Internet Localization as a Minimal Defense against Internet Weaponization

By Dr. George Kostopoulos
Professor of Cybersecurity
University of Maryland University College, USA

Introduction

In the recent years, a new resource has become available to the world that has greatly enhanced communications, having equally enhanced the productivity of practically all sectors. This resource covers the world like the sun and the moon, having become an infrastructure for the creation and implementation of previously impossible accomplishments. This resource is the Internet – a centrally managed network of networks – that is a valuable asset beyond quantitative valuation.

A natural question is: Who owns the Internet? "*The Internet is a network of networks. Each of the separate networks belongs to different companies and organizations, and they rely on physical servers in different countries with varying laws and regulations*." [1]

The Internet is nominally managed and administered by ICANN (Internet Corporation for Assigned Names and Numbers) [2]. ICANN " *. . . is a nonprofit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, ensuring the network's stable and secure operation.*" [3] Physical nodes are located in countries around the world facilitating the network's speedy and effective operations. [4]

It is a fact that in the Internet, conceptually, there are no physical borders, and that the world is fully interconnected with unlimited benefits to be derived. As the Internet grows in usefulness and in coverage, this bona fide assumption is being shaken by the thought of potential actions that will isolate or divide the world. A world that the Internet has in some way united.

In reality, *" . . . the Internet is a network of networks . . . "* [1] . These networks, consisting of routers and servers, miles of cables - optical and copper - as well as of wireless links. They belong to various companies or national organizations, where they must comply with the rules and decisions of the governments of the respective countries. The fears of the Global Commission on Internet Governance is that, " . . . *the political controls imposed by governments would cause people to lose trust in the Internet . . .* " [5] As described further down in this paper, there are numerous cases where governments have shut down the Internet in selected areas and at selected times, presumably for the common good.

It is beyond doubt that most of the Western World's data physically reside in servers that are located in the United States. The various social media entities, that enjoy worldwide trust and offer free services, have their data warehouses with billions of accounts in the US. Universities for their convenience have their email accounts managed by gmail, which is a US-based business organization. Even the Ministry of Foreign Affairs of a European

country, after a major email system crash, of unknown cause, has now employed the gmail services. That is, now all of the Ministry's emails are stored in the gmail servers, thousands of miles away.

In an ideal world there is nothing wrong with all of the above, but in today's world, governments may access all accounts and data of all servers, routers and data warehouses physically residing in their territories. Furthermore, governments may oblige certain businesses not to accept a client's email account if the respective server is inaccessible by them.

A real life example is where recently in the US an American lady wanted to open a bank account. Among the various required personal data the lady, was asked to enter her email account. Because her account was @yandex.com, a company that has its servers outside of the US, she was denied the opening of a bank account.

We hear right and left of American sanctions against other countries [6]. What if such sanctions include the cut off of Internet communications in and out of the US? Then, the Internet will turn from being a valuable asset into a dangerous liability.

The objective of this paper is to raise fears that the Internet is progressively becoming a politico-economic weapon and that only Internet Localization could possibly minimize the adverse impact of such an Internet Weaponization. Through an Internet Localization plan, data will be stored and services will be provided out of organizations physically located in the clients' country, along with their data storage systems.

Internet Utilization

There are endless examples where the Internet has been used as an information, or misinformation medium. It is believed that " *. . . the Internet plays a larger role in governance, campaigns and activism, . . .* "[7] Indeed, governments very effectively use the Internet to make citizens knowledgeable of the various laws, rules and regulations. However, when it comes to political campaigns, "*In 2008, voter-generated content on social media altered the trajectory of the campaign several times.*"[8]

Unfortunately, besides the knowledge and information the Internet serves as a loudspeaker for false news. However, such news reach different populations at different rates. While the west side of the Atlantic was flooded with false news accusing Russians " *. . . of trying to interfere with the most recent* (US) *presidential elections, . . "* [9] on the east side of the Atlantic *" . . . most of the false news . . . reached* (only) *1 percent or less of the . . . online population . . .* "[9]

By now, it must be realized that, the Internet has become an integral part of the technologically developed world, and its disruption will create unthinkable and irreparable damage. Internet's contribution to business, and to the economies at large, is fundamental, and it has established a very valuable platform. In the education sector, where information and knowledge flows on a continuous basis, any disruption on the Internet services will be catastrophic. As for the health industry, the " *. . . Internet is an indispensable utility service for health care industry. Most of patient information repositories, documentations and records are maintained on online servers."* [10], and any Internet services shut down will effectively shut down the hospitals.

Internet Shutdown

It is reported that "*Governments across the world are increasingly resorting to Internet shutdowns . . . with the objective of controlling the exchange of information online*." [10]. Disabling access to the Internet has been a standard practice in India for a variety of reasons ranging from riots prevention, to avoidance of cheating in academic examinations. [11]. For the latter reason the government of Algeria, as well as that of Iraq, disabled their Internet for a limited period of time [12]. During the so called, Arab Spring,*" . . . Egypt took the unprecedented step of severing all Internet connections and shutting down its cellphone services . . . "* [13]. Also, in Russia the Internet was disabled in Crimea to prevent " *. . . an alleged terror attack that Ukraine had plotted in the region . . .* " [14].

Besides the government authorized Internet shut downs, there are also frequent anonymous Internet access shut downs having targeted specific websites. Such shut downs are created through excessive artificial demand for services out of particular websites. One such attack, known as DDoS, Distributed Denial of Service, took place in the USA on Friday October 21, 2016.

This attack disabled several popular websites including the *" . . . Vox, Twitter, Spotify, Amazon, PayPal and Reddit . . . that overloaded websites by sending them more than 150,000 requests for information per second. "* [15] Some intelligence analysts rushed saying that " *. . . their analysis pointed to Russia . . . and others saying it could just be "internet vandalism."* [15] Either way, the attack proved the Internet's vulnerability. However, it can always be determined whether these DDoS attacks saturated the attacked servers, or saturated the Internet nodes that were associated with those servers. Of course, it has to be realized that, it is impossible to design and build an infinite-capacity network system. Furthermore, it has to be recognized that there is no absolute way to explicitly identify the person or organization behind a cyber attack.

Internet Weaponization

It is not known when the Internet became a weapon of destruction. In most cases, it is practically impossible to absolutely identify the cyber attacker. One can only guess based on the potential recipient of any derived benefits.

However, some of the early weaponizations of the Internet include the notorious *Stuxnet*. It is a powerful malware " *. . . believed to be a jointly built American/Israeli cyberweapon."* [16] that surfaced in 2010, and has been designed to attack programmable industrial controllers that are exposed to the Internet. Another early malware was the *Love Letter*. " *This worm sends itself to email addresses . . . overwrites files on local and remote drives, . . . destroying the original contents.* " [17] It is believed that that world's major powers maintain such cyber weapons arsenal to be launched as the need arises. The US in its sanctions arsenal has a *Cyber-Related Sanctions Program* that spells out the " *. . . cyber-enabled activities subject to sanctions*." [18] There is even a set of Cyber-Related Sanctions Regulations. [19]

The Internet Weaponization activities can be broadly classified as being passive, active or "informative". Where in the passive there is a silent communications monitoring; in the active, data destruction and denial of service; and in the "informative", is " *. . . propaganda which uses social media & news media outlets to disseminate information with the intention of swaying public opinion."* [20]

A well documented example of Internet Weaponization, as a surveillance instrument, is the *PRISM Program*. This is where "*The National Security Agency has obtained direct access to the systems of Google, Facebook, Apple and other US internet giants."* [21] According to Cybersecurity experts "*The only self defense from all of the above is universal encryption. Universal encryption is difficult and expensive, but unfortunately necessary."* [22]

Currently, the number one victim of Internet Weaponization has been the social media, where all kinds of news, fake or otherwise, flood the subscribers. The social media has become a "*battlefield*" where military engagement concepts may equally apply.[23]. In this intense information/misinformation war any weak truth is overshadowed by the powerful lies which demand that the public accept them unquestionably. *"Researchers are still trying to get a clear picture of how many people are influenced by false news and its digital reach."* [24] The consequent question becomes " *. . . what role do ordinary people now play in international conflicts?*" [25]. Ordinary people are merely confused bystanders, who unable to play any role.

The so called social media initially offered their Web platforms as a "community service". Now, that thousands entrusted them and invested in them, having acquired millions of subscribers, the media removed the mask and showed their true self. Credible news delivery organizations, openly declare that "*Social Media is a tool . . .* " of state intelligence agencies [26]. Furthermore, hundreds of social media accounts were closed because they were perceived to having been " *. . . linked to Russia or to Iran.*"[27] In violation oits own rules, Facebook " *. . . removed more than 800 pages* (with millions of followers) *just in time for the 2018 midterm elections."* [28, 29].

There can be numerous examples proving that by now it is beyond the shadow of a doubt that the Internet is two edge sword. On one side, it is a technological platform for bona fide cultural and economic globalization; and on the other, it is weapon in a position to suffocate all those who placed their trust on it, with first victim being the truth.

Internet Localization

For the purpose of this paper, Internet Localization is the concept where data, personal or otherwise, are located in the sovereignty of the user's geographic location, with no external means able to block access or alter them without the user's explicit knowledge and permission.

The present centralization of vast amounts of business and personal data in physical servers located in one country - the United States - poses a paramount twofold danger. One is the lack of contingency plan in the event of a loss due to non-malign causes. The other is that access to those data by their legitimate owners depends on the political/economic relations between the US and of the data owners' country.

In a war environment, whatever is possible to happen must be assumed as equally probable to happen. If the US blocks Internet access from a country where its citizens have entrusted their data to US cyber service providers, the resulting consequences are beyond estimation. A partial defense to such a possible/probable hostile action is Internet Localization. With today's technological options, it makes no sense to have an email account physically located 3,000 miles away, especially if it falls in another country. Neither

does it make sense to have an e-store 3,000 miles away when the addressed market is next door.

Considering that " *the U.S. and UK governments regularly monitor private* (Internet) *communications . . . a number of countries are considering a new type of law called "data localization*." [30]. Such laws would oblige businesses operating on the Internet to hold their data, and those of their clients, inside the territorial sovereignty of the country where the businesses take place, instead of being held in servers located in other countries. "*Vietnam, China, Indonesia, and India have implemented similar laws."* However, *"Brazil implemented but later withdrew data localization, reportedly because of its potential for economic damage."* [31]. It does not take genius to recognize that the withdrawal of the law was under pressure from the international cloud operators.

In Russia, a data localization law requires, that *" . . . all personal data of Russian users to be stored in data centers within the country's borders . . . "* In order to continue doing business in Russia, many companies including " . . . *eBay, Google, and others are in the process or have already moved user data in-country."* Furthermore, *" . . . eBay is transferring data from Switzerland to Russia."* [31].

Economists estimate that the application of data localization laws will cost the US cloud computing industry about US$60 billions per year. With data localization, this amount not only will become a revenue for the respective local economies, but it will also increase local cyber skills and employment. Data localization in no way does it alter the Internet's concept of globalization.

In conclusion, the Internet Localization issue is mainly a state security issue with the economic aspects coming next, and it provides only a partial defense against the increasing Internet Weaponization.

REFERENCES (Valid on October 12, 2018)

[1] Who owns the Internet?
https://www.weforum.org/agenda/2016/08/who-owns-the-internet-and-who-should-control-it
[2] Internet Corporation for Assigned Names and Numbers
http://www.icann.org
[3] Wikipedia on ICANN
https://en.wikipedia.org/wiki/ICANN
[4] Internet Major Nodes Map
https://www.internetexchangemap.com
[5] Global Commission on Internet Governance – Report Volume 6
https://www.cigionline.org/sites/default/files/documents/GCIG%20Volume%206web.pdf
[6] US Department of the Treasury – Sanctions Program
https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx
[7] ***Effects of the Internet on politics: Research roundup*** by John Wihbey
https://journalistsresource.org/studies/politics/citizen-action/research-internet-effects-politics-key-studies
[8] *The Rise and Fall of Social Media in American Politics (And How it May Rise Again)*
http://techpresident.com/news/23103/rise-and-fall-social-media-american-politics-and-how-it-may-rise-again
[9] **Measuring the reach of "fake news" and online disinformation in Europe by Richard Fletcher et al.**
https://reutersinstitute.politics.ox.ac.uk/our-research/measuring-reach-fake-news-and-online-disinformation-europe
[10] Living in Digital Darkness: A Handbook on Internet Shutdowns in India by SFLC.in
https://sflc.in/sites/default/files/reports/Living%20in%20Digital%20Darkness%20-%20A%20Handbook%20on%20Internet%20Shutdowns%20in%20India%2c%20May%202018%20-%20by%20SFLCin.pdf
[11] Internet Shutdowns in India
https://internetshutdowns.in/
[12] Algeria and Iraq shut Internet to prevent exam cheating
https://www.aljazeera.com/news/2018/06/algeria-iraq-shut-internet-prevent-exam-cheating-180621074343644.html

[13] Egypt Shuts Down Internet, Cellphone Services
https://www.wsj.com/articles/SB10001424052748703956604576110453371369740
[14] Russia cuts off internet in Crimea
https://www.buzzfeednews.com/article/hayesbrown/russia-cut-off-the-internet-in-crimea
[15] Who Shut Down the Internet Friday? By Robert Windrem et al.
https://www.nbcnews.com/news/us-news/who-shut-down-u-s-internet-friday-n671011
[16] Stuxnet
https://en.wikipedia.org/wiki/Stuxnet
[17] The Love Letter Malware
https://www.symantec.com/security-center/writeup/2000-121815-2258-99?tabid=2
[18] Cyber Related Sanctions Program
https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber.pdf
[19] Cyber Related Sanctions Regulations
https://www.ecfr.gov/cgi-bin/text-idx?SID=41f7a6c1c344bde4b08d2667df8dbf1d&mc=true&node=pt31.3.578&rgn=div5
[20] The Weaponization of the Internet: Options & Tactics for States
https://medium.com/@jessesandoval/the-weaponization-of-the-internet-options-tactics-for-states-2686df1b776c
[21] NSA PRISM Program
https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
[22] Our Government has Weaponized the Internet
https://securityintelligence.com/the-weaponization-of-iot-rise-of-the-thingbots/
[23] Thomas Nissen: The Weaponization of Social Media
https://www.stratcomcoe.org/thomas-nissen-weaponization-social-media
[24] ***What research says about how bad information spreads online*** by *Denise-Marie Ordway*
https://journalistsresource.org/studies/society/news-media/fake-news-bad-information-online-research
[25] LikeWarBook: The Weaponization of Social Media
https://www.likewarbook.com
[26] ***CBS News: Social Media is a Tool of the CIA***
https://www.cbsnews.com/news/social-media-is-a-tool-of-the-cia-seriously/
[27] ***Facebook-shuts-652-accounts-linked-Russia-Iran***
https://www.dailymail.co.uk/news/article-6085555/Facebook-shuts-652-accounts-linked-Russia-Iran.html
[28] Facebook purges accounts
https://www.rt.com/usa/441140-facebook-purge-victims-speak/
[29] ***Facebook Deletes Accounts***
https://www.rt.com/usa/441040-facebook-deplatforms-political-pages/
[30] Will Data Localization Kill the Internet? by Peter S. Vogel
https://www.ecommercetimes.com/story/79946.html
[31] Firms Rethink Russian Data Center Strategy, as Data Sovereignty Law Nears Activation
https://www.datacenterknowledge.com/archives/2015/07/21/russian-data-localization-law-spurs-data-center-strategy-changes/