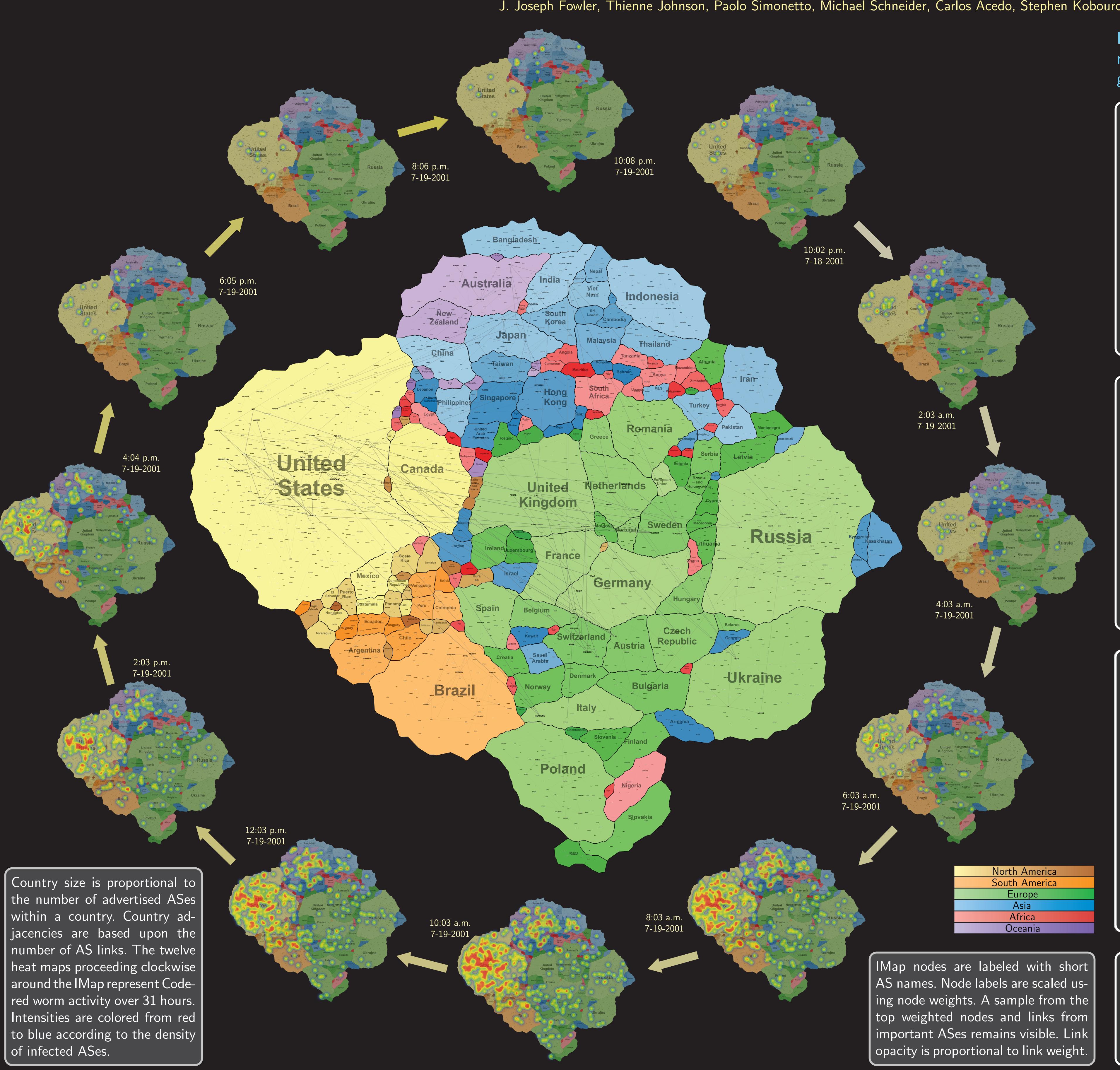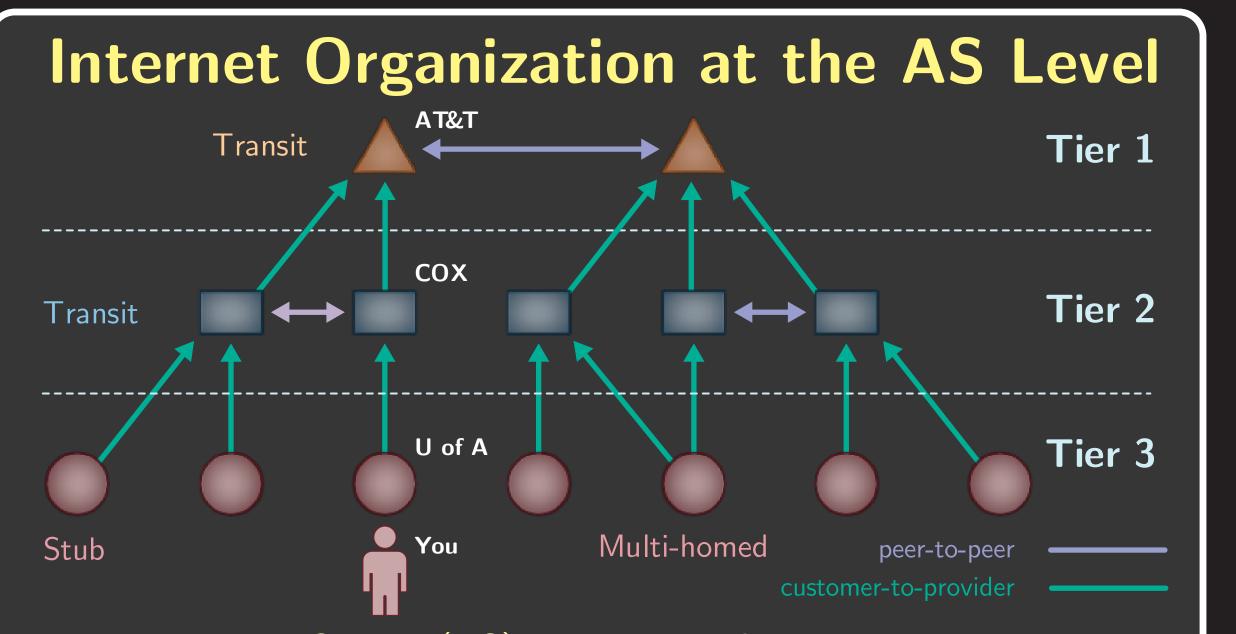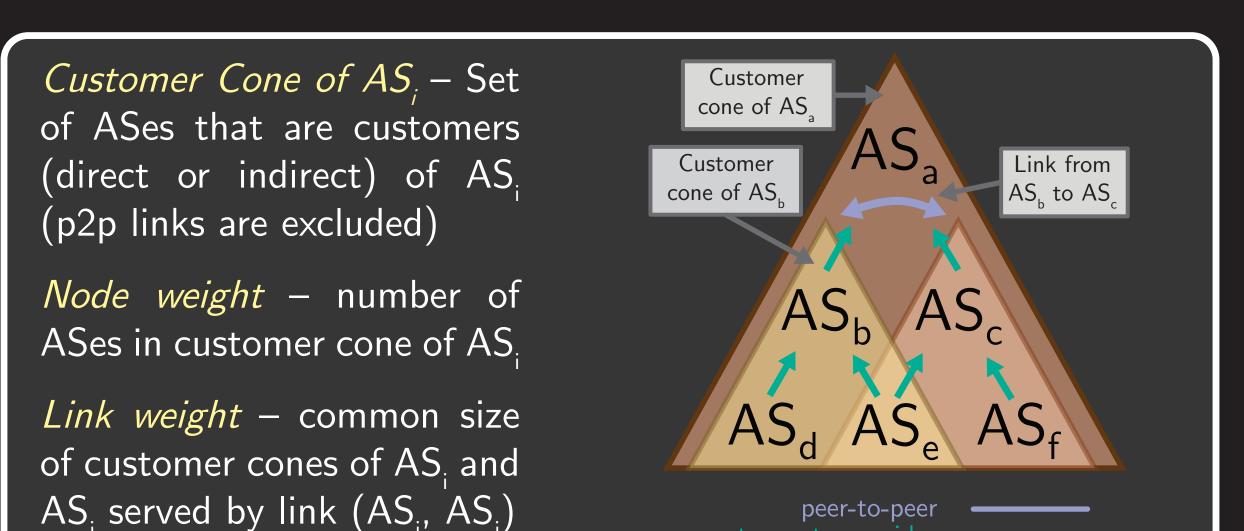# IMap: Visualizing Network Activity over Internet Maps

J. Joseph Fowler, Thienne Johnson, Paolo Simonetto, Michael Schneider, Carlos Acedo, Stephen Kobourov, Loukas Lazos - University of Arizona

IMap represents the Internet topology as a geographic-like map of the world. Large volumes of dynamic network data are overlaid in the form of heat maps to facilitate the detection of security threats. Aggregated IP traffic is mapped to geographic points based on the traffic origin.
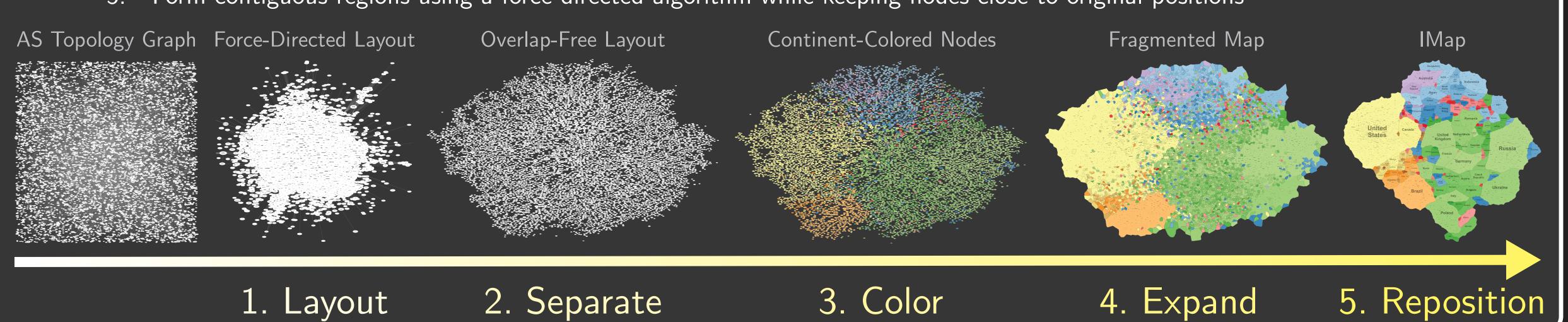

8:06 p.m. 7-19-2001

10:08 p.m. 7-19-2001

10:02 p.m. 7-18-2001

6:05 p.m. 7-19-2001

2:03 a.m. 7-19-2001

4:04 p.m. 7-19-2001

4:03 a.m. 7-19-2001

2:03 p.m. 7-19-2001

6:03 a.m. 7-19-2001

12:03 p.m. 7-19-2001

10:03 a.m. 7-19-2001

8:03 a.m. 7-19-2001

Country size is proportional to the number of advertised ASes within a country. Country adjacencies are based upon the number of AS links. The twelve heat maps proceeding clockwise around the IMap represent Code-red worm activity over 31 hours. Intensities are colored from red to blue according to the density of infected ASes.

Legend: North America, South America, Europe, Asia, Africa, Oceania

Internet Organization at the AS Level

Transit — AT&T — Tier 1

Transit — COX — Tier 2

U of A — Tier 3

Stub — You — Multi-homed

peer-to-peer
customer-to-provider

An *Autonomous System* (AS) is a group of computer networks, typically under the same administrative authority, using the same routing policy. Business relationships at the AS level govern the flow of network traffic across the Internet. The Internet topology can be abstracted to a hierarchical and directed AS topology graph.

Customer Cone of AS – Set of ASes that are customers (direct or indirect) of AS_i (p2p links are excluded)

Node weight – number of ASes in customer cone of AS_i

Link weight – common size of customer cones of AS_i and AS_j served by link (AS_i, AS_j)

Customer cone of AS_a
Customer cone of AS_b
Link from AS_i to AS
AS_a
AS_b AS_c
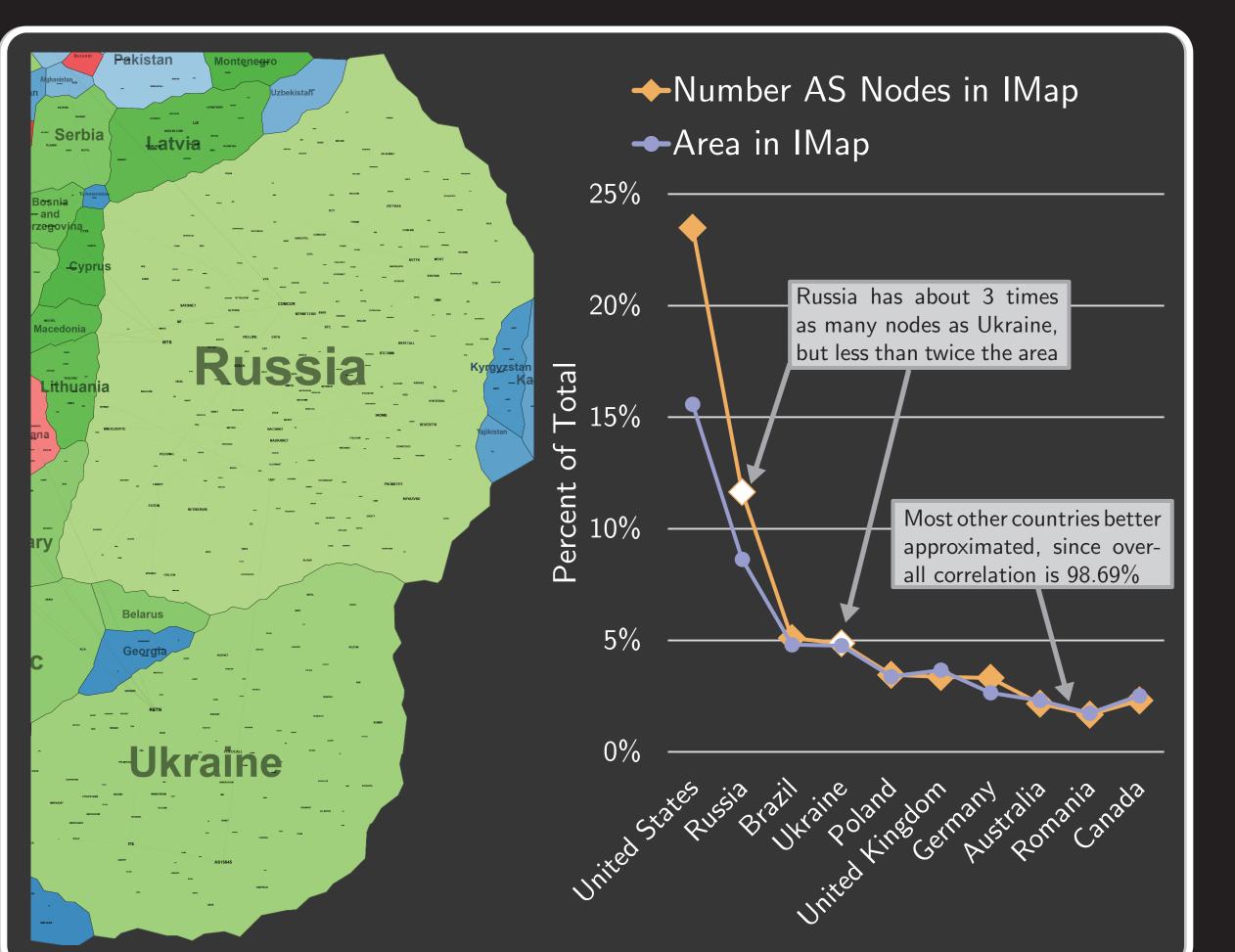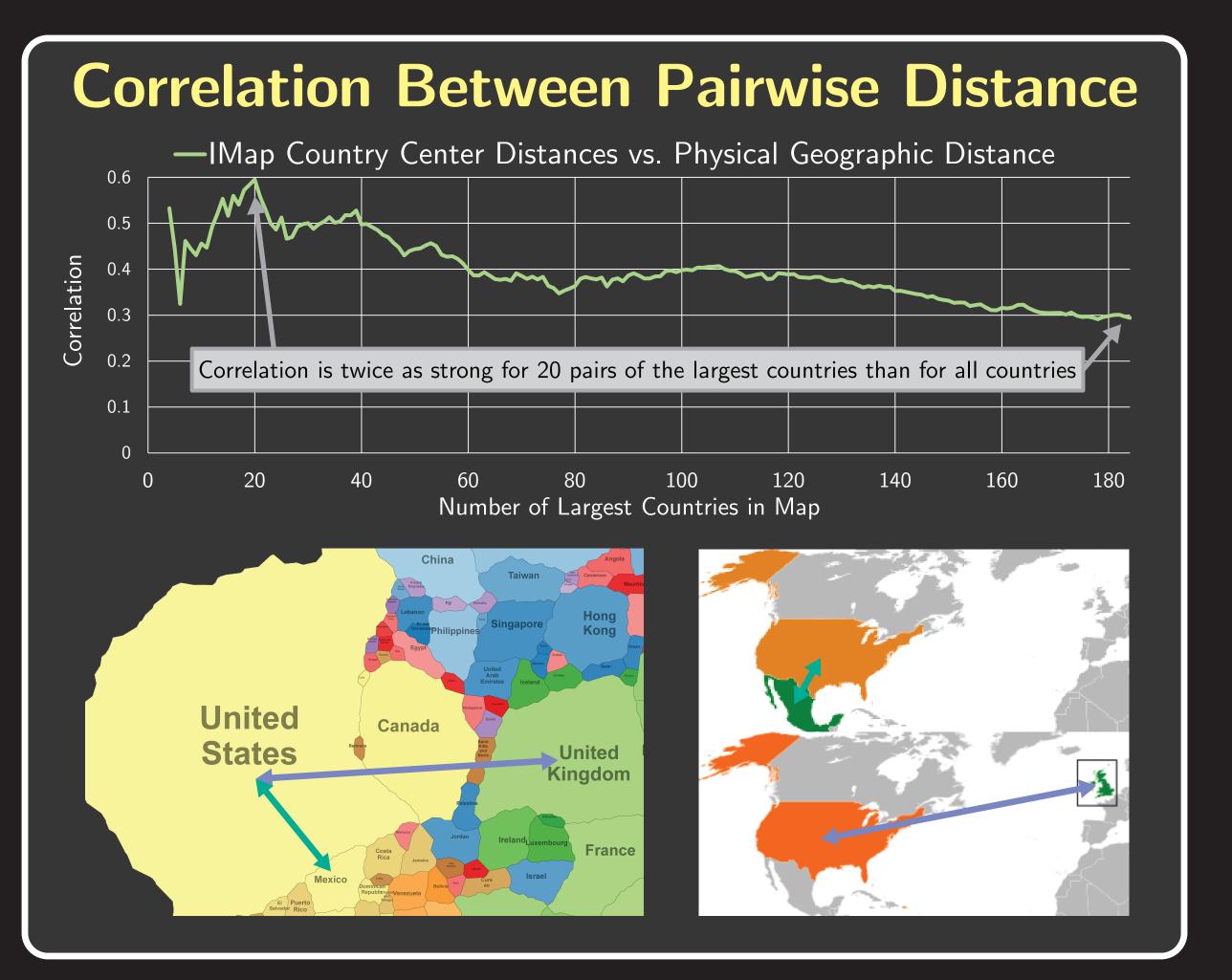AS_d AS_e AS_f

peer-to-peer
customer-to-provider

Number of registered ASes (2014): 67,494
Number of ASes used to create IMap: 45,220
Number of stub ASes aggregated to transit ASes: 35,059
Number of aggregated transit ASes: 10,161
Number of transit AS-to-transit AS links: 177,510

Five-step process for generating an IMap from the AS topology graph:

1. Apply force-directed layout, which models physical forces, to create meaningful node positioning based on link weights
2. Separate and spread out nodes keeping relative proximities to eliminate node overlap
3. Color nodes by continent while shading countries from the largest to the smallest in terms of the number of nodes
4. Expand nodes to fill in gaps in order to create a geographic-like map with a surrounding ocean
5. Form contiguous regions using a force-directed algorithm while keeping nodes close to original positions

AS Topology Graph — Force-Directed Layout — Overlap-Free Layout — Continent-Colored Nodes — Fragmented Map — IMap

1. Layout   2. Separate   3. Color   4. Expand   5. Reposition

IMap nodes are labeled with short AS names. Node labels are scaled using node weights. A sample from the top weighted nodes and links from important ASes remains visible. Link opacity is proportional to link weight.

Russia
Ukraine

Number AS Nodes in IMap
Area in IMap

Russia has about 3 times as many nodes as Ukraine, but less than twice the area

Most other countries better approximated, since overall correlation is 98.69%

Percent of Total

United States, Russia, Brazil, Ukraine, Poland, United Kingdom, Germany, Australia, Romania, Canada

Correlation Between Pairwise Distance

IMap Country Center Distances vs. Physical Geographic Distance

Correlation

Number of Largest Countries in Map

Correlation is twice as strong for 20 pairs of the largest countries than for all countries

United States   Canada   United Kingdom   France

Number of Affected ASes

On July 19th, 2001, a variant of the Code-Red worm appeared and spread very rapidly around the world. Each hotspot represents an AS that contained a computer host infected by the worm. The worm reached many ASes within a very short time of its existence. Data was obtained from CAIDA[1].

[1] http://www.caida.org/data/passive/codered_worms_dataset.xml

Propagation Hour