

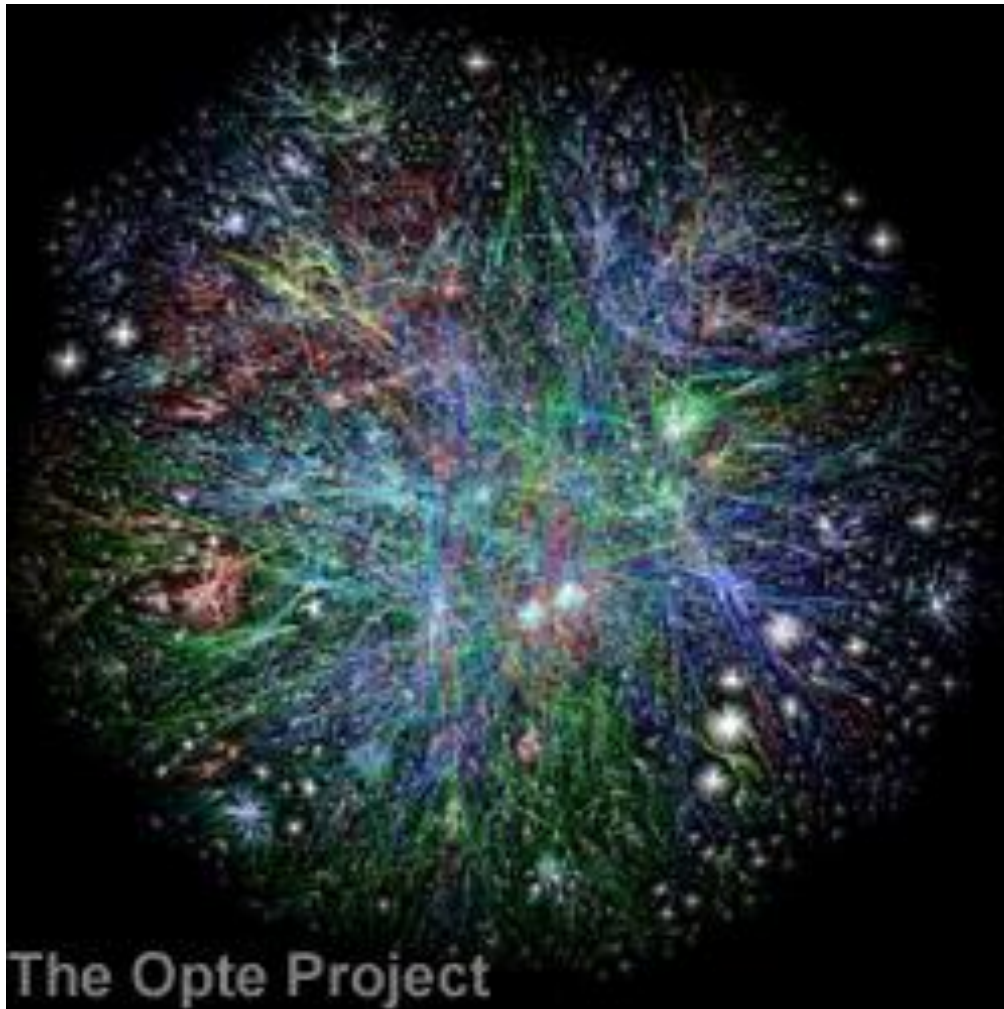
# ***Understanding and Representing the Cyber Threat***

**Dr Jeff McNeil  
Scientific Research Corporation  
jmcneil@scires.com**

***NOT FOR PUBLIC RELEASE***

**ITEA Cyber Conference  
28 November 2012**

# The Environment



Nov 24, 2003 Map of the Internet by the OPTe project ([www.opte.org](http://www.opte.org)):

Graph Colors:

Asia Pacific - Red

Europe/Middle East/Central

Asia/Africa - Green

North America - Blue

Latin American and Caribbean  
- Yellow

RFC1918 IP Addresses - Cyan

Unknown - White

# Shaping the Future Environment

“The most significant deterrence challenge posed by the threat of cyberspace attack is the perceived difficulty of attributing such attacks to a specific attacker, be it a state or non-state actor.”

-General Kevin Chilton, CDRUSSTRATCOM (2009)

- Lack of technical detection capability moves the problem into the legal realm
- Lack of domestic and international cyberspace legislation makes the problem one of international cooperation

*Need an International Approach to Curb Aggression in Cyberspace*

# The Threat

Welcome to HoneyMap. This is an ALPHA version! Bug reports welcome :-)  
Note that this are not all honeypots of the HoneyNet Project,  
only those who voluntarily publish their captures to hpfeeds!

```
11:47:14 dionaea.capture - New attack from Moscow, Russia (55.75,37.62) to Aachen, Germany (50.77,6.11) [md5: 893937e0ed567cb925ba4ed33f434]
11:47:15 dionaea.capture - New attack from Bucharest, Romania (44.43,26.10) to Zagreb, Croatia (45.80,16.00) [md5: fead84c5df2e585749a8da2]
11:47:15 dionaea.capture - New attack from Itaboraí, Brazil (-22.75,-42.07) to Aachen, Germany (50.77,6.11) [md5: f0d984704a2f2633c44886c9]
11:47:15 dionaea.capture - New attack from Laurinburg, USA (34.72,-79.46) to Aachen, Germany (50.77,6.11) [md5: 0ba4d8ca33f4d121c6e2e4]
11:47:15 dionaea.capture - New attack from Kaluga, Russia (54.53,36.28) to Aachen, Germany (50.77,6.11) [md5: fead84c5df2e585749a8da2ce593c]
11:47:15 dionaea.capture - New attack from Taipei, Taiwan (25.04,121.53) [md5: 2dfbfeaa1e3959b767d9da13f2a198eb]
11:47:15 dionaea.capture - New attack from Ljesica, Bosnia and Herzegovina (43.38,17.59) to Aachen, Germany (50.77,6.11) [md5: c9742668]
11:47:16 dionaea.capture - New attack from Hungary (47.00,20.00) to Aachen, Germany (50.77,6.11) [md5: 1ac18c404a9504722812b69b46d96498]
11:47:16 dionaea.capture - New attack from Nanchang, China (28.55,115.93) to Aachen, Germany (50.77,6.11) [md5: fdc2ccdcf4b77e1868d3c9c26d]
```

**Honeynet Project**

**IT SECURITY RESEARCH GROUP**

Mann-galleys-Orion-....pdf | JTC study.pdf | James Mackenzie Fallo....pdf | K1 Package Return for....pdf | 2012 Book Award Con....pdf | 0214bc9970e6378f0....PDF | Show All

<http://map.honeynet.org/>

# Cyber Threat Challenges and Opportunities for the International T&E Community

- ▶ Threat Definition
- ▶ Threat Validation and Accreditation
- ▶ Threat Resource Support to Program Reviews
- ▶ Threat Resource Management

*Improve “Cyber Trust” among partners in dynamic coalition network environments, and further help to assess and mitigate cyber threats to operational joint networks.*