated to full capacity.

**5313-03 / -11** 08-0925 EST Feb 2006  
Border Routers incoming traffic have returned to normal levels.

**5313-04** 08-1010 EST Feb 2006  
All morning we've been getting complaints for network users that the "Internet is 'down'" and that they can't get any e-mail from outside the State Network. Complaints are almost constant.

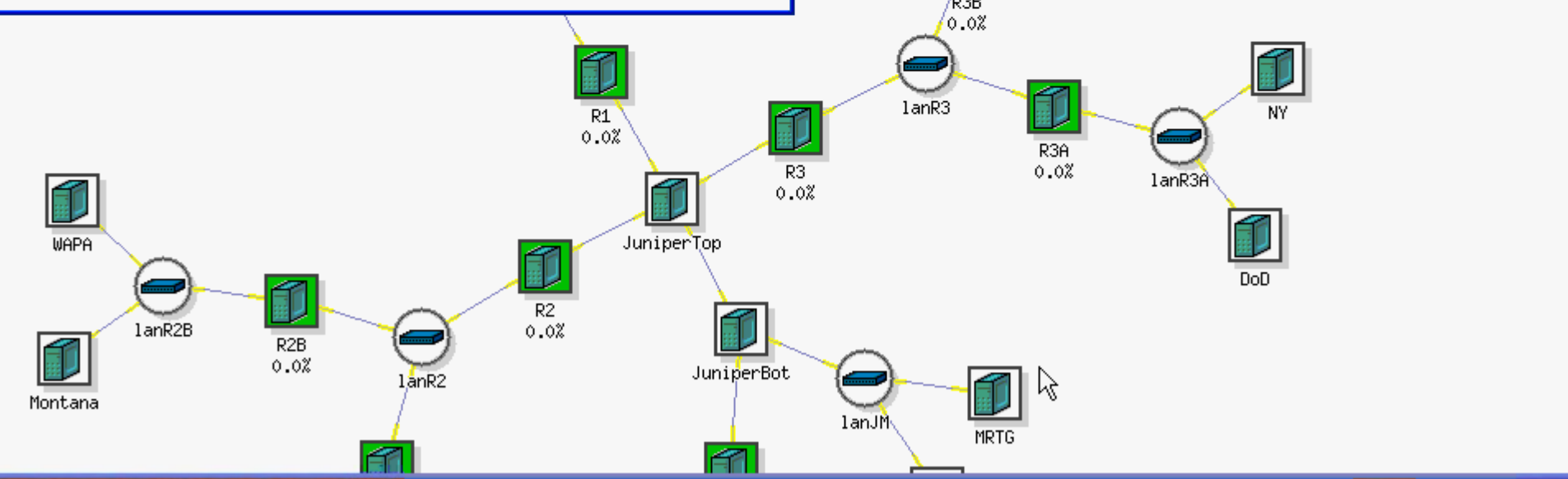
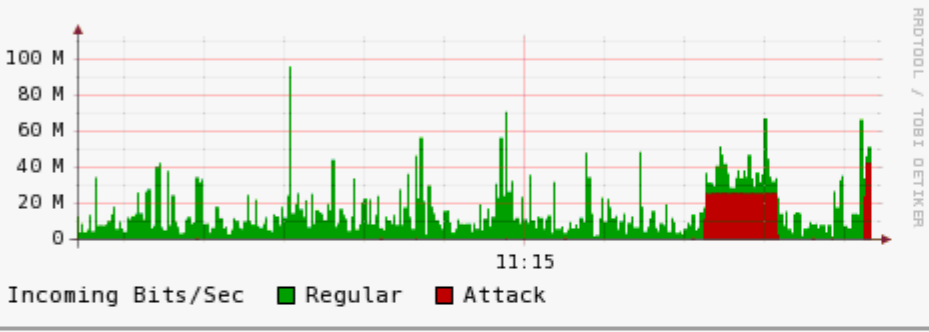
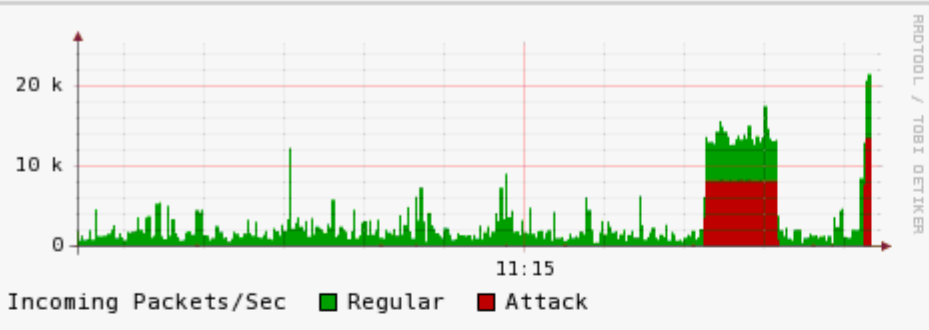
**5313-05 / 13 /14** 08-1055 EST Feb 2006  
Greetings. I am the author of the code that has DDoS'd you for the past two days. I designed it so that I can control it at will and turn off or turn on access to your external network ... All this can stop for one easy payment of \$9999.99 made by 2PM to account 1234 of the Darkhat Virtual Credit Union. Make the payment or else!!

**5313-06 /15** 08-1105 EST Feb 2006  
Border routers now at 95 percent saturation

**5313-07/16** 08-1110  
Border routers incoming throughput has returned to normal levels.



# R3A Forward Traffic - 11:17:10



## Cyber Storm Exercise Report - Remarks Submitted to NCSD

8.3 Cyber Storm demonstrated potential uses for DHS S&T & NSF sponsored DETER testbed in the operational and exercise arenas. DETER features were used to model MSEL event threads in support of Cyber Storm scenario and to facilitate the exercise after action review process. The success of experience suggests that integration of relevant technology testbeds and experimentation within the framework of future cyber security exercises should be encouraged.

# Lessons Learned from DETER Participation in Cyber Storm

- **Need more application layer modeling capability**
- **Improve fidelity of instrumentation**
- **Add additional routers, routing protocols**
- **Community interests in modeling root DNS**
- **Need ability to model security counter measures (i.e., firewalls, IDS...)**
- **Evolve feature usability for in-situ course of action analysis capability**