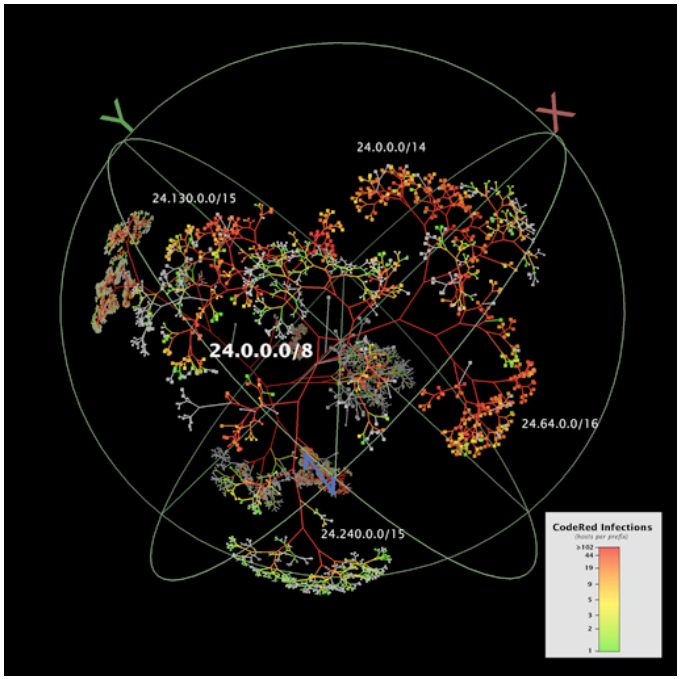
Macroscopic Internet Data Collection and Analysis



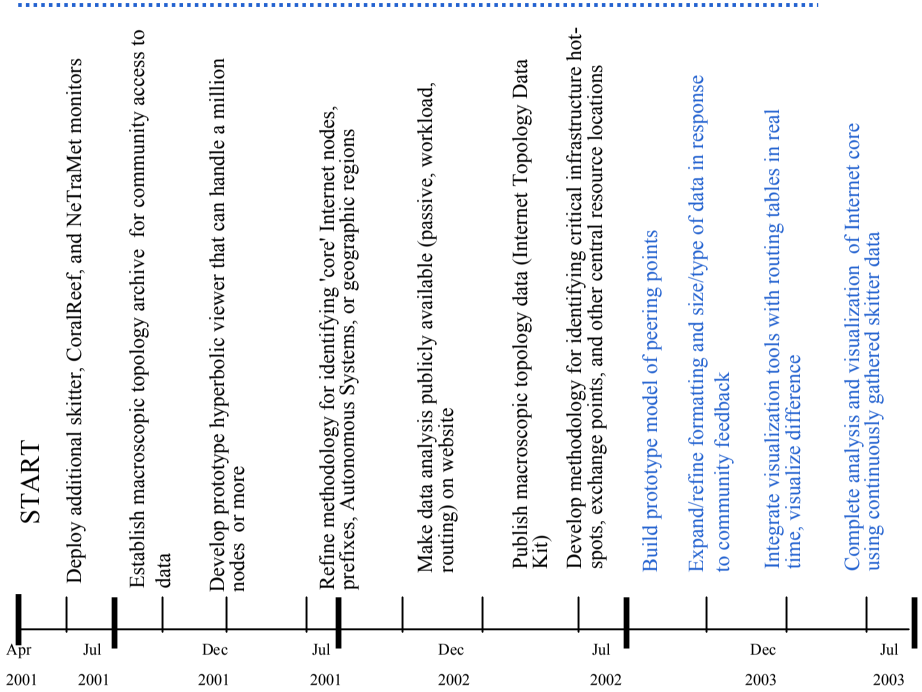
Visualization of hosts infected by CodeRed worm on July 19, 2001.

Impact

- Ability to track and visualize the spread of Internet worms, viruses, and other denial of service (DoS) attacks.
- Uniquely positioned to provide DARPA and the research community with highly relevant real-world Internet data sets, including active topology measurements from 21 sources to over a million destinations, and passive trace data for evolving workload characterization of an OC48 link at a major exchange point.
- Customized CoralReef passive monitoring tools for use by DoD for both operational and military/battlefield simulation use..
- Collection of path specific global measurement data useful in analyses relevant to the commercial Internet as well as to operations of a DOD network. For example:
  - Comparisons between articulated routing policies and actual traffic flow
  - Calculus for analysis of IP-level topology & inter-domain (BGP) routing
  - Methodology for identifying critical infrastructure hot-spots, exchange points, and other topologically 'central' locations.

New Ideas

- Use of walrus hyperbolic 3D visualization tool to show traffic anomalies such as high delays or the spread of the CodeRed worm through Internet routing infrastructure
- Developed methodology for ranking the relative importance for Autonomous Systems (AS) seen on a topology sample
- Internet routing geopolitical analysis and visualization
- Analysis results refute commonly held assumptions about Internet domain growth and routing dynamics
- Use of NeTraMet passive monitors from several sites to track DNS root and gtld nameserver performance on a daily basis



Cooperative Association for Internet Data Analysis / UCSD - Dr. K Claffy, PI