[9] N. S. Evans, R. Dingledine, and C. Grothoff. A practical congestion attack on Tor using long paths. In *USENIX Security Symposium*, 2009.

[10] Y. Gilad and A. Herzberg. Spying in the dark: TCP and Tor traffic analysis. In *Privacy Enhancing Technologies*, pages 100–119. Springer, 2012.

[11] K. P. Gummadi, S. Saroiu, and S. D. Gribble. King: Estimating latency between arbitrary Internet end hosts. In *ACM Internet Measurement Workshop (IMW)*, 2002.

[12] N. Hopper, E. Y. Vasserman, and E. Chan-Tin. How much anonymity does network latency leak? *ACM Transactions on Information and System Security (TISSEC)*, 13(2):13, 2010.

[13] R. Jansen, J. Geddes, C. Wacek, M. Sherr, and P. Syverson. Never been KIST: Tor's congestion management blossoms with kernel-informed socket transport. In *USENIX Security Symposium*, 2014.

[14] A. Johnson, C. Wacek, R. Jansen, M. Sherr, and P. Syverson. Users get routed: Traffic correlation on Tor by realistic adversaries. 2013.

[15] C. Lumezanu, R. Baden, D. Levin, N. Spring, and B. Bhattacharjee. Symbiotic relationships in Internet routing overlays. In *Symposium on Networked Systems Design and Implementation (NSDI)*, 2009.

[16] S. J. Murdoch and G. Danezis. Low-cost traffic analysis of Tor. In *USENIX Security Symposium*, 2005.

[17] Neustar IP Geolocation. `https://www.neustar.biz/services/ip-intelligence`.

[18] T. E. Ng and H. Zhang. Towards global network positioning. In *ACM Internet Measurement Workshop (IMW)*, 2001.

[19] T.-W. Ngan, R. Dingledine, and D. S. Wallach. Building incentives into Tor. In *Financial Cryptography (FC)*, 2010.

[20] A. Panchenko and J. Renner. Path selection metrics for performance-improved onion routing. In *Symposium on Applications and the Internet (SAINT)*, 2009.

[21] L. Peterson, T. Anderson, D. Culler, and T. Roscoe. A blueprint for introducing disruptive technology into the Internet. In *Workshop on Hot Topics in Networks (HotNets)*, 2002.

[22] M. K. Reiter and A. D. Rubin. Crowds: Anonymity for web transactions. *ACM TISSEC*, 1(1):66–92, Nov. 1998.

[23] Reporters Without Borders. Enemies of the Internet 2013 Report. `https://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf`, Mar. 2013.

[24] RIPE NCC. RIPE Atlas. `https://atlas.ripe.net`.

[25] SamKnows. `https://www.samknows.com`.

[26] S. Savage, A. Collins, E. Hoffman, J. Snell, and T. Anderson. The end-to-end effects of Internet path selection. In *ACM SIGCOMM*, 1999.

[27] A. Schulman and N. Spring. Pingin' in the rain. In *ACM Internet Measurement Conference (IMC)*, 2011.

[28] M. Sherr, M. Blaze, and B. T. Loo. Scalable link-based relay selection for anonymous routing. In *Privacy Enhancing Technologies Symposium (PETS)*, 2009.

[29] R. Sherwood, B. Bhattacharjee, and A. Srinivasan. $\mathcal{P}5$: A protocol for scalable anonymous communication. *Journal of Computer Security*, 13(6):839–876, 2005.

[30] Stem Controller Library. `https://stem.torproject.org`.

[31] S. Sundaresan, S. Burnett, N. Feamster, and W. De Donato. BISmark: A testbed for deploying measurements and applications in broadband access networks. In *USENIX Annual Technical Conference*, 2014.

[32] Tor Metrics. `https://metrics.torproject.org`.

[33] B. Wong, I. Stoyanov, and E. G. Sirer. Octant: A comprehensive framework for the geolocalization of Internet hosts. In *Symposium on Networked Systems Design and Implementation (NSDI)*, 2007.