Rami Khater

Georgetown University

rk299@georgetown.edu

Digital Protectionism: Preparing for the coming Internet Embargo

Presented at the Center for Contemporary Arab Studies 2010 Annual Symposium

Information Evolution in the Arab World

For years developed countries in the West have spoken of the threat of the ‘end of oil’ or another embargo that would debilitate and destabilize their economies and lifestyles, which are hungry for fossil fuels. Many of these developed nations are taking concrete steps to become energy independent, to reduce the risk and magnitude of a future interruption to supplies of oil.

In a reversal of roles, the Middle East is now as dependent on Western Internet services as the West is on Middle East oil. While the United States government takes tentative steps to become oil independent and free itself of the influence of other nations, the Middle East must begin its own Internet independence campaign, before the first embargo hits. Middle Eastern countries that do not prepare suitable alternatives to the most popular Internet services, such as email, blog platforms, search engines and cloud computing software, run the risk of economic and social disruption. Furthermore, and of equal importance, the data collected by websites and companies through the Internet services they provide can give them unique, in depth, and real-time insight into countries around the globe. The possession of this knowledge by foreign entities, whether private or government-owned, is a challenge to the sovereignty of other nation states.

Virtual Infrastructure

The Internet is a distributed architecture by design, with many nodes connected in an infinite mesh. If portions of the network go out of service, the network is durable and capable of working around the problem areas. However, the Internet *services* that users around the globe depend on (Google, Facebook, Youtube, Wikipedia, Blogspot, Amazon etc) are in a very concentrated, centralized, and non-durable service network that does not adhere to the distributed and decentralized architecture of the Internet itself.

The most used Internet services have become essential virtual infrastructure upon which many other services and infrastructures operate. Email and chat are the equivalent of dynamically created phone lines, blogs are instantly accessible newspapers and search engines are our indices of knowledge. We take these services for granted and do not realize the potential interruption if only one of them were to be inaccessible for any serious length of time.

So far, the Internet has been a largely uncontrolled domain where the traditional rules and priorities of the nation state have been largely ignored. Faced with its unprecedented growth and innovation, many countries have been unwilling to control the activities of their citizens in the belief that it would undermine potential gains. However, a small number of countries control the vast majority of popular services[1] and this has given them a great deal of power over all other nations.

Unlike an oil embargo, an Internet embargo would disrupt communications between individuals, business and government, as well as creating traditional economic problems. Many Middle Eastern countries rely on Google and Yahoo as search engines, Microsoft for chat, Wordpress for blogs, and many other American or European companies for the

[1] Alexa rankings as of March 2010 - http://www.alexa.com/topsites/global

hosting of websites. In the event of political fallout between an Arab country and the United States, the Internet weapon could be used as a sanction. This would not mean a complete cessation of Internet activity in that Arab country, but users would be unable to access services and websites from 'American' companies. Imagine a Middle Eastern netizen unable to access a piece or the whole of foreign virtual infrastructure. Major Arab corporations' websites could fall as well, as they are commonly hosted by American or European website hosting services. They would go offline and disappear from the Web. The speed and ease [2] with which this partial or total embargo could be accomplished would astonish those who have not prepared for the possible use of Internet services for leverage or as a weapon.

A number of recent events have brought the potential of an Internet embargo to the forefront. On January 21, 2010, Secretary of State Hilary Clinton gave a speech[2] on the U.S. government's Internet doctrine and said the Internet was a tool for democracy and that 'American' companies should not bow to the desires of nations with unethical practices or laws. Secretary Clinton made it readily apparent; American Internet companies should toe the national line in full, and are no longer exempt from American ideals and laws; they must act ethically, even at the risk of alienating others. This is in direct contrast to the activities of American Internet services in the past when dealing with countries such as China [4].

Days after the Clinton speech, the massively popular website sourceforge.net, a repository for open source projects and collaboration, blocked access [6] to any visitors from Iran, North Korea, Syria, Sudan, Cuba and others nations[3]. Only after an uproar from the open source community, on the grounds that the blocking violated the very

[2] Link to speech - http://www.state.gov/secretary/rm/2010/01/135519.htm

[3] Denied Persons List and the Entity List, and other lists

nature (and laws) of the open source movement [8], was the policy adjusted. Individual open-source projects on sourceforge.net may now decide if they want to block access from this predefined list of countries to their project group or not.

SourceForge released a statement explaining why it had restricted access.

> *'...restrictions on the free flow of information rub us the wrong way. However, in addition to participating in the open source community, we also live in the real world, and are governed by the laws of the country in which we are located. Our need to follow those laws supersedes any wishes we might have to make our community as inclusive as possible.' [9]*

The message was clear to nations dependent on this virtual infrastructure: 'We control access to knowledge and critical services on the Internet'. This was a small example, perhaps even a warning. If SourceForge were a Swedish organization hosted in the UAE, would they have blocked access to its site from these nations as well?

Iran has taken the first step in the Middle East towards digital protectionism. Taking a hint from the Clinton speech and the sourceforge.net debacle, Iran struck the first blow by blocking all access to Gmail[4] [10] from their national IP address range[5] to the Google service. This is not an act against the interests of Google; rather it is against the United States. Iran views the virtual infrastructure (in this case email) as a proxy for American interests, and since Iran cannot control or monitor the Gmail service, it simply decided to block it. Iran plans to launch a state-run email service [2] for its citizens, so that they may not only communicate effectively but also reduce the likelihood that a disruption in services, prompted by a foreign entity, will affect their national economy and stability.

[4] Google's email service, http://www.gmail.com

[5] Any traffic that appears to originate from inside Iran

The Iranian government did not choose to block Yahoo or Hotmail email services, which leads many to believe that this is a symbolic move to let the United States know that it is prepared to act. Logically, Iran has taken the first necessary step to reduce its dependence on Western Internet services for its own stability and future.

Iran has chosen to use a state-run email service, but it could have used a privately run system through an Iranian corporation. The important point is that the organization, private or public, in charge of these critical services, is loyal to that specific nation or the region (the Middle East) and willing to cooperate when needed [2]. In essence, Iran wants to be in a position similar to that of the United States, with uninhibited access to data and control over virtual infrastructure [2].

Digital protectionism in the Middle East does not need to be on a country-by-country basis. For example, the Gulf Corporation Council (GCC) may decide that it desires to have a regional system, or Syria, Lebanon and Palestine could opt to work together as well. Countries may go it alone for certain services such as email, and will combine their efforts for larger problems such as search engines. This infrastructure cannot possibly be built over weeks or even months; it would take years to reach a level of sophistication found in offerings by world-class providers. However, this is an investment in their future, for reasons of sovereignty and economics.

Creating homemade virtual infrastructure and Internet services has many positive effects, apart from being a wise precaution against hostile Internet behavior. Setting up such services in the Middle East will help create knowledge centers and the services should be better suited to the regional culture and population. These services would not be exclusively for the Middle East either; an Arab-made blogging tool and platform may be massively popular in the Arab world and translated into other languages, so users worldwide may leverage the service. While the initial point is to protect against hostile activity from outside, the Middle East would benefit from competing with the same Internet services that they are protecting themselves from. *The best way to protect against a virtual infrastructure blockade is to create an alternative.*

Businesses would also benefit as they could use virtual infrastructure in the Middle East to host their websites and offer those same services to foreign clients as well. The skills required to build these services would create a new class of professionals in the region who could market their skills at home and abroad. It is a win-win-win situation for the state, business and individual in the region.

Iran took the route of completely blocking a foreign service so that it could move its citizens to its own offering. However, this is not a viable option in the long run as it does not build trust with their local population, and trust will be necessary for the new virtual infrastructure and services to thrive. The best way to move people to government-approved services (private- or state-owned) would be through silent degradation of traffic to foreign websites.

These ‘virtual tariffs’ - inconveniences such as the random blocking of websites or fake 404 (‘Not Found’) messages - will nudge local users towards preferred services, because the local offerings will appear quicker and more responsive than their identical foreign counterparts. If Middle Eastern users believe that the local email service is superior to the outside offering, *but they still have access to the outside service*, then they will voluntarily make the move to the ‘better’ provider. When users voluntarily make the switch, they are likely to stay. However, this switch will not take place overnight, but will take years. Many individuals in the Arab world have invested a great deal of time in the Western Internet services they use, and an abrupt switch is simply not possible or desirable in most cases.

Issues of Sovereignty

The same companies who run the most popular global virtual infrastructure have benefited immensely from the amount of data they are constantly collecting. David Bollier notes in *The Promise and Peril of Big Data* that at times Google knows more about what is going on inside the United States than the government itself. This is not meant to insinuate that this knowledge is negative; on the contrary, Google has used it for good. Google provided swine flu trends to the government up to two weeks before a government report on the subject was finished, with over 95 percent accuracy when compared to the final official document [14].

The United States government benefits immensely from access to this kind of data in times of need. In fact, access to the data helps the government *govern* more effectively. However, providers also have similar data and knowledge about other nations as well; these data give these private entities an enormous amount of power. Search engines may know more about the current economic issues in Greece than the country itself or the entire European Union, in real time. Twitter may have statistics showing that the search terms ‘coup’ and ‘revolution’ have increased two hundred times in a country since a disputed election.

Marc Lynch of Foreign Policy has displayed a quick and simple example of the knowledge that is waiting to be unearthed in these massive datasets. Lynch searched Google for ‘third intifada’ in Arabic and tweeted that he found ‘123,000 hits in the last month vs 178,000 in all of 2009’[6]. Such a massive increase in a phrase with direct ties to the Israeli-Palestinian conflict could be an indicator of the negative outlook the Arab world has on the current state of affairs.

[6] http://bit.ly/9vxr0U

What makes this data even more interesting is the collective and peer-produced nature of it. There was no concerted effort from millions of Arabic-language Internet users to use the phrase ‘third intifada’ in the past month, and this statistic is the collective truth gathered from separate actions. Therefore the data being collected in micro-increments is honest data, somewhat of a collective conscious. If Lynch found a trend in the ocean of publicly available data, what could he find out if he had access to the private and public datasets?

These private corporations will soon know more about foreign sovereign nation states than those states know about themselves. As the use of foreign virtual infrastructure increases, they are capable of more data mining for past trends and statistically accurate predictions of the future. The sovereignty of these nation states is directly challenged when a foreign entity beholden to the laws and desires of a foreign nation can effectively predict its economic, political and social future. Therefore the need for virtual infrastructure is also an investment in the future of regional stability and in the sovereignty of each individual nation state in the Arab world.

Issues of Individual Control

Implicit in the term sovereignty is control. However, the issues laid out in the previous section speak to the collective action of the masses rather than the acts of the individual. Every form of Internet access is by nature adding to the collective and is individual at the same time; therefore we cannot completely separate the two.. However, the nature of the device used for that Internet action may enhance the individualistic aspect of the action, as in the case of smartphones.

When surfing the web on a laptop or regular computer, the user is mostly stationary, and in many parts of the world multiple individuals share one traditional computing device.

Mobile phones on the other hand are usually used by one person, and are unique in that every action is traceable back to that specific individual.

Mobile phones, especially smartphones, make further inroads into the sovereign domain of many states. Research In Motion (RIM), the creator of the massively popular Blackberry device, is based in Canada, and the architecture of their service is, out of all the most popular smartphone services, the most centrally controlled. Other than traditional mobile phone services such as SMS and phone calls, all other data and services run through RIM’s servers in Canada. The most notable of these centrally controlled services are traditional web browsing and the Blackberry Messenger; the latter is in and of itself a global phenomenon. The issue is that governments cannot view conversations or censor web browsing over these centrally controlled services. Both of the services encrypt data, which is then sent back to Canada, where data is stored and, when needed, encrypted and sent back to the user. All of the world's Blackberry data for these centrally controlled services are kept in Canada, and the data is currently accessible by only a few governments, including the United States and Canada.

Many Middle Eastern states, especially in the Gulf region, view this as completely unacceptable. Kuwait, the United Arab Emirates, and Saudi Arabia all threatened to impose restrictions on Blackberry services if RIM did not give them access to data and the ability to censor specific websites [16]. The Blackberry devices have always had this centrally controlled mechanism, but it is only recently that there have been claims that the devices are used for nefarious means and are security risks [18]. Of course many governments simply want to eavesdrop on their citizens’ conversations and when they cannot do so, they imagine a cornucopia of potential criminal uses for the device.

The Center for Democracy and Technology believes that this is an attack on *Internet Freedom [20]* – but it is not. Rather, these sovereign states want the same rights as

Canada and the United States in monitoring their citizens' actions. It is hard to argue that one government's demand for access to information is legitimate while identical demands by other governments are an attack on individual rights.

RIM is reported to have come to agreements with all Middle Eastern countries that have expressed concern thus far. They will censor websites for Kuwait, they have made adeeal with the UAE, and will give Saudi Arabia access to their users data via a control system within Saudi borders [19]. Internet forums and blogs have been abuzz with claims that "the flood gates have opened", indeed, the Middle East, heavy users of the latest technology but with little virtual infrastructure or devices of their own are realizing the new great game – control of and access to Internet information data and flows.

Conclusion

It is not a matter of *if* but of *when* the Internet will be used as an economic and social weapon similar to any other weapon used throughout history when there is dependency relationship. The world has been mislead to believe that the Internet is a place that cannot be controlled and which has no boundaries. Nation states will find that their dependence on the Internet and related services may prove to be detrimental if they are unwilling to create their own services and virtual infrastructure to offset some of that need.

The warning shots have been fired and the lines drawn in virtual space. The Middle East has been in a precarious position over the last 100 years, being semi-dependent on foreign countries for various services. There are no Middle Eastern search engines, email services, chat or cloud platforms, or online retailers that are worth discussing in earnest. The entire region and its users may be removed from accessing the Web, with no viable options to turn to. Protectionist policies exist in every nation, for a variety of reasons; digital protectionism is the next logical step.

BIBLIOGRAPHY

[1] L. Lessig, *Code and other laws of cyberspace*, Basic Books, 1999.

[2] C. Rhoads, C. Cummins, and J.E. Vascellaro, ‘Iran to Suspend Google's Email’, *wsj.com*, Feb. 2010.

[3] ‘Google “may end China operations”,’ *BBC*, Jan. 2010.

[4] J. Yang, ‘Google Defends Censorship of Web Sites,’ *ABC News*, Jan. 2006.

[5] S. Levy, ‘Google and the China Syndrome’, *Newsweek*, vol. 147, 2006, pp. 14-14.

[6] K. Shoemaker, ‘When Ideologies Collide: SourceForge Blocks Countries on US Sanction List’, *OSTATIC: Find . Evaluate . Collaborate*, Jan. 2010.

[7] ‘Google to stop censoring Chinese search results “soon”, China warns of consequences -- Engadget.’

[8] I. Abdulrahman, ‘Post Clinton’s Internet Freedom Speech:US- SourceForge Blocked Syria, Sudan, Iran, N. Korea & Cuba: Is Open Source Still Open?’, *ArabCrunch*.

[9] ‘SourceForge.net: Clarifying SourceForge.net’s denial of site access for certain persons in accordance with US law.’

[10] C. Rhoads, C. Cummins, and J.E. Vascellaro, ‘Iran to Suspend Google's Email’, *wsj.com*, Feb. 2010.

[11] ‘Iran Shuts Down Gmail, Announces National E-Mail Service,’ Feb. 2010.

[12] B. Etling, J. Kelly, R. Faris, and J. Palfrey, ‘Mapping the Arabic Blogosphere: Politics, Culture, and Dissent,’ *Berkman Center Publication Series*, 2009.

[13] H. Norman, ‘Sex, Social Mores and Keyword Filtering: Microsoft Bing in “Arabian Countries”,’ 2010.

[14] D. Bollier, ‘The Promise and Peril of Big Data,’ 2010.

[15] J. Palfrey, ‘The Public and the Private at the United States Border with Cyberspace’.

[16] J.L. Goldsmith and T. Wu, *Who controls the Internet?: illusions of a borderless world*, Oxford University Press, USA, 2006.

[17] D. Goodin, ‘SourceForge bars 5 nations from open source downloads,’ *The Register*, Jan. 2010.

[18] J. York, ‘Jillian York: LinkedIn Alienates Syrian Users: Why Now?’, *The Huffington Post*, Apr. 2009.

[19] R. Waters, ‘Google to shut China search engine’, *The Financial Times*, Mar. 2010.