

- end-system characteristics. In *Passive and Active Network Measurement Workshop (PAM)*, 2005.
- [17] E. Chien. Downadup: Attempts at Smart Network Scanning. www.symantec.com/connect/blogs/downadup-attempts-smart-network-scanning, 2009.
- [18] CIA. The World Factbook: Population.
- [19] Í. Cunha, R. Teixeira, and C. Diot. Measuring and Characterizing End-to-End Route Dynamics in the Presence of Load Balancing. In *Passive and Active Network Measurement Conference (PAM)*, 2011.
- [20] A. Dainotti, R. Amman, E. Aben, and k. claffy. Extracting Benefit from Harm: Using Malware Pollution to Analyze the Impact of Political and Geophysical Events on the Internet. *SIGCOMM Comput. Commun. Rev. (CCR)*, 42, Jan. 2012.
- [21] A. Dainotti, K. Benson, A. King, k. claffy, E. Glatz, X. Dimitropoulos, P. Richter, A. Finamore, and A. Snoeren. Lost in Space: Improving Inference of IPv4 Address Space Utilization. Technical report, CAIDA, Oct 2014.
- [22] A. Dainotti, K. Benson, A. King, k. claffy, M. Kallitsis, E. Glatz, and X. Dimitropoulos. Estimating Internet Address Space Usage through Passive Measurements. *SIGCOMM CCR*, 44(1), Dec. 2013.
- [23] A. Dainotti, A. Pescapè, and K. Claffy. Issues and future directions in traffic classification. *IEEE Network*, 26(1):35–40, Jan 2012.
- [24] A. Dainotti, C. Squarcella, E. Aben, k. claffy, M. Chiesa, M. Russo, and A. Pescapè. Analysis of Country-wide Internet Outages Caused by Censorship. In *Internet Measurement Conference (IMC)*, 2011.
- [25] A. Dhamdhere and C. Dovrolis. Twelve Years in the Evolution of the Internet Ecosystem. *IEEE/ACM Transactions on Networking*, 19, Sep 2011.
- [26] Z. Durumeric, M. Bailey, and J. A. Halderman. An Internet-Wide View of Internet-Wide Scanning. In *USENIX Security*, 2014.
- [27] N. Falliere. Sality: Story of a Peer-to-Peer Viral Network. www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/sality_peer_to_peer_viral_network.pdf, 2011.
- [28] J. Goubault-Larrecq and J. Olivain. Detecting Subverted Cryptographic Protocols by Entropy Checking. Technical Report LSV-06-13, Laboratoire Spécification et Vérification, ENS Cachan.
- [29] J. Heidemann, Y. Pradkin, R. Govindan, C. Papadopoulos, G. Bartlett, and J. Bannister. Census and Survey of the Visible Internet. In *IMC*, 2008.
- [30] V. Jacobson, R. Braden, and D. Borman. TCP Extensions for High Performance. RFC 1323 (Proposed Standard), May 1992.
- [31] E. Katz-Bassett, H. V. Madhyastha, J. P. John, A. Krishnamurthy, D. Wetherall, and T. Anderson. Studying Black Holes in the Internet with Hubble. In *NSDI*, 2008.
- [32] A. Kumar, V. Paxson, and N. Weaver. Exploiting Underlying Structure for Detailed Reconstruction of an Internet-scale Event. In *IMC*, 2005.
- [33] Z. Li, A. Goyal, Y. Chen, and V. Paxson. Automating Analysis of Large-scale Botnet Probing Events. In *ACM Symposium on Information, Computer, and Communications Security (ASIACCS)*, 2009.
- [34] Y. Liu and Y. Yang. Analysis of P2P Traffic Identification Methods. *Emerging Trends in Computing and Information Sciences*, 4(5), 2013.
- [35] A. Loewenstern and A. Norberg. DHT Protocol. www.bittorrent.org/beps/bep_0005.html, Jan 2008.
- [36] A. Lutu, M. Bagnulo, and O. Maennel. The BGP Visibility Scanner. In *Global Internet Symposium (GI)*, 2013.
- [37] B. McDanel. TCP Timestamping - Obtaining System Uptime Remotely. seclists.org/bugtraq/2001/Mar/182, 2001.
- [38] K. McNamee. Malware Analysis Report: New C&C Protocol for ZeroAccess/Sirefef. botnetlegalnotice.com/zeroaccess/files/Ex_14_Decl_Anselmi.pdf, 2012.
- [39] D. Moore, C. Shannon, D. Brown, G. Voelker, and S. Savage. Inferring Internet Denial-of-Service Activity. *ACM Transactions on Computer Systems*, 24(2), May 2006.
- [40] A. Norberg. uTorrent transport protocol. www.bittorrent.org/beps/bep_0029.html, June 2009.
- [41] R. Pang, V. Yegneswaran, P. Barford, V. Paxson, and L. Peterson. Characteristics of Internet Background Radiation. In *IMC*, 2004.
- [42] V. Paxson. End-to-end Routing Behavior in the Internet. In *ACM SIGCOMM*, 1996.
- [43] M. Prince. The DDoS That Almost Broke the Internet. blog.cloudflare.com/the-ddos-that-almost-broke-the-internet, March 2013.
- [44] M. Sargent, J. Czyz, M. Allman, and M. Bailey. On The Power and Limitations of Detecting Network Filtering via Passive Observation. In *PAM*, 2015.
- [45] K. Schomp, T. Callahan, M. Rabinovich, and M. Allman. On Measuring the Client-side DNS Infrastructure. In *IMC*, 2013.
- [46] The Bro Project. TCP Scan detection. bro.icir.org/sphinx/scripts/policy/misc/scan.bro.html, 2014.
- [47] B. Van Nice. Drilling Down into DNS DDoS. www.nanog.org/sites/default/files/nanog63-dnstrack-vannice-ddos.pdf. NANOG 63, Feb 2015.
- [48] E. Wustrow, M. Karir, M. Bailey, F. Jahanian, and G. Huston. Internet Background Radiation Revisited. In *Internet Measurement Conference (IMC)*, 2010.
- [49] M. Zalewski. p0f v3: passive fingerprinter. lcamtuf.coredump.cx/p0f3/README, 2012.
- [50] S. Zander, L. L. H. Andrew, and G. Armitage. Capturing Ghosts: Predicting the Used IPv4 Space by Inferring Unobserved Addresses. In *IMC*, 2014.
- [51] M. Zhang, C. Zhang, V. Pai, L. Peterson, and R. Wang. PlanetSeer: Internet Path Failure Monitoring and Characterization in Wide-Area Services. In *Operating Systems Design and Implementation (OSDI)*, 2004.