Key Findings of the 2015 Ashburn, VA Data Center Resilience Project

Michael Thompson
Cyber Security Analyst
Argonne National Laboratory
thompsonm@anl.gov

Regional Resiliency Assessment Program

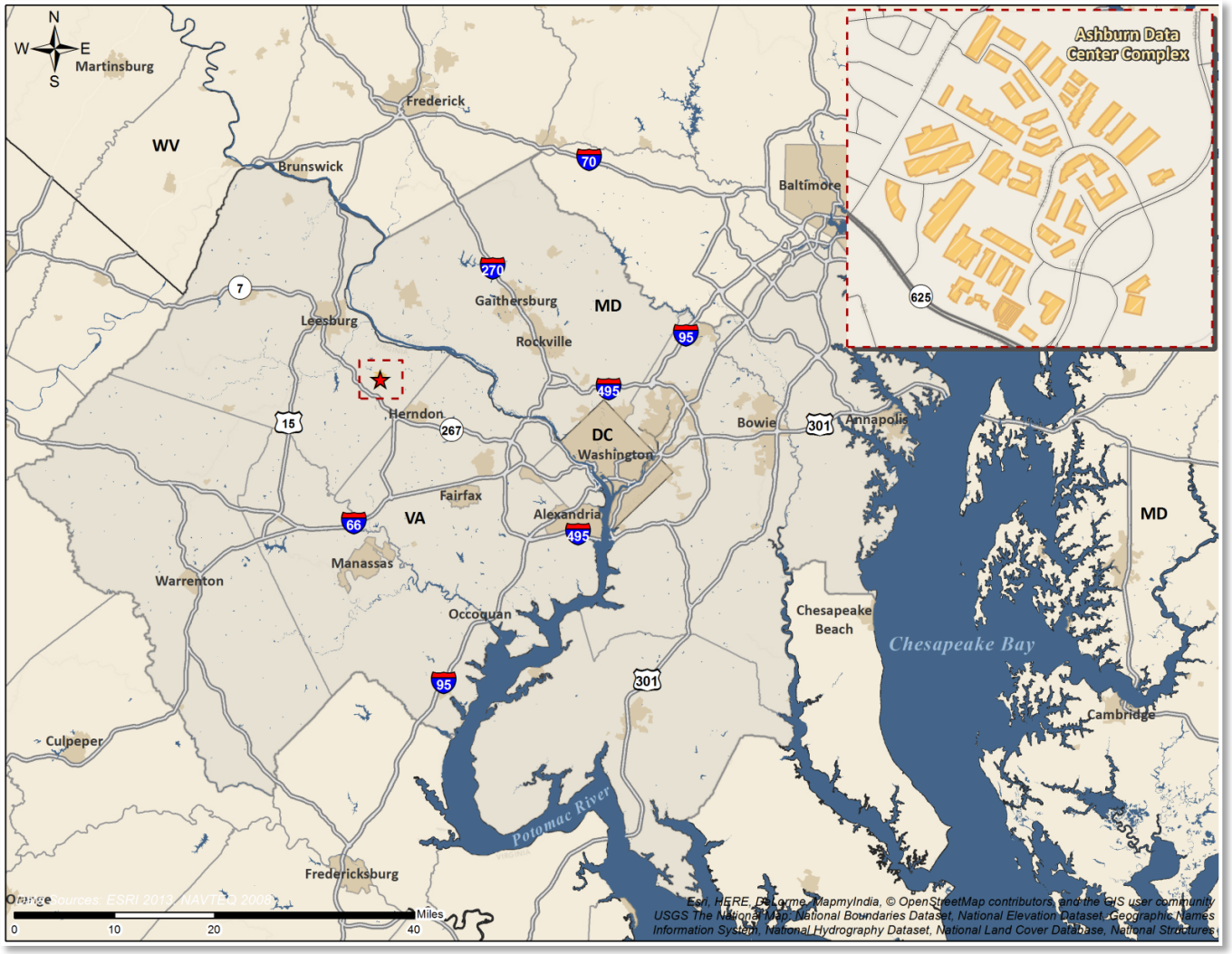
Argonne is supporting the U.S. Department of Homeland Security's Regional Resiliency Assessment Program (RRAP) in exploring the resilience of the Ashburn Data Center Cluster

In looking at a problem of this scope, we found two central questions that bear a closer examination for Internet resilience:

- Assess the resilience and vulnerabilities of the lifeline infrastructure supporting data center operations and their collective interdependencies
- Assess the collective preparedness and protection capabilities of Ashburn Data Centers and Internet Infrastructure.

For more information on the Regional Resiliency Assessment Program contact: resilience@dhs.gov or on the Ashburn RRAP: kelly.wilson@hq.dhs.gov

Ashburn Study Footprint



Courtesy of Argonne National Laboratory

Ashburn, VA, Data Center Cluster RRAP

Why Ashburn?

Beyond Ashburn's history as an interconnection point, there remain several factors that spur its current and continued growth:

- Abundant low cost energy
- Abundant water
- Abundant land
- Favorable tax incentives
- Proximity to Washington, D.C. and Transatlantic Fiber

Ashburn / Washington Fiber (*Source: Zayo.com*)

References:
- Chen, I.-W., et al., 2016, "Geographically Speaking: Geo-location Analysis Based on Traces from AIX," Center for Applied Internet Data Analysis, accessed June 7, 2016
- Interview with Buddy Rizer, 2015

Ashburn, VA, Data Center Cluster RRAP Findings

- The properties that make this infrastructure resilient also make it difficult to gather data and conduct data-driven analysis of potential failures.

- It is in part owing to this difficulty in data collection that the Ashburn, VA RRAP project's Key Findings focus on improving communication and information sharing.

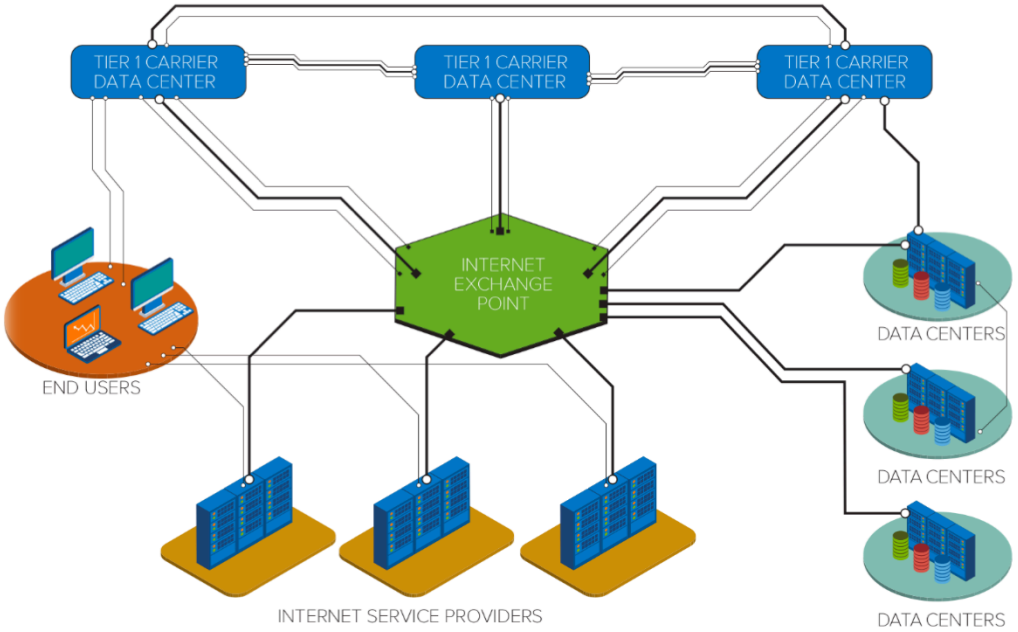
- The Ashburn, VA RRAP project identified vulnerabilities that may affect the Internet community's ability to prepare for and recover from the impacts of a variety of natural and manmade threats to its infrastructure assets.

References:

- Facilitated Discussion, March 24, 2015
- Argonne EP Fast Analysis, 2015
- Interviews with Private Sector Stakeholders, 2015
- Infragard Data Center EMP Workshop, May 28, 2015

Internet resilience is contingent on a limited number of centralized Internet exchange points (IXPs).

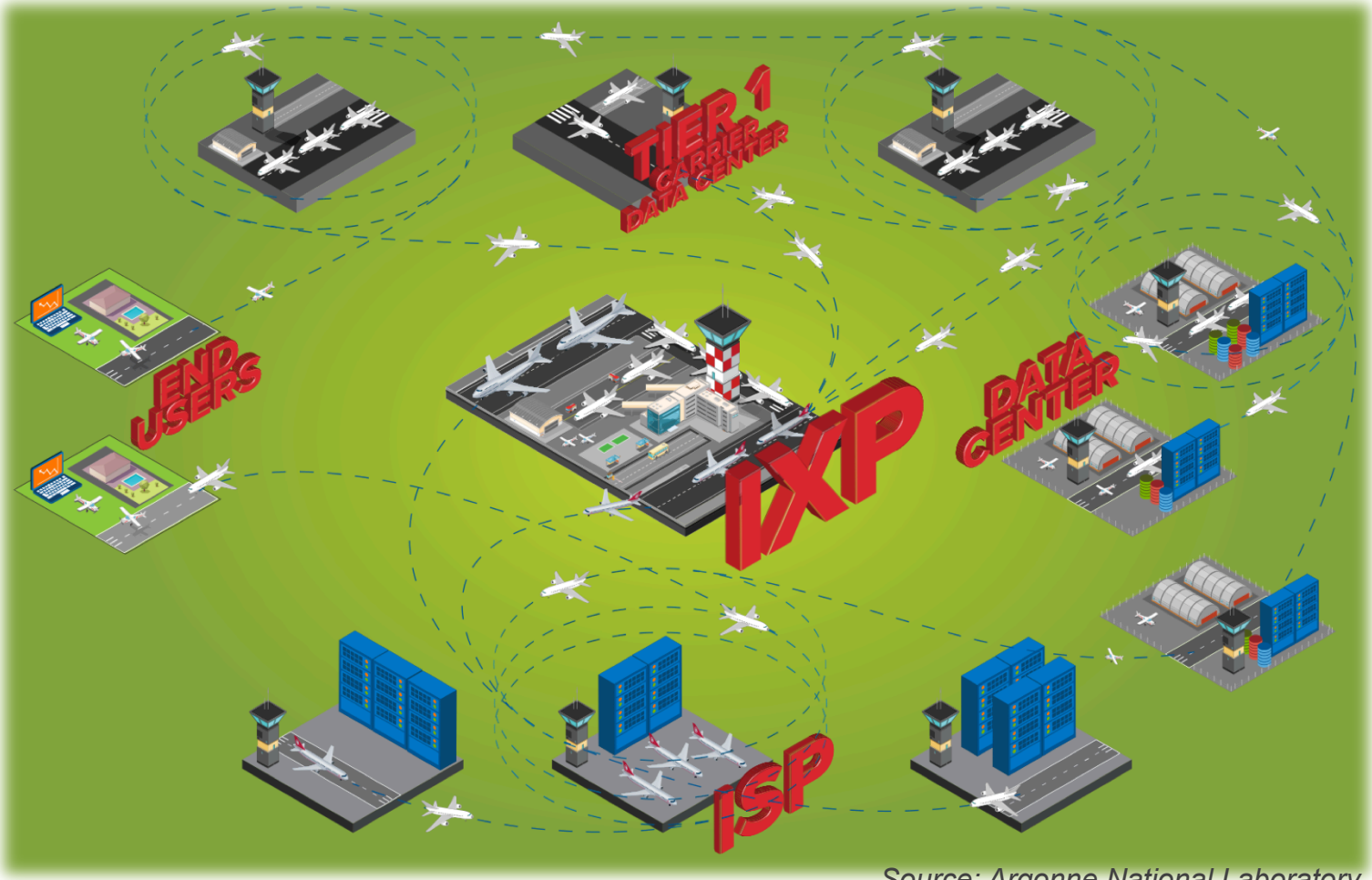
- A study should be conducted that simulates the outage of an IXP. Such a simulation would include modeling the traffic and Transmission Control Protocol congestion during an outage of IXP facilities in the greater Ashburn area.



Source: Argonne National Laboratory

References:
•Facilitated Discussion, March 24, 2015.
•Di Bartolomeo, M., G. Di Battista, R. di Lallo, and C. Squarcella, 2015, "Is It Really Worth to Peer at IXPs? A Comparative Study," *2015 IEEE Symposium on Computers and Communication (ISCC),* Larnaca, pp. 421–426.
•Ahmad, M.Z., and R. Guha, 2012, "A Tale of Nine Internet Exchange Points: Studying Path Latencies through Major Regional IXPs," 2012 IEEE 37th Conference on Local Computer Networks, (LCN), Clearwater, Fla., pp. 618–625.
•Chatzis, N., G. Smaragdakis, A. Feldmann, and W. Willinger, 2013, "There Is More to IXPs than Meets The Eye," *SIGCOMM Comput. Commun. Rev*. 43, 5:19–28.
•Open IX, 2014, "Building Community and Consensus to Foster Data Center and Interconnection Standards," http://www.open-ix.org, accessed August 31, 2015.

Modeling an IXP outage



Source: Argonne National Laboratory

References:
•Facilitated Discussion, March 24, 2015.
•Interview with Equinix, March 17, 2015.
•Open IX, 2014, "Building Community and Consensus to Foster Data Center and Interconnection Standards," http://www.open-ix.org, accessed August 31, 2015.
•Chatzis, N., G. Smaragdakis, A. Feldmann, and W. Willinger, 2015, "Quo vadis Open-IX?", *SIGCOMM Comput. Commun. Rev*. 45, 1:12–18.
•Chatzis, N., G. Smaragdakis, J. Böttger, T. Krenc, and A. Feldmann, 2013, "On the Benefits of Using a Large IXP as an Internet Vantage Point," in *Proceedings of the 2013 Conference on Internet Measurement Conference (IMC '13)*, ACM, New York, pp. 333–346

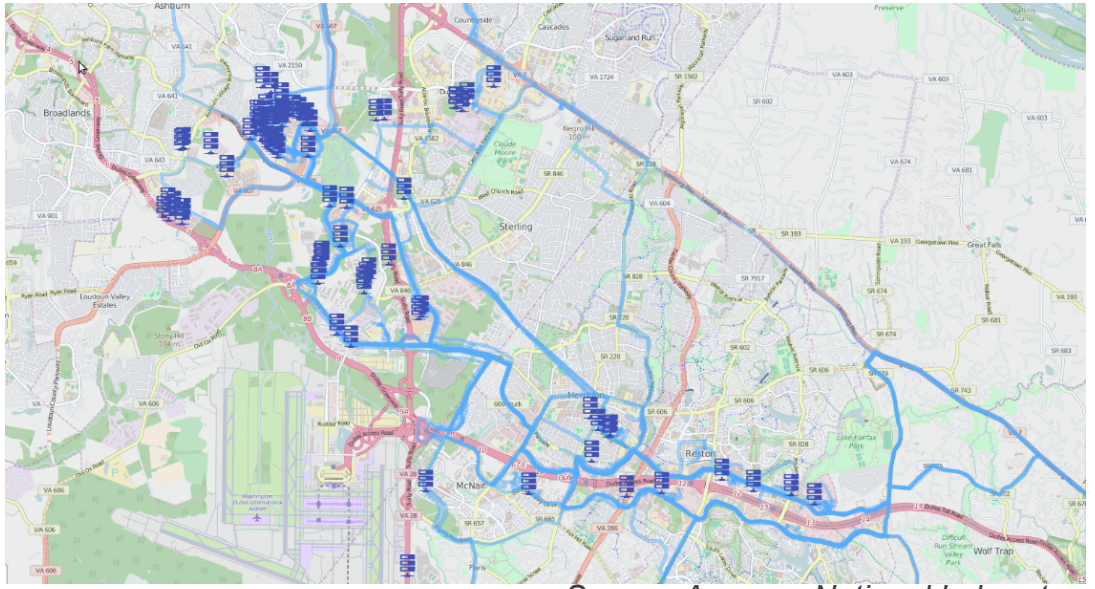
Transparency in both network and data center infrastructure would enhance resilience planning.

- A workshop should be coordinated on the development of cloud and data center service taxonomies and assessments. Such taxonomies and/or assessments should allow for equal comparison of resilience features across providers and empower customers by fostering open, honest competition.

References:
•Facilitated Discussion, March 24, 2015.
•Interview with CenturyLink Communications, March 17, 2015.
•Ted Alford and Gwen Morton, "The Economics of Cloud Computing," Booz Allen Hamilton, accessed July 7, 2014, http://www.boozallen.com/media/file/Economics-of-Cloud-Computing.pdf.
•Brian Hays, "Cloud computing," *Communications of the ACM* 51 (July 2008): 9–11, accessed April 27, 2014, http://cacm.acm.org/magazines/2008/7/5368-cloud-computing/fulltext.
•ISACA (Information Systems Audit and Control Association), Calculating Cloud ROI: From the Customer Perspective, undated, accessed July 7, 2014, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Calculating-Cloud-ROI-From-the-Customer-Perspective.aspx.
• Sarita Paudel, Markus Tauber, and Ivona Brandic, "Security Standards Taxonomy for Cloud Applications in Critical Infrastructure IT," accessed June 20, 2014, https://www.seccrit.eu/upload/Paudel-ICITST-2013.pdf.
•Christopher Wolf, Winston Maxwell, and Hogan Lovells, "Dangerous assumptions about clouds," *CSO,* July 31, 2012, accessed July 9, 2014, http://www.csoonline.com/article/2132027/cloud-security/dangerous-assumptions-about-clouds.html.

Local law enforcement personnel would benefit from training and the exchange of information concerning how to recognize suspicious activity around IT infrastructure assets.

- Law enforcement personnel should engage industry stakeholders to facilitate training and education on fiber routes and suspicious activity. This training should also address how and when to approach maintenance personnel and how to confirm that they are authorized to work in a given area.



Source: Argonne National Laboratory

References:
•Facilitated Discussion, March 24, 2015.
•Interview with Virginia State Police and Loudoun County Sheriff's Department, March 4, 2015.
•Biddle, S., 2012, "How to Destroy the Internet," *Gizmodo,* May 23, http://gizmodo.com/5912383/how-to-destroy-the-internet, accessed August 31, 2015Ahmad, Miller, S., 2006, "Fiber Optic Networks Vulnerable to Attack," *Search Security,* November 15, http://searchsecurity.techtarget.com/news/1230106/Fiber-optic-networks-vulnerable-to-attack, accessed October 11, 2015

Data center and content providers may not have a pathway to contribute to resilience efforts and/or communicate criticality during an emergency.

- A workshop should be conducted for the data center community so that all parties can communicate their needs for points of contact and access to emergency operation center (EOC) resources and for communication pathways during an emergency.

References:

•Facilitated Discussion, March 24, 2015.
•Interview with Virginia State Police and Loudoun County Sheriff's Department, March 4, 2015.

Argonne NATIONAL LABORATORY

Questions? Comments? Please Make Contact

Michael Thompson
Cyber Security Analyst
Argonne National Laboratory
thompsonm@anl.gov

U.S. DEPARTMENT OF ENERGY