Middle East Political Protest And Internet Traffic Report

February 12 – 20, 2011

Craig Labovitz
Chief Scientist, Arbor Networks

The success of the Tunisian and Egyptian protest movements inspired demonstrations throughout the Middle East last week, including large-scale social media coordinated protests in Libya, Iran, Bahrain, Algeria, Jordan and Yemen. In several of countries, governments responded to the calls for reform with arrests and violent suppression of public demonstrations. Increasingly, several Middle Eastern governments also may be disrupting phone and Internet communication to contain the spread of unrest.

These new Internet filtering efforts come a week after Egypt returned to the Internet following an abortive effort to block protests demanding the then president, Hosni Mubarak, resign. While other countries, including Iran and Myanmar, disrupted telecommunication following social unrest in the past, the Egyptian outage represents a new Internet milestone – the first highly connected, telecommunication dependent society to intentionally disconnect from the Internet [1,2].

This analysis uses real-time data from the 110 Internet providers around the world to identify possible ongoing Internet traffic manipulation in Middle East countries with active protest movements. More details on our data collection infrastructure and methodology are available in our recent academic paper [3].

Overall, our data shows pronounced changes in Internet traffic levels in two Middle East countries last week: Bahrain and Libya. While network failures and other exogenous events may play a role in decreased traffic volumes, we observe the changes in Bahrain and Libya are temporally coincident with the onset of recent protests. Several Bahrain telecommunication companies blamed the slowdown on "overloaded circuits" and extremely high usage [4].

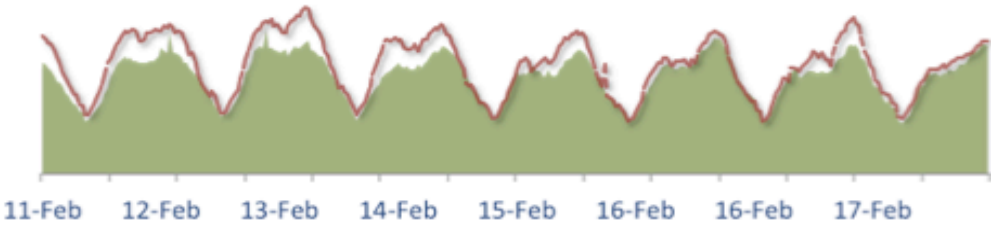
We note that many countries in the region maintain some level of permanent Internet limits, including blocks on dissident web sites, social media and adult content [5]. The traffic volumes graphed on the following page represent possible traffic manipulation beyond normal filtering practices.

In the below chart, we show the "normal" traffic in and out of each country averaged over the proceeding three weeks in green. The dotted red line in each graph shows the traffic over the last seven days. Orange shaded areas indicated periods of statistically abnormal traffic either last week. Abnormal traffic volumes may represent transient network failures or periods of intentional traffic manipulation. Due to the near complete block of all Internet traffic (January 27 – February2), the Egyptian graph three week average in shaded green is lower than the traffic volumes seen last week.. Yemen Internet traffic also exhibited brief, though unusual dips, during the prior week (February 7-14) and also includes an orange period.

Middle East Internet Scorecard

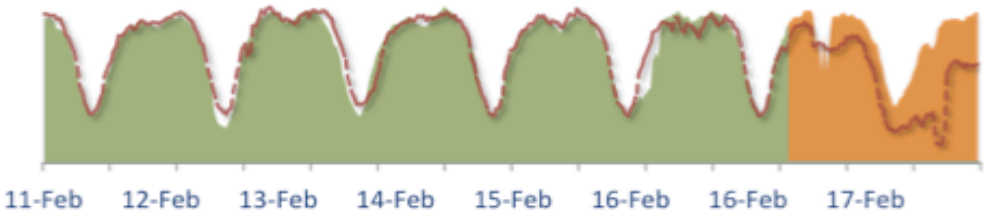
Iran

While Iran aggressively filtered Internet access during past unrest, Iranian traffic showed little significant change over the last two weeks.



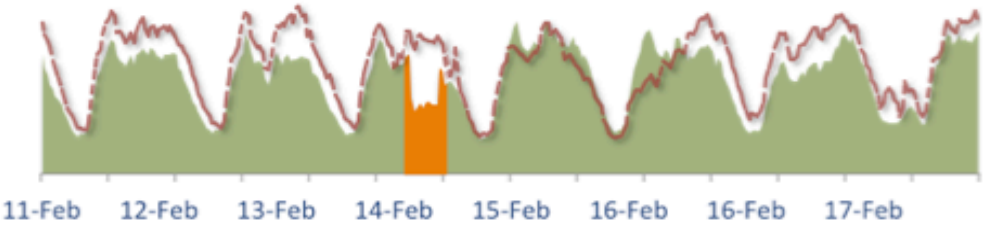
Libya

A traffic slow down beginning late last week culminated in the abrupt loss of all Internet traffic on February 18th.



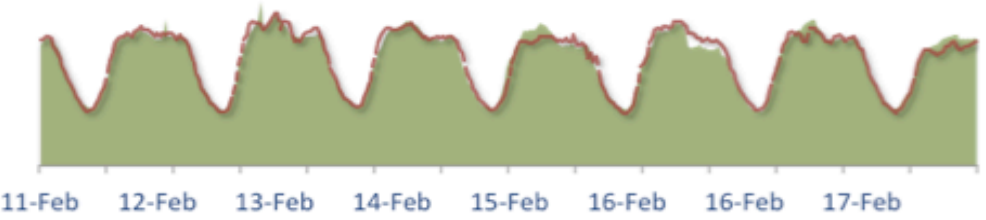
Yemen

After traffic drops earlier in the month possibly related to added filtering, Internet traffic was higher than average last week.



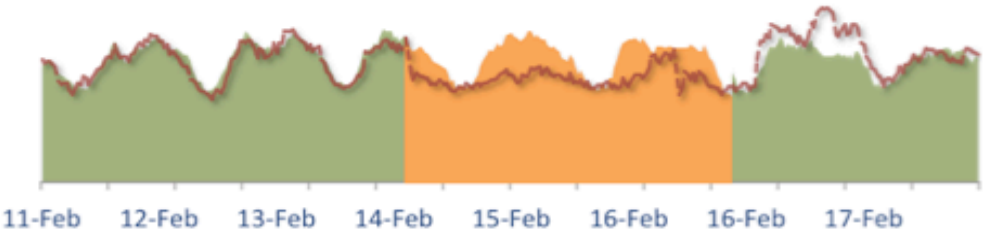
Algeria

Traffic remained remarkably constant over last several weeks. No sign of added filtering.



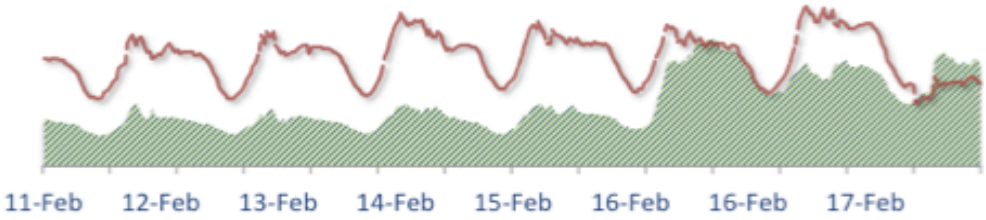
Bahrain

Pronounced drop in traffic during the mid-part of last week. Government blamed the slow-down on "overwhelmed Internet circuits".



Egypt

After a week of near complete loss of Internet, Egypt returned to the net last week with normal traffic volumes.



Anomalous traffic | Average traffic (previous three weeks) | Traffic last week

While the Internet has proven a powerful tool for rallying social and political change, so too have governments recognized their regulatory and technical capability to disrupt communications. The next few weeks will likely prove a major contest between the continued evolution of the Internet as a vehicle for political change and authoritarian governments' continued assertion of control.

End Notes

[1] Craig Labovitz, "Egypt Loses the Internet". Arbor Networks blog post. Available at http://asert.arbornetworks.com/2011/01/egypt-loses-the-internet. January 28, 2011.

[2] James Cowie, "Egypt Leaves the Internet". Renesys blog post. Available at http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml. January 27, 2011.

[3] Craig Labovitz, Scott Iekel-Johnson, Danny McPherson, Jon Oberheide, and Farnam Jahanian, "Internet Inter-Domain Traffic". Proceedings of ACM SIGCOMM 2010, New Delhi. August, 2010.

[4] Christopher Rhoads, "Technology Poses Big Test for Regimes". Wall Street Journal. February 12, 2011.

[5] OpenNet Initiative. Web site at http://opennet.net.

About the Author

Craig Labovitz is Chief Scientist at Arbor Networks where he is responsible for the core technology, architecture and commercial strategy behind Arbor's successful carrier security products. Labovitz is the author of more than a dozen peer-reviewed networking research papers, journal articles and patents. Dr. Labovitz received his PhD and MSE from the University of Michigan and his BSE from the University of Pennsylvania. More information about the author is available at http://www.monkey.org/~labovit.

About Arbor Networks

Arbor Networks, Inc. is a leading provider of network security and management solutions for converged carrier networks and next-generation data centers, including more than 70 percent of the world's Internet service providers and many of the largest enterprise networks in use today. Arbor's proven network security and management solutions help grow and protect customer networks, businesses and brands. Through its unparalleled, privileged relationships with worldwide service providers and global network operators, Arbor provides unequalled insight into and perspective on Internet security and traffic trends via the Active Threat Level Analysis System (ATLAS®). Representing a unique collaborative effort with 100+ network operators across the globe, ATLAS enables the sharing of real-time security, traffic and routing information that informs numerous business decisions.

ARBOR NETWORKS

Corporate Headquarters
6 Omni Way
Chelmsford, Massachusetts 01824
Toll Free USA +1 866 212 7267
T +1 978 703 6600
F +1 978 250 1905

Europe
T +44 208 622 3108

Asia Pacific
T +65 6299 0695

www.arbornetworks.com

Copyright ©1999-2011 Arbor Networks, Inc. All rights reserved. Arbor Networks, the Arbor Networks logo, Peakflow and ATLAS are all trademarks of Arbor Networks, Inc. All other brands may be the trademarks of their respective owners.