Technologies to support, enhance and protect social networking freedoms during periods of social unrest and political disruption

Martin Dudziak, PhD [1,2]

Keywords: social network, security, encryption, wireless, continuity, integrity, disruption, politics, intrusion, freedom

Abstract
We address the topic of internet and communications integrity and continuity during times of social unrest and disturbance where a variety of actions can lead to short-term or long-term disruption of conventional, public and private internet and wireless networks. The internet disruptions connected with WikiLeaks in 2010, those in Egypt and Libya during protests and revolution commencing in January of 2011, and long-standing controls upon internet access and content imposed within China and other nations, are considered as specific and contemporary examples. We examine alternatives that have been proposed by which large numbers of individuals can maintain "connectivity without borders." We review the strengths and weaknesses of such alternatives, the countermeasures that can be employed against such connectivity, and a number of innovative measures that can be used to overcome such countermeasures.

Introduction and Some History

Less than a generation ago, even well into the 1980's, the internet was a relatively rarely used means of communication among people. Access was for the most part unrestricted because the internet was mainly a vehicle for exchange of academic and corporate data among relatively small and isolated populations. Many nations had virtually no access because of the slow pace and the high costs of telecommunication system development, and even within the USA and Western Europe, using the internet for email, much less anything more complex such as videoconferencing and group collaboration, was not a commonplace practice except for those isolated population groups who were not only "computer literate" but serious "aficionados." Figure 1 below provides an illustration, based upon the growth of internet hosts of the situation leading up to and including the very earliest years after the invention of the World Wide Web (WWW) at CERN in the early 1990's. Figure 2 compares internet usage growth, along with population growth, in the decade 2000 – 2010, during which social networking and mobile telephony and wi-fi usage alike came to be a global and ubiquitous experience.

Electronic communication in the pre-Web era was generally limited to text messaging and the transmission of files via ftp. Simply put, things were not as convenient and easy, and certainly the use of audio and video was a virtual impossibility for the vast majority of people in almost all parts of the world. Reflect upon the now-antiquated steps that would have been required to do something as simple as to make a video clip of a public scene (e.g., the Hudson River emergency landing of USAIR Flight 1543 on Jan. 15, 2009 [3] or a scene from Tahrir Square in Cairo in late January during the height of the populist protests and revolution) and to send that clip to even one single recipient, much less to make it available upon demand for millions worldwide. First, using a videocamera operating with a tape. Then doing a tedious conversion process to convert that video footage into digital format and get it into a file on a computer workstation or personal computer.

[1] Member of Graduate Faculty, Stratford University, Richmond, Virginia http://stratford.edu
[2] Scientific Director, CIBI (Center for Integrating Biosustainability Innovations) http://cibi.tetradyngroup.com
[3] The first reports and photos of the airliner crash-landing in the Hudson River were made by Janis Krums, a traveler on a nearby passenger ferry, using his iPhone camera. http://articles.nydailynews.com/2009-01-15/local/17914601_1_airways-crash-plane-users

Next, or perhaps before the digitization and transfer, performing the edits necessary to have a completed "clip." Next, having the proper software and the bandwidth for transmitting a very large file over the internet, at a time when 28k and 56k were for many considered to be "fast" speeds. Finally, having recipients able to view this sort of data. Working with medical images (MRI, X-ray, CT) and very short ultrasound video clips even in 1995-1996, in order to manage bidirectional exchanges in near-real-time between users from the USA, Latin America, Russia and areas in the Balkans, Caucasus and Himalaya, was extremely tedious and full of delays, lost packets, and additional exchanges by phone in order to synchronize and coordinate online exchanges and conference meetings. [4]

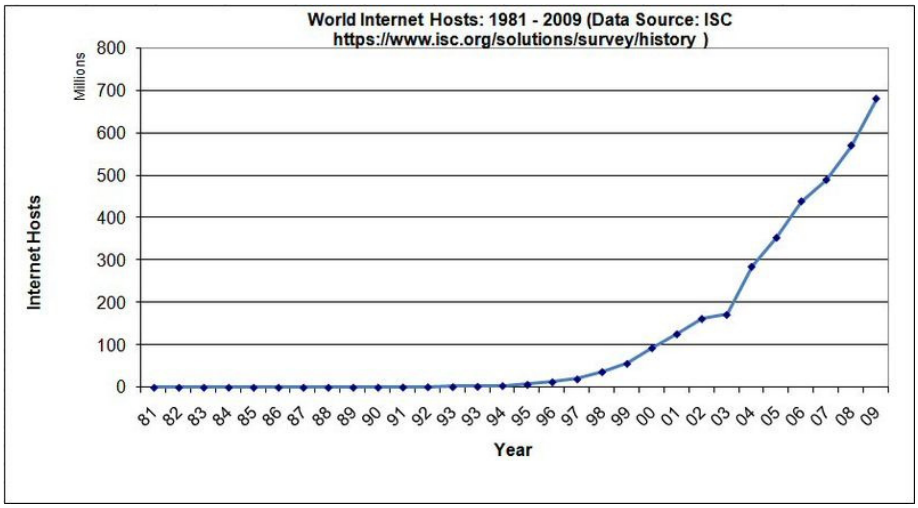


Figure 1

WORLD INTERNET USAGE AND POPULATION STATISTICS

World Regions	Population (2010 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2010	Users % of Table
Africa	1,013,779,050	4,514,400	110,931,700	10.9 %	2,357.3 %	5.6 %
Asia	3,834,792,852	114,304,000	825,094,396	21.5 %	621.8 %	42.0 %
Europe	813,319,511	105,096,093	475,069,448	58.4 %	352.0 %	24.2 %
Middle East	212,336,924	3,284,800	63,240,946	29.8 %	1,825.3 %	3.2 %
North America	344,124,450	108,096,800	266,224,500	77.4 %	146.3 %	13.5 %
Latin America/Caribbean	592,556,972	18,068,919	204,689,836	34.5 %	1,032.8 %	10.4 %
Oceania / Australia	34,700,201	7,620,480	21,263,990	61.3 %	179.0 %	1.1 %
WORLD TOTAL	6,845,609,960	360,985,492	1,966,514,816	28.7 %	444.8 %	100.0 %

NOTES: (1) Internet Usage and World Population Statistics are for June 30, 2010. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the US Census Bureau . (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, local Regulators and other reliable sources. (5) For definitions, disclaimer, and navigation help, please refer to the Site Surfing Guide. (6) Information in this site may be cited, giving the due credit to www.internetworldstats.com. Copyright © 2000 - 2010, Miniwatts Marketing Group. All rights reserved worldwide.

[source: http://www.internetworldstats.com/stats.htm]

Figure 2

With the introduction of the Web into the general mainstream of internet usage and the release of several browsers (Mozilla, Netscape, Internet Explorer, Opera, plus others), the Web as a medium of exchanging information began to reshape the ways that the general population thought and acted

[4] cf. Dudziak [1], Dudziak [2]

about finding information, publishing data, conducting dialogs and discussions, doing business, and conducting politics and the governance of society. While a number of visionaries and pioneers saw from early-on the opportunities and the directions in which technology and social behavior would progress, it seems unlikely that anyone could have predicted the scope at which mass information exchange and dialog would develop, to such levels and details as have been witnessed in recent years and particularly in events throughout the world in 2010 and 2011. One can point a virtual "telescope" at almost any part of the globe and find remarkable instances of where large and seemingly disparate groups of people have been brought together on issues ranging from humanitarian relief to political upheaval, reform and revolution. This is not only a change in communication methods – it is a change in how people think and act about social issues and especially "ECE" type events – Emergent Critical Events, including all types of response to such events. Here, for instance, is one brief list of some that occurred over the past six years:

- The Indian Ocean earthquake and tsunami (2004)
- Hurricane Katrina (2005)
- Chile mine disaster and rescue (2010)
- China earthquake – Sichuan region (2008)
- China unrest and upheavals in Xinjiang and Tibet (throughout)
- Ivory Coast and Sierra Leone (throughout)
- Darfur and Ethiopia (throughout)
- Tunisia - Egypt – Yemen – Iran - Jordan – Syria – Libya (2010—present)
- The Japan earthquake, tsunami and nuclear disaster (2011 and continuing)

Present society has transformed into where there are expectations and dependencies for information linked with disruptive events. If a government or other organization wants to disrupt the ways that people can respond, as civilians, not as organized military organizations but as masses of adults and children, then the way to do such disruption is in the social media. The dependencies enable those who would aspire to limit open peer-to-peer and broadcast communications alike among civilian populations by providing such control-seekers with vulnerability points, namely the means to curtail the internet and cellular networks. Figures 3 and 4 below illustrate the significant growth in these communications, and thereby the dependencies of populations upon these channels.

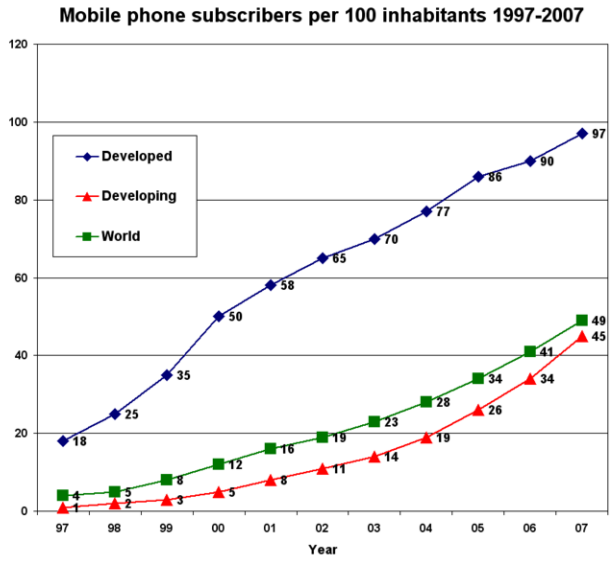


Figure 3 - [source: ITU (http://www.itu.int/ITU-D/ict/statistics/ict/graphs/mobile.jpg)]

	United States	Europe	Japan
Used connected media (browser, app or download)	46.7%	41.1%	76.8%
Used browser	36.4%	28.8%	55.4%
Used application	34.4%	28.0%	53.3%
Used messaging			
Sent text message	68.0%	82.7%	41.6%
Instant messaging	17.2%	14.2%	3.6%
Email	30.5%	22.2%	57.1%
Accessed entertainment/social media			
Took photos	52.4%	57.5%	62.9%
Social networking or blog	24.7%	18.0%	19.3%
Played games	23.2%	25.3%	16.3%
Recorded video	20.2%	26.1%	15.8%
Listened to music	15.7%	25.0%	12.9%
Watched TV and/or video	5.6%	5.7%	22.8%
Accessed financial services			
Bank accounts	11.4%	8.0%	7.0%
Financial news or stock quotes	10.2%	8.0%	16.5%
Accessed news, sports, weather, search, retail, travel, reference			
News and information	39.5%	32.2%	57.6%
Weather reports	25.2%	16.4%	34.7%
Search	21.4%	14.9%	31.5%
Maps	17.8%	13.0%	17.1%
Sports news	15.8%	12.0%	18.2%
Restaurant info	10.0%	6.5%	9.7%
Traffic reports	8.4%	7.4%	14.0%
Retail site	6.5%	5.2%	8.5%
Classifieds	7.3%	4.8%	3.6%
Travel service	4.4%	4.6%	2.9%
Source: comScore MobiLens (Feb 2011)		**via:** mobiThinking	

Figure 4

The Growth of Social Networking and its Natural Disposition for Politicking

Social networking has, of course, existed as long as there have been human beings. However, the term, "social network," in the context of the internet, became popular first in the early years of this 21st century as a description of an emergence, on an qualitatively "exponential" scale, of people using the internet to communicate with friends, acquaintances, and total strangers, on a myriad of subjects of common interest. Before the web, there were "newsgroups" along with traditional email. As the web grew in terms of availability, usage, speed, and types of applications, there emerged blogging – "web logging" as the original term – and this suddenly afforded millions of people the opportunity to "have their say" about any and all subjects, to be an instant author, to potentially gather together a regular and even supportive audience of readers and respondents. Still, the older protocol and style of communication tended to prevail:

"June" writes something – a blog or a web page or an entire website – and she makes it available and promotes it to the Many. Some of the Many respond, and potentially this starts a dialog and

also gathers more people into being readers. Suddenly "June" has a WebMD or any of a huge variety of sites with a lot of activity, a lot of visits and posts, and many of these progressed to become successful businesses because of the attraction of such websites to advertisers. A plethora of such sites developed, along with the software for sustaining such user communities and their activities. Open Net, based upon the OpenStream architecture and OSML (Open Stream Markup Language) was one early development that provided, in applications such as *vMessaging* and *ePresents*, the basics of the kind of social networking environments that one finds today in YouTube, FaceBook, and other environments.

The years 1998 through early 2001 were a time when "dot com" was all the rage in the world of emerging new businesses, startups financed by cash-rich venture capitalists and small investors wanting to play at the VC game. However, this was not a time when society, anywhere on the planet, was ready, ripe, and poised for the emergence of a mentality, a psychology, a "group think" that is the grounding for social networking of today. Facebook and GroupOn could not have started in the 1990's or in the first years of the 21st century. Many things not yet in place, not ready, socially. Not enough people were actively using the internet and web-based applications or facilities. Speed and bandwidth were still lacking, particularly for the widespread use of exchanging high volumes of images and especially audio and video clips. Large numbers of people simply did not have broadband access or access of any sort. Mobile devices were widely used in some parts of the world but they were not yet universal, and email/web access for mobile phones was still a comparatively new thing. Texting did not "catch on" in a major way until later in this first decade of the 21st century, and now it is commonly viewed as a principal means of messaging especially among youth. Most of all, people were simply not ready and this is offered as one of the factors that curtailed earlier forms of social uprising and "self-organization" among large and disparate, geographically-separated population groups.

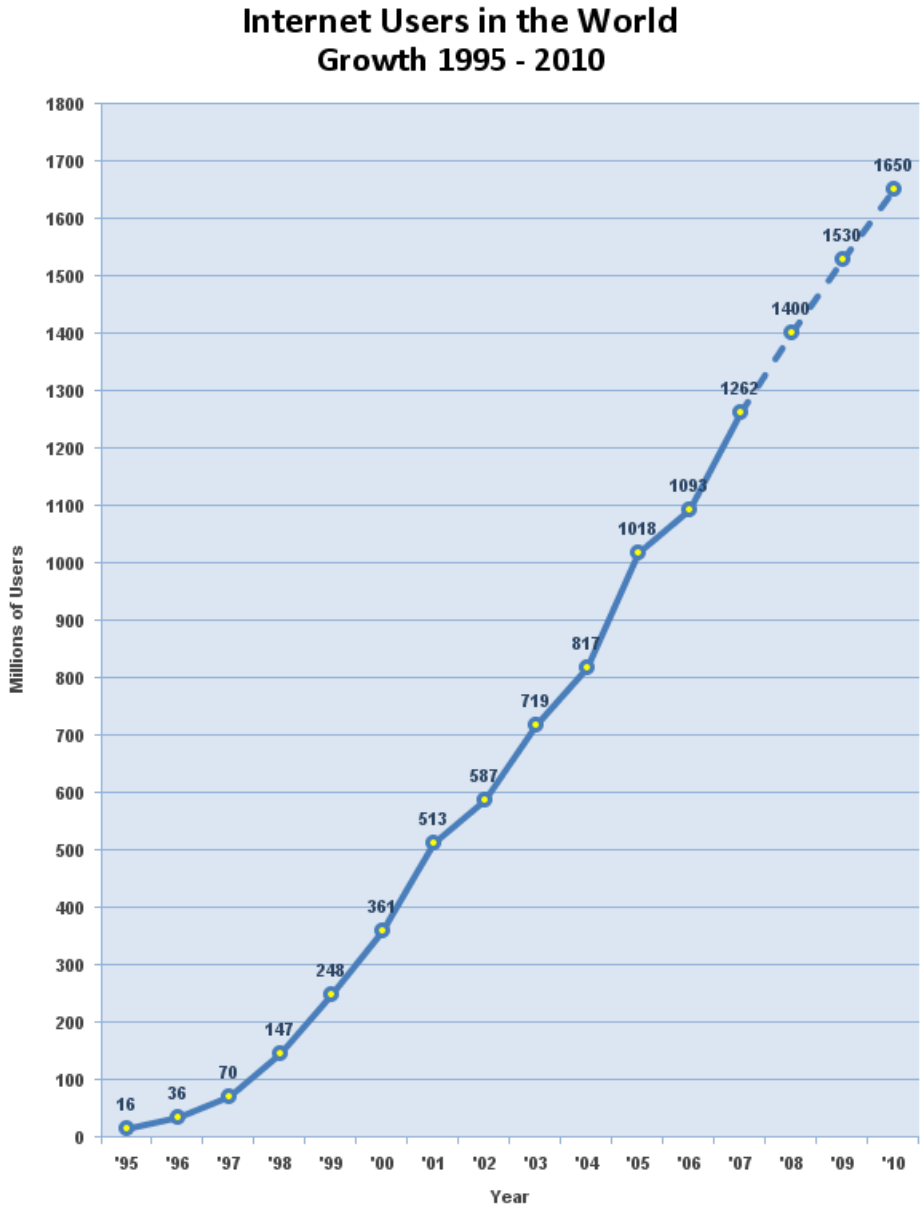
(R)Evolution via Social Networking

It is only natural, a "fait accompli" in advance, that when there is a substrate in place, namely a base of social networking communities such as Facebook, YouTube, MySpace, LinkedIn, and specialty interest groups, then there is a matrix that will support faster introductions into new, previously "virgin" populations. When the means to implement "yet another" social network website is easily accomplished through easy-to-use open-source software, generally free without cost, then there follows a growth of activity among people who previously would not be so likely to venture into "trying out something new." When sufficiently large numbers of that social network are sharing with others in that network that they are dealing with common problems, issues, fears, and challenges in life, including political repression and the suppression of free speech and self-determination, then more people begin to reflect upon their own situations and many of them become emboldened to speak out, to share, and to sharpen their rhetoric into swords and spears of social change.

We have seen this particularly in the time since Sept., 2008 within not only the USA but worldwide, following the "meltdown" of the capital markets and in particular the massive problems with consumer real estate and general (un)employment. We witnessed a particular and slightly different, or mixed, massive surge of social network activity including the formation of many organizations, following the DeepWater Horizon Oil Spill Disaster in the Gulf of Mexico (April, 2010 and for months thereafter). [5] However, nowhere has there been such a comprehensive, organized, and sustained use of social networking for political purchases than in American politics

[5] The problems are definitely not resolved even to this day (March, 2011) but the most intensive social networking activity began to subside after the BP DeepWater Horizon wellhead was finally capped in July, 2010.

commencing with the 2008 US presidential election and even more intensively and energetically, with the rise of the conservative Tea Party movement in 2009 and thereafter. This paved the way for broader use in political events worldwide, such as with the WikiLeaks disclosures of 2010 and throughout the Middle East in early 2011 and continuing presently. The medium (internet and mobile phone nets) became the tool of choice for activating large numbers of people for "social causes." Figure 5 shows the growth of internet users worldwide and figure 6 the particular growth of Facebook usage. Both of these illustrate the rise in usage that has lent itself to a comfort level and dependency which in turn can be pinpointed and exploited by forces wanting to curtail the exchange of ideas and the planning of public events.



Source: www.internetworldstats.com - January, 2008

Figure 5

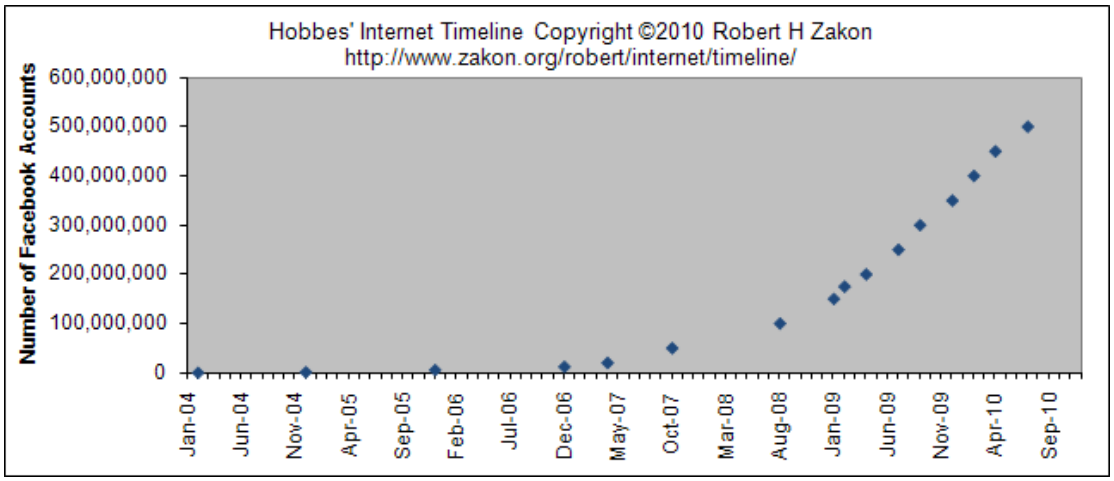


Figure 6

Closing the Gates and Building Walls

When increasingly large numbers of people gather together, for any reason, it is typical for governments and political rulers to become concerned, especially if those governments feel that they have some reasons to fear what those people may do. In the past, it took a great deal of effort and organization to get hundreds and even thousands of people together into one public area, much less to channel those minds and their energies into doing any particular, focused activity, such as to march or boycott or to occupy a building or square and demand Change from an unresponsive government. That planning and preparation was something that could not help but to noticed, monitored, and even repressed, nipped in the bud and stopped by any number of countermeasures, such as arresting the organizers and the first attendees to some type of event. Reflect upon marches and gatherings in many countries around the world during the 20th century. There was plenty of time for governments and opposition "camps" to make counter-preparations.

However, through the use of the internet, vast numbers of people can be reached in seconds, minutes, hours. The ability to spread information - including "worth a thousand word" type pictures and video clips - is at the fingertips of anyone today who has a cell phone with a camera plus internet access. Kiosk posters are replaced by Twitter and Facebook posts. Stemming this type of easy and fast broadcasting and networking then becomes critical for those who want to maintain a repressive regime, anywhere. Too many people can be activated, too much can happen in a shorter period of time, than the typical regime can manage to handle with traditional countermeasures – at least that can be and has been demonstrated to be the viewpoint in recent years and especially in recent months.

Thus, "cutting the cable" becomes a major countermeasure weapon for those who want to control and suppress open communications among people, and who aim to allow only a particular type of information to reach the public, namely, some type of "party line" dogma. This cutting may involve censorship of data traffic, as has been conducted by several governments including those of China and Iran, or it may involve the physical shutting down of internet and cellular services such as occurred in Egypt and Libya in 2011, in Burma (2007), Nepal (2005), and as have been alleged in several other countries. A third form of repression of information exchange can be found in various reactions to the WikiLeaks disclosures in late 2010, whereby services including financial transaction processing were denied to different parties by various corporations.

Our main interest is in considering the alternative measures that can be taken by people, as individuals and as groups, to ensure continuity in communications via internet (land-line and

wireless) and mobile telephony, so that freedom of expression among people can be sustained without interference by government agencies or freelance agents employed by politically-focused groups. It is a given that repressive regimes, just like hackers, will do everything possible that they can achieve in order to disrupt the ability of people to connect and share opinions, emotions, intentions, wishes and most of all, concrete plans. Our claim is that by avoiding centralized and fixed architectures, by sacrificing many qualities such as speed, bandwidth, durability, and even constant reliability, it is possible to avoid having a society cut off from the rest of the world and from within itself. The key, we argue, is to not provide the "Other Side" with easily identifiable, reliable, fixed, constant targets. If someone cannot see the target, that someone cannot aim the gun, and valuable resources in a time of conflict will be consumed by that opposition force in trying to identify where are the targets that should be hit.

There are two "standard" ways in which such shutdowns can occur. Focusing upon the internet, all of the routers which direct traffic over a state's border can be shut down, thereby "hermetically sealing" the country from outside traffic. Alternatively, the operation can be performed within a state, further down the chain, by switching off those routers located at individual ISPs in order to prevent access for most users dependent upon those ISPs. Consider briefly here a few observations made regarding the internet shutdown in Egypt in January, 2011, beginning on 28.January and leaving only a handful of connections (e.g., the stock exchange) with connectivity outside the country.

There have been multiple reports of blockades against specific service providers such as Twitter and Facebook. However, when the cutoff began in Egypt, it came on strong and fast. Renesys, an internet monitoring body, indicates major shutdowns across all providers (ISP) just shortly after midnight. This type of "sweep" most certainly required advance planning. It was premeditated, and it had a dual focus: keep people from getting "out" to the rest of the world (with text and especially photos and video), and keep the world from getting "in". Both DNS level and Border Gateway Protocol shutoffs were employed, creating a firm lock-down for internet traffic through regular ISP-based pathways inside the country and blocking rerouting to get in and out of country.

There is an important social-psychological dimension to our era of dependence and security upon having broad-reaching, open connectivity. More and more people have come to look upon the internet, and social networks like Facebook and Twitter in particular, for some of the security that gets them through the days and weeks and months of distress, anxiety, and trauma stemming from personal, economic, environmental, and political disturbance. We can see this in the upsurges of activity during some crisis and trauma times, such as the 2008 Sichuan earthquake in China, the 2010 DeepWater Horizon Oil Spill, the 2011 Japan earthquake and tsunami.

Immediately following the March 2011 Japan quake, Tweets from the Tokyo region alone were averaging over 1,200 per minute, as reported in a Wall Street Journal article by Andrew Royce.[6] Figures 7 and 8 below provide some perspective on both the annual increase in general Twitter activity, and usage trends during the January-February 2011 period of crises in Tunisia, Yemen and Egypt.

Paul Ziolo, in a seminal paper, *Trauma and Transcendence: Psychosocial Impacts of Cybernetics and Nanotechnology*, [7] writes pointedly about the "imminent wave of so-called GRAIN technologies - Genetics, Robotics, Artificial Intelligence and Nanotechnology" and this wave's influence, including through what is enabled in contemporary microelectronics and global

[6] http://online.wsj.com/article/SB10001424052748703597804576194100479604290.html
[7] Ziolo [1]

communication network technologies, upon how "social and political infrastructures are adapted and transformed, society reaches a psychological compromise with these reformed structures and the lifestyles they give rise to, and products developed from the innovation cycle finally reach market saturation point." Ziolo raises challenging, provocative and important questions about potential collective trauma and even widespread falling-domino style cultural collapse.

> "Psychohistorical studies show that cultural collapse occurs when the level of complexity attained by that culture exceeds the capacity of its group and psychoclass structures to contain primordial anxieties within the collusionally-defensive construct upon which that culture was built. Group and psychoclass boundaries disintegrate and collapse, leading to paranoid-schizoid regression and a destructive internal conflict - the 'axial conflict'. After this conflict, existing cultural capital is utilised to create a 'universal state', an imperialistic structure maintained through increasing totalitarian control, during which anxieties are contained, not by defensive strategies constructed from ideational systems, but by increasing emotional investment (catharsis) in materialistic expansion and in ultimately futile efforts to dominate and control that civilisation's outmoded resource base through a parallel investment in even greater administrative complexity." [8]

Ziolo's queries can be redirected at the world's increasing dependence upon "instant" and "global" communications – and of course the effects from any element in society, such as a totalitarian government, manipulating and constricting, even cutting off, such communications in order to establish severe and absolutist dominance and control. That the internet and cellular networks can be shut off suddenly, across a nation or several nations, is something that affects much more than the ability of people in that nation or region to organize for demonstrations and political actions. This potency can affect the very fundamental fabric of daily life and bring about chaotic disruptions and upheavals that go beyond the scope of what may be in any organization's or community's plans of action, practical intentions or psychological expectations.

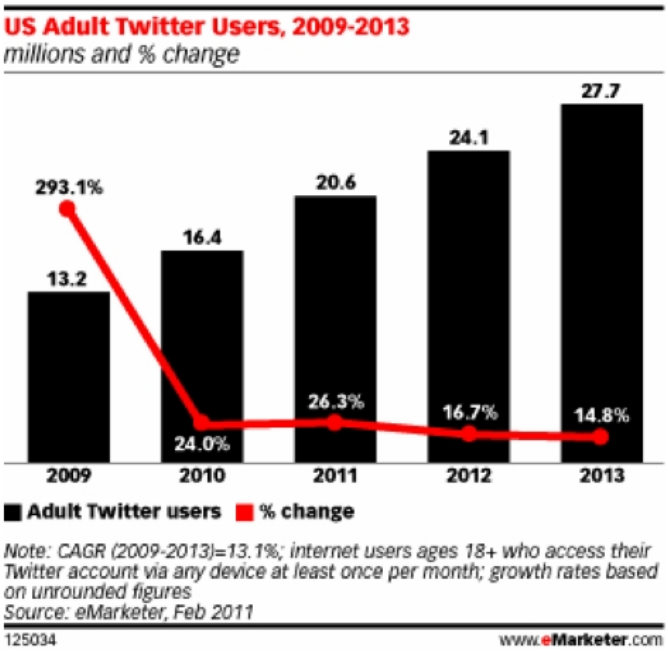


Figure 7

[8] Ziolo [1], page 5 of 7.

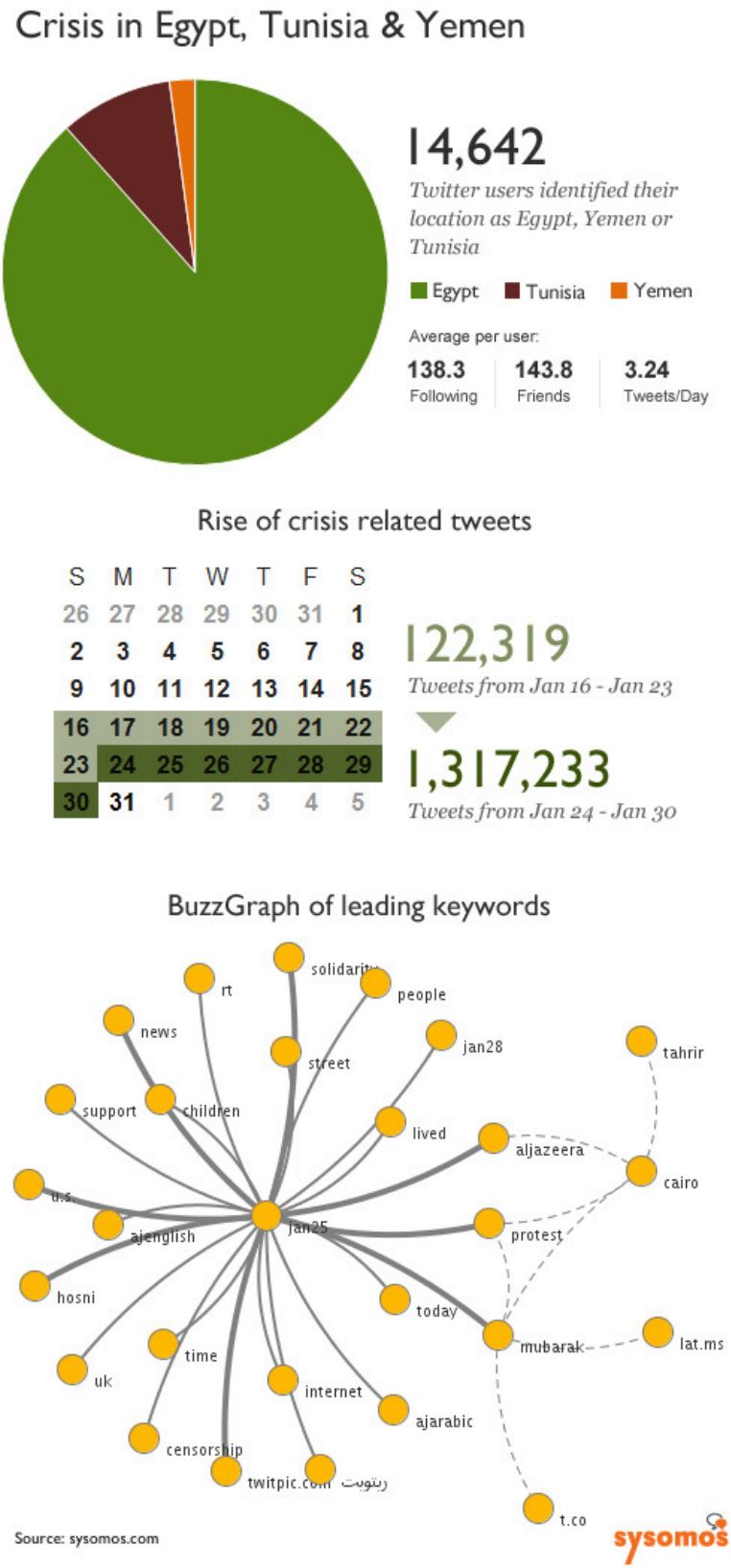

Crisis in Egypt, Tunisia & Yemen
14,642
Twitter users identified their location as Egypt, Yemen or Tunisia
Egypt
Tunisia
Yemen
Average per user:
138.3
Following
143.8
Friends
3.24
Tweets/Day
Rise of crisis related tweets
S M T W T F S
26 27 28 29 30 31 1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
30 31 1 2 3 4 5
122,319
Tweets from Jan 16 - Jan 23
1,317,233
Tweets from Jan 24 - Jan 30
BuzzGraph of leading keywords
rt
solidarity
people
news
street
jan28
tahrir
support
children
lived
aljazeera
cairo
uk
ajenglish
jan25
protest
hosni
today
mubarak
lat.ms
time
uk
internet
ajarabic
censorship
twitpic.com
t.co
Source: sysomos.com
sysomos

Figure 8

"Connectivity without Borders" – viable alternatives to when someone "pulls the plug"

The all-important pragmatic question now arises. What can be done to overcome when, for instance, a Mubarek or Gaddafi or any one regime (force, cartel) shuts down the main connective links between a region or country and the rest of the world? How can people quickly, and in large numbers, get around the blockages, so that functionally the desired and bidirectional communications can occur? How can things be done in ad hoc manners, without requiring a massive distribution of information (that would require precisely what has been cut off, namely internet and phones), or different hardware (no time, no money, no physical means to do so undetected and undisturbed), or different training (it is one thing for masses of people to quickly adapt to a new web-based protocol or a new cell phone app; it is too much to expect large numbers of non-technical people to suddenly learn about short-wave radio transceiver operations.

There are many alternatives being developed and explored by which people can maintain the basic social networking connectivity and throughput that exists in most countries today, during periods when the usual connectivity, via the usual internet, may be subject to attack by forces wishing to prevent public access and communications. It is hardly possible in one paper to cover or do justice to all of the viable alternatives. However, a few stand out for discussion and analysis here. The objective is to present a few that are most active, and appearing to be most promising, for use in today's climate of technology, knowledge, and resources by large numbers of people in many different countries. Some alternatives are simply not practical for many parts of the world, and for the types of equipment that can be expected to be available. Three approaches stand out, and they are not exclusive of one another. Indeed, a fundamental position argued within this paper is that there must, necessarily, be a multiplicity of communication methods linked together, integrated, in order to prevent blockages and shutdowns. This is a matter of thinking, designing, and acting by principles of Fault Tolerance and Fail-Safe. There is also another element of practice and skill that may be best described by the idiom, "learning to [fly, drive, act] by the seat of one's pants." In other words, learning by jumping into the situation and Doing, which means making mistakes, snafus, and setbacks, but with enough people and enough attempts, eventually things stat working out more correctly than not.

Six approaches are mentioned here, of which the first three are seen as the most practical and safe, from both technical and political perspectives, for most societies and this includes in both G8 well-developed economies as well as G20 and "Gxx" (almost all other) countries. these are actually not six disparate approaches but they are complementary and can – and probably must – work together. Mix-and-match, and hybridization, in building and keeping an ad hoc network "alive" does make for problems, mistakes, breakdowns, miscommunications and other slip-ups, but it also opens up pathways for work-arounds, for avoiding and getting past the roadblocks that have been and will continue to be put up by those who want to deny and prevent free speech and open communication.

The six are listed here and then described very briefly in the paragraphs that follow. Thereafter, the benefit of "hybridization" and "blending" of certain features from the first three are considered for situations such as where there is a paucity of resources, including time and technical equipment, compounded by direct adverse operations from a hostile force.

- **Point-to-Point Ad Hoc "MESH" wireless networks**
- **Short-wave radio-based networks and burst-broadcasts linked with other nets**
- **Mobile Ad Hoc Cellular and Wi-Fi Networks**
- Hybrid "Rim" Networks
- Adaptive Encryption Strategies
- "Sticks and Stones" Networking

These six are by no means the only that have surfaced as suggestions and some of which others have had some experimentation in recent months and years. Among the wide-ranging list of other suggestions, some of which are truly "interesting," to say the least, are these as a selection:

- A return to FIDONET type mini-networks and the use of older bulletin-board protocols from the 1980's and earlier. Essentially these approaches fit under the category of "assuming there is no problem with land-based phone lines, one could go back to 28k and even 8k or lower transmission rates for the simplest of packet-based messaging. However, in many parts of the world, there is no reliability or wide-scale distribution of such lines, and the majority of people do not have the 'antique" equipment for doing such slower, older communications.
- Operating outside the customary and regulated frequency spectra, especially in ranges > 10 GHz; obviously there are severe issues of equipment and power for such undertakings, not to mention that operations will still be detected and result in countermeasures that can be severely dangerous to the well-being of the network operators
- Establishing "line of sight" communications by using the equivalent of ancient "mountain-top beacon" systems, or by means of vessels offshore that are carrying satellite uplinks. Infrared lasers linking with boats 10 miles offshore could be hard to detect. However, once again, power and equipment technology become extraordinary disablers for such methods, especially thinking in terms of reliability, security, weather issues, and technical skillsets in operating the equipment.
- Using UAV drones consisting of instrumentation suspended from balloons, equipped with long-duration batteries or solar power units, plus altimeter, wireless, GPS, and directional laser communications. Operationally, each unit would "find" the altitude and GPS coordinates of another "laser link drone" and automatically aim the communication laser in order to establish line-of-sight laser communications for long-distance network link-ups. It is obvious how fast this kind of architecture becomes complex beyond practicality for the general purposes in which restored and fault-tolerant basic communications are needed.
- USB flash drives carried by drone aircraft or carrier pigeon – one of the more "original" ideas indeed! With a network of very small remote controlled "hobby" aircraft and helicopters, this is theoretically conceivable, but immediately there is a plethora of problems about equipment access, operational skills, weather issues, and coordination at the sending and receiving ends. As with many similar suggestions, these are not the kind of answers that will work for 90%+ of the people and environments.
- Re-use and refurbishing of older technologies, combined with today's easy-to-use web/phone application development software (especially for the GUIs). Mentioned and promoted by various individuals and groups have been nearly everything under the sun: GSM phone sets, satellite dishes, a DIY packet radio uplink kit, a one-click install for installing a Fidonet node on an older laptop with a modem, modified Open Source PGP software to convert netbooks and smartphones into encrypted communication devices, cell mini-towers that can be placed in a variety of settings and rapidly disassembled and moved about, and "pirate cell tower" which can be used to re-enable SMS communications on conventional handsets when a government deactivates mobile service.

It is obvious that the "World" has been thinking about this and that there are many minds speculating about all sorts of alternatives. It is also clear that most of the above are not seriously practical or in some cases feasible even without the concern of interference, disabling, seizure, and destruction by whatever organization or faction wants to prevent popular, open communications.

So now, a few remarks about some methods that can have promise and how they may be implemented and also work in tandem together.

Point-to-Point Ad Hoc "MESH" wireless networks

MESH networks are classical structures and not at all new. They have been employed for decades in MIMD-type parallel processing machines[9] before wireless communications became widespread. Each node has the tasks of capturing and disseminating its own data, but in addition each node serves as a *relay* for other nodes, upon demand. Nodes must collaborate in order to propagate the data in the network. Some of the nodes of the network are connected to more than one other node in the network with a point-to-point link, thereby making it possible to take advantage of redundancy provided by a what would be in a fully connected mesh topology but without the expense and complexity required for such a total-connection network. The data transmitted between nodes in the network will travel along the shortest or nearly shortest path between nodes. The exception is when there is a break in one of the links between nodes. In such a case the data takes an alternative path to the destination, even though it may be significantly longer. How that alternative is determined rests in the routing algorithm that selects what new path to follow at any particular time. Figure 9 provides an illustration of three forms of mesh networks showing a variety of multiple and redundant paths among nodes. [10]

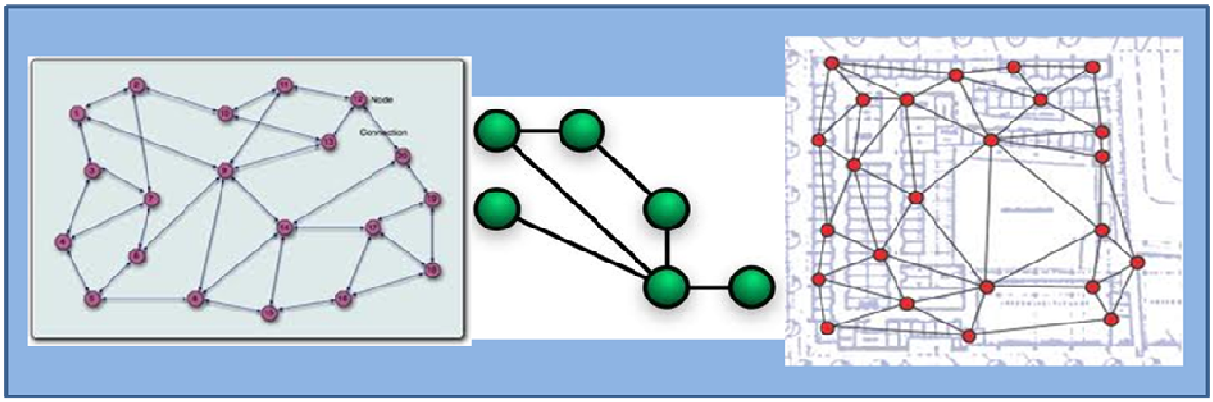


Figure 9

A Mobile Ad-Hoc Network (MANET) is a further evolution of the MESH architecture and is discussed further below. One of the strong points of a MESH approach, even in a very classical and non-mobile configuration, is the ability to introduce redundancy and fault-tolerance. However, one of the weaknesses is in the dependence upon fixed locations, power sources, risk of detection and prevention of functionality, and the major dependence upon maintaining the basic architecture during a period of time when certain critical nodes and links may become inaccessible due to political and social strife.

One alternative that can be considered is the employment of highly directional 802.11 antennas (shotgun or yagi) which can themselves be physically disguised or semi-mobile, such as with movement from one building (rooftop) to another. If such antennae have minimal side lobe bleed, they may be indistinguishable from typical AP background levels and thus less detectable. It may

[9] MIMD = Multiple Instruction, Multiple Data, as with the INMOS transputer family (T4xx, T800, T1000) from the 1980's and 1990's.

[10] cf. also the design of OpenWRT Wireless "Battle Mesh" for ad hoc collaborative meetings: http://battlemesh.org/BattleMeshV4

be possible to obtain 2 - 10 km of connectivity from such a link. It has been suggested that a few dozen such links could serve to criss-cross and provide connectivity for a large, spread-out metropolis such as Cairo.

Short-wave radio-based networks and burst-broadcasts linked with other nets

Although short-wave packet radio has been in practice for decades and is often suggested as the possible backbone for non-disruptable, or at least more resilient and tamperproof social communications, there are limitations because of technology, training, cost, sensitivity, and the risks for countermeasures by a hostile force. The Packet Radio AKA AX25 exists as a network that spans the globe with gateways to the internet. These gateways are multiple and redundant, at various locations within many different countries. The network is operated by a worldwide and loose-knit community radio amateurs using FSK modulation on regular HAM equipment. However, bandwidth has been, is and will continue to be quite restricted by virtually all national governments.

The problems with short-wave resources includes the cost and technical sophistication of equipment and the limitations for operating a major site. Operators must be trained, dedicated and determined (devoted) to keeping up their part of the operation. There are challenges that can emerge by the simple fact of their being a large numbers of nodes worldwide, in order to avoid the opposite problem from lack of connectivity, namely, having a confusion over what is new information and what is old. Clutter can build up quickly, and this can be a big problem when large volumes of text and video may be involved. In rural areas there can be problems due to large areas that may lack reliable without connectivity. Weather can be a major disruptive factor. Furthermore there is the issue of network congestion which can arise if the number of competing nodes should get large or if simply too many people all at once are competing for the same channels. Figures 10 and 11 below illustrate two configurations in simple form of how this type of network can be implemented on a long-distance scale.

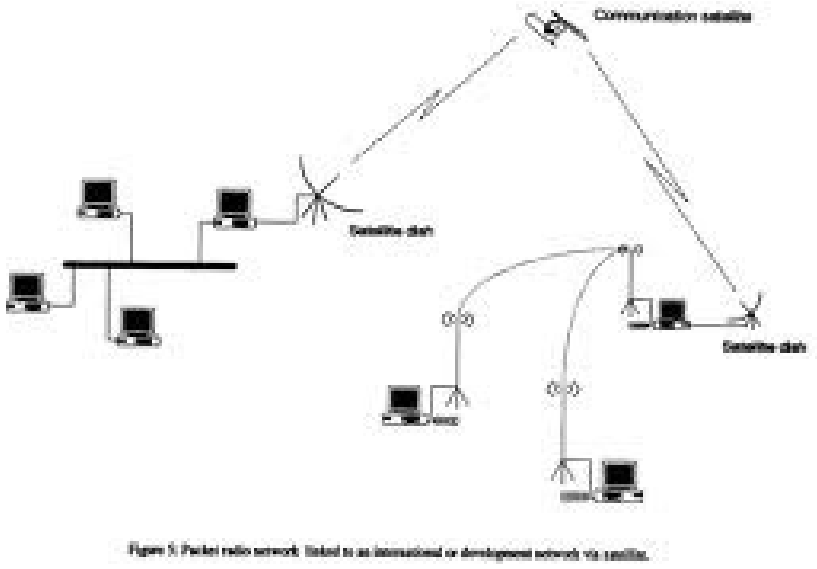


Figure 10

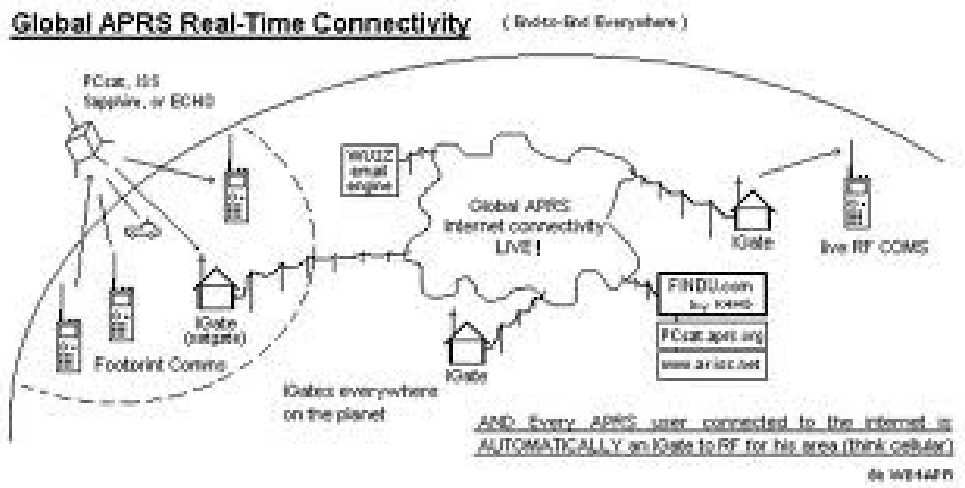


Figure 11

Mobile Ad Hoc Cellular and Wi-Fi Networks

A mobile ad hoc network (MANET) may consist of multiple device types and both the configuration and the typology may vary over time. By definition the physical distribution of the network nodes, the communication/computing devices, will vary over time since they are being moved, physically. Such a network is designed to be self-configuring (or "self-repairing) and to be without a fixed infrastructure, all communications being via wireless links. The term, *ad hoc*, is a Latin phrase meaning "for this purpose".

Within a true MANET there is no requirement for any node device to be fixed or to have any pre-programmed sequence of movement. A device is free to move independently of all others, in any direction. As a result, for any given device, its links to other devices will be liable to change, with no predictable pattern or schedule. These changes in linkage may be frequent or slow – some may not change for days or weeks. Each node (device) must function also as a "router," forwarding data traffic that is unrelated to its own function by (for instance) an individual, family, or some organization. There are severe challenges to building and maintaining a robust and reliable MANET and especially in situations of stress and duress, but the advantages are also strong. Each device must be capable of continuously maintaining within itself the information that is required to perform its routing tasks, and to thereby aid in sustaining the network flow of traffic. At the same time, the device will often be used for other functions (e.g., for voice communication or for taking pictures or video) and these computational and power-sensitive tasks must be balanced along with the routing tasks. One of the major supports for the growth of MANETs has been the widespread distribution of both 802.11 wireless "Wi-Fi" networks plus the wide distribution of capable devices, including smart phones, tablet devices, and cameras that have the capacity for significant storage, data management, and coupling to wireless devices. Add to all this the shrinkage of physical size and the improvements in battery life, and one of the results is that in many urban and semi-urban population centers, throughout the world, there are ample resources that can be employed. Figures 12 and 13 below each illustrate two conceptual views of MANET architectures – the abstract views of heterogeneous subnets and team/reference nodes (figure 12), and two hypothetical examples of implementation (figure 13).

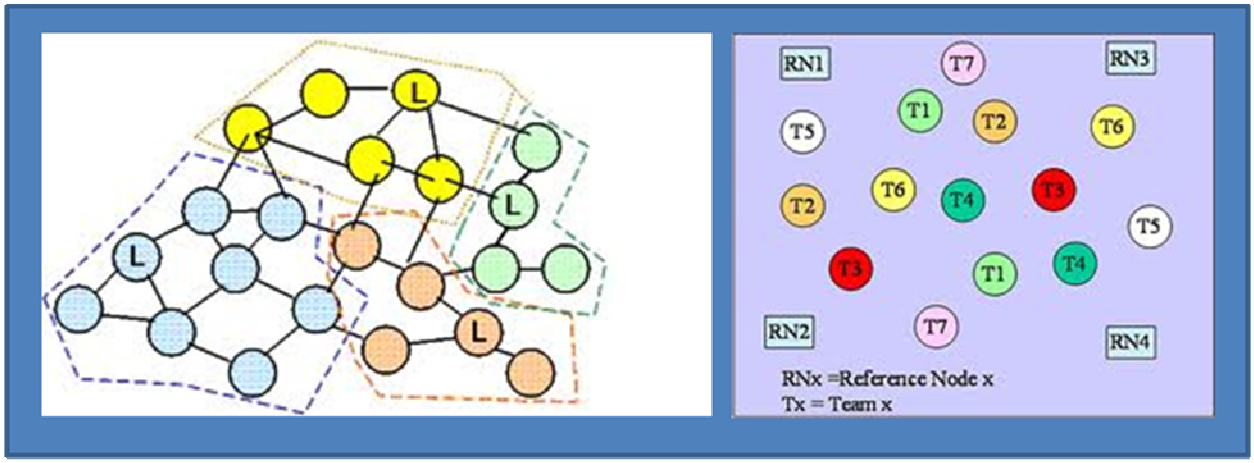


Figure 12

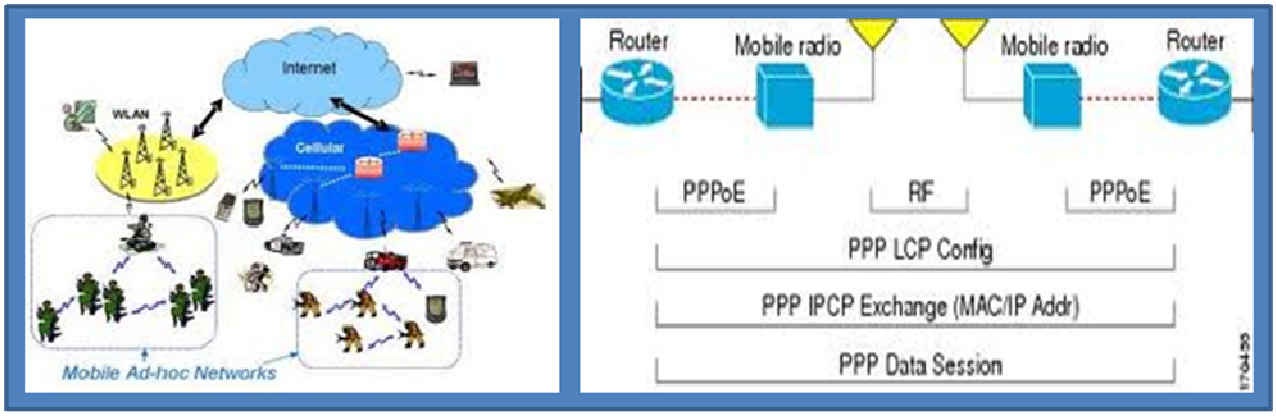


Figure 13

Hybrid "Rim" Networks

The concept of the hybrid "rim" is rather simplistic and is based upon the assumption that there are other forms of connectivity "in country." The "rim" is the border, of the region or nation-state that is affected. This border will in many cases be problematic for physical travel back and forth and for standard telecommunications of both wired and wireless forms. However, by drawing upon many of the suggested forms of communication described earlier here, it may be possible to engineer ad hoc "gateways" that operate even for a temporary period, or on a fluctuating schedule, in order to perform the equivalent of what in an older era of computing known as "business data processing" was the nightly backup, the archiving and re-arranging of files and resources.

In this case, however, what is at issue is the (bidirectional) transfer of critical information, including potentially large-sized video and other media files, across a physical barrier that will enable the information to reach certain populations and groups on the outside of the affected and closed-off region (e.g., foreign media correspondents, other governments and NGOs, the general public), and vice versa, moving critical data to individuals and populations on the inside of the region. Here is where the role of fixed or mobile short-wave packet installations, or reliable satellite transceivers, could be employed with benefit, since few in number would be required in order to achieve the cross-border key transfers.

Adaptive Encryption Strategies

Only brief mention will be made of this rather novel and little-explored approach. It is based upon a commonly used form of encryption, but with simple alterations intended to shrink down data content and also to combat against seizures and forced disclosure of encryption methods used by people doing the communications. Many forms of data encryption have been developed and PGP (Pretty Good Privacy) is a popular system. PGP is based upon a serial combination of data hashing, then differential compression, symmetric-key cryptography[11], and finally, public-key cryptography. The heart of the encryption process and the software that implementations (e.g., PGP both open-source and proprietary) is the public-key method, relying upon asymmetric key algorithms. PGP's roots are based in great part upon the RSA algorithm, widely used in many internet and web applications.[12] The non-message-content public key that is needed to transform the message into a secure form is different from the information required to reverse the process. The latter is the private key, known only by the recipient in each transaction. The person (A) who anticipates receiving messages first creates both a public key and an associated private key. The public key is published and used by others who will send encrypted messages to person (A).

The "adaptive" strategy, or class of strategies, that can help to secure and protect ad hoc and civilian-centric measures to maintain communications in spite of cut-offs and blockages of standard internet and cellular networks, is rather simplistic and it is so for good reasons – again, mainly to make the methods usable by the widest range of the population and to minimize the opportunities for harm to people by a totalitarian regime. First of all, in times of conflict and social defragmentation, it is important to get the message through, but not so important to have everything in "King's English" and "large, clear fonts." (These are meant as metaphorical allusions.) There are several algorithms for reducing the size and detail of either text or image data. Letters can be skipped according to a pattern as simple as removal of every third or fourth character from a non-numeric text. Video frames can be reduced greatly, and frames can be skipped. Images can be reduced drastically in size. All this leads to a reduction in content, but before any encryption has been undertaken.

Now the adaptive encryption comes in play. Using a one-time pad type of coding, or very conveniently a separate set of PGP-encrypted message, there can be slicing of message stream content such that different methods of using PGP on the data are employed. In other words, the public and private keys for a given user (node) X will vary. Even though the high-level method (algorithm) may remain the same, the content that is passing through as keys and later as data will change according to any number of agreed-upon parameters. Time (day, segment of day, hour), commonly accepted subject matters, or even clearly demarcated shifts within the semantic flow of a message, or an encoding based upon characteristics of the audience, including intermediate nodes within something like a MESH or MANET, can all be used to effect subject changes in the way that the type or the specifics of encryption used will change.

One major problem with this approach is the fact that it puts more demands upon all of the participants in network operation to be very knowledgeable of specific software packages and very accurate in how signals for change are generated, received, and interpreted. This is not an easy

[11] e.g., Blowfish, Triple-DES, CAST, IDEA

[12] PGP was originally designed as a combination of RSA encryption and a symmetric key cipher known as Bass-OMatic. RSA (a public key cryptographic algorithm named after its designers Ronald Rivest, Adi Shamir, and Leonard Adleman) depends upon the difficulty in factoring very large composite numbers and is currently the most commonly used encryption and authentication algorithm in the world.

method; it may be very strong, but it is one in which many mistakes can be made that could render inaccurate or useless the data of any given exchange.

"Sticks and Stones" Networking

This does not refer to literal sticks and stones, of course, but to the employment of compact and physically separate, non-communicating (non-wired, non-wireless) digital memory devices such as flash cards and memory sticks. Data from whatever computing device source including digital cameras is placed onto the card/stick medium. These can be simply transferred, physically, by individuals, and used in the very traditional way as memory devices. However, they can also be coupled with compact, easy-to-install, easy-to-run applications that are designed to be stored onto the physical media and executed from that media, by being installed onto whatever is the new platform (e.g., desktop, laptop, iPad, smart phone). While this approach may seem primitive in comparison to other architectures and protocols, the fact is that in times of stress and duress, from whatever causes (natural disaster on earth, solar flares, political and military actions), this form of networking can in fact help to fix "holes" or "gaps" in something like a strong MESH or MANET network. This can at times be the plug that fills the hole in the dike.

"Point – Counterpoint" – strengths, weaknesses, countermeasures, and overcoming them to preserve Open Social Networks

Each of the network models introduced earlier have strengths and weaknesses for achieving the type of resilient and durable connectivity necessary when socio-political forces are very likely to be actively working to disrupt whatever network is functioning. For success on a regional (sub-national), national or trans-national (multiple nation-states in close proximity or under control of the same occupational force) it is important to address more than the technical (architectural) issues. Ultimately the success of maintaining continuity and overcoming active disruption will rest upon the ability of a sufficient number of individuals to maintain routers, transceivers, access points, servers, and other hardware that is employed. Simplicity and ease-of –use are very important if diverse non-specialist members of the general civilian population will be able to contribute their talents and take their risks in keeping the network "alive." Replacement of parts, convenient means of maintaining and replenishing power, and the ability to operate without a highly visible physical or organizational infrastructure, plus rapid and convenient mobility – all of these are among the most important features that must be present in a system if it is to stand a worthy chance at operational survivability.

An approach that offers promise is one that takes into account all of the above issues as well as what are the resources and means of any opposing forces seeking to shut down the internet and cellular communications intra-nationally or internationally. The strongest system will (to use a "charged" idiomatic acronym) be "MAD" – Mobile, Adaptable, Diversified. This means to be hybrid and not susceptible to simple or linear attacks for disruption. Such a network will use a MANET architecture but one that employs some of the best-known features of classical MESH designs, where at any given time exist multiple paths that may open up from one node to others.

The paths must be changeable and no node can be critical. Reliance upon only one form of transmission should be avoided. For this reason, it will be good to create options for short-wave and satellite links if and when those may exist, but not to rely upon those either, for some of the reasons discussed above. There may be redundancy, but this can be employed to reduce the operations of any particular set of links so that no nodes – and their operators – stand out as being key operators. Thus, there are no ISPs per se. No place, no hub, no equipment, no team is an "ISP;" that function is shared by multiple agents, equipment and methods of transferring data.

There are precedents for such networks, and historically much work was done in the field of MIMD parallel processing during its early years of the 1980's and early 1990's. Self-healing networks were built using arrays of processors such as the T800 and T1000 transputer and also ARM cores. Figure 14 gives an illustration of such a network recovering from a series of faults. Applying these older models from the parallel processing world to today's era of smart phones and wi-fi devices can be useful for designing the type of network that will draw in the best from the MESH and MANET worlds.

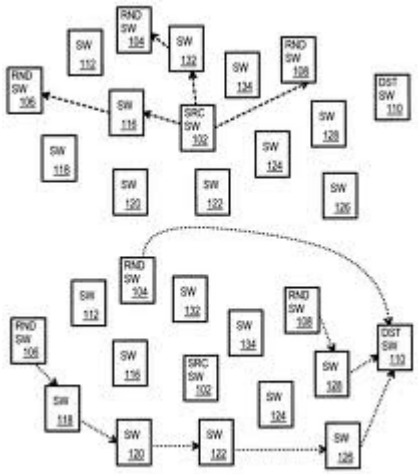


Figure 14 – A Self-Healing Network Topology in Action

If there are a sufficient number of operators and paths, then the ability of the network to provide essential data transfers will be strengthened, with a concomitant reduction in risk of detection and intervention by those working against the network. The latter will be further disabled by not having a definite "map" of how communications are being created, routed and stored at any given time. Indeed, there is no static network map, and this is an advantage. If knowledgeable participants (internet "freedom fighters") are apprehended, they will not divulge critical information that can be used to shut everything down. Apart from and beyond the courage and dedication of such people, the fact is simply that, in the best case, no such critical layout of connectivity and traffic exists, or ever exists, and thus any information surrendered or divulged will not be sufficient for bringing down the whole network.

In the domain of sensor systems including interactive, human-assisted wireless units for such tasks as chemical, biological and radiation sensing (e.g., Nomad Eyes) there have been examples of networks that demonstrate capabilities which can be translated into the non-sensor world of basic audio and video communications. Nomad Eyes [13] was designed in order to accommodate loss of large segments of critical infrastructure due to events such as natural disasters of WMD terrorist attacks. There is no reason that some of the same technology cannot be "redeployed" into the context of preserving social networks for large domiciled and mostly non-mobile populations. Figure 15 below provides a simple illustration of one application from the sensor network world.

Widespread use of as many consumer-class devices for maintaining a MESH-grounded MANET will be important. This will help keep in readiness a supply of sufficient and diverse devices. High on the list are smart phones, iPods, iPads, and media that can generate and also display audio, video, and text. However, purely audio radio communications, even two-way radios without any short-wave or digital packet transfer capabilities can also be important. How is this so? They can serve to help people to find out where there are important "gathering places" for information to be

[13] Dudziak [4], [5], [6]

fed into the network that does have links to the outside world, as well as to discover where there are broken links in the net that need to be fixed (filled) by those who have the resources and means.

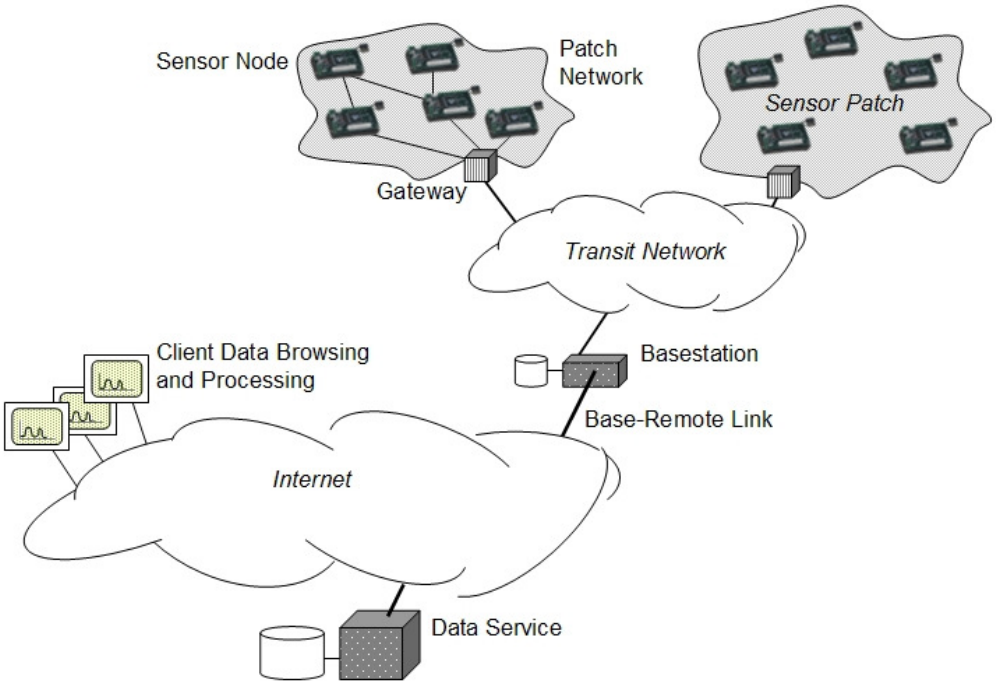


Figure 15 – Sensor Nets (or Mass-communication sub-nets) linkable via mobile base stations

In conclusion, a robust and defensible network has no center, has no critical hubs, and makes use of all forms of communication and transfer, including the aforementioned "sticks and stones" model of using compact static but highly portable and concealable digital storage devices such as flash sticks and memory cards. Ultimately the strength rests upon the people in the society who have the commitment and the drive to maintain the connections within their society and with the outside world. They will be able to persevere, and networks will be maintainable, because the opposing forces cannot be omniscient and omnipresent, and because there will never be a static "map" that can lead to physical sites and to easily disruptable public power sources. Even if individuals or groups in the network are compromised, physically, by terror-pressure or other subterfuge, there will be backups even of the slower and more cumbersome forms. History shows this to be the case, from past eras where there were neither internet nor computers.

Closing Remarks

We live in very trying and tenuous times. Challenges present themselves to our society on the most local level all the way to the global, planetary level. Unpredictable, emergent (and emergency) critical-impact events, of natural and human origin, disrupt the normal flow of information and prevent response to life-threatening crises, even without negative actions by forces opposed to freedom, integrity, liberty and the basic needs of families and peoples everywhere. The recent (March, 2011) events in Japan along with many throughout North Africa and the Middle East are experiences that can teach and help us to learn. The technologies that have become commonplace, truly "everyday" for hundreds and now billions of people, can themselves be the best foundations for people to defend and preserve their lives in these and coming trials.

References and Recommended Further Reading

Anastasi, G., A. Passarella, A., Towards a Novel Transport Protocol for Ad hoc Networks, *Proc. PWC 2003* (2003).

Awerbuch, B. et al., High Throughput Route Selection in Multi-Rate Ad Hoc Wireless Networks, Johns Hopkins Univ. Technical Report (March 2003)

Cavin, D. et al., On the accuracy of MANET simulators, *Proc. ACM Workshop on Princ. Mobile Computing* (POMC'02), pp. 38-43 (Oct. 2002).

K.-W. Chin et al., "Implementation Experience with MANET Routing Protocols," *ACM SIGCOMM Computer Communications Review*, Nov. 2002, pp. 49-59 (2002).

Corson, M. et al., Internet-Based Mobile Ad Hoc Networking," *IEEE Internet Computing*, July-August 1999, pp. 63-70 (1999).

Datta, A., A fault-tolerant protocol for energy-efficient permutation routing in wireless networks, IEEE Transactions on Computers, Vol. 54, No. 11, pp. 1409 - 1421 (Nov. 2005).

Dudziak, M. [1], IMEDNET : Information Gateways and Smart Databases for Telemedicine and Distance-Based Learning Using the Internet and the WWW, *Internet Medicine Conference*, Chicago, (Oct. 23-24, 1995).

Dudziak, M. [2], CommonHealthNet as an Architecture for Practical Global Medicine, *Global Telemedicine and Federal Technologies Conference*, Williamsburg, VA, (July, 1996).

Dudziak, M. [3], MediLink -- A SmartCard-Assisted Wearable Data Acquisition and Communication System for Emergency and Mobile Medicine, *INABIS*, Toronto, CA (Dec., 1998).

Dudziak, M. [4]. Mobile Early Warning, Intervention and Public Health Response to Nuclear Terrorist Actions, 3rd Int'l Conf. on Radiation Countermeasures, St. Petersburg, Russia, (Oct., 2004).

Dudziak, M. [5], I^{3}BAT and Nomad Eyes - Countermethods of Sensing and Preventive Response, European Symposium on Counterterrorism Response, Berlin, Germany, (Dec., 2004).

Dudziak, M. [6], Angus, C., Life-Saving Technologies Critical to Improving Speed and Scope of Response to Mass-Population Emergency Events and Pandemics, *17th World Conference on Disaster Management*, Toronto, CA, (July, 2007).

Elliott, C., Heile, B., Self-Organizing, Self-Healing Wireless Networks, *Proc. 2000 IEEE Int'l Conf. on Personal Wireless Comm.*, pp. 355-362 (2000).

Gogate N., Chung, D., Panwar, s., Wang, Y., Supporting Image/Video Applications in a Mobile Multihop Radio Environment Using Route Diversity and Multiple Description Coding, *IEEE Trans. CSVT, Vol. 777* (2002)

Jetcheva, J. G. et al., Design and Evaluation of a Metropolitan Area Multitier Wireless Ad Hoc Network Architecture, *Proc. 5th IEEE Workshop on Mobile Computing Syst. & Applications* (WMCSA 2003), Monterey, CA (October 2003).

Kaufman, Charles, et. el. *Network Security: Private Communication in a Public World,* 2nd. ed. Prentice Hall, Upper Saddle River, NJ (2002).

Lee, C. K.-L., Lin, X.-H., Kwok, Y.-K., A Multipath Ad Hoc Routing Approach to Combat Wireless Link Insecurity, *Proc. ICC 2003, Vol. 1*, pp. 448–452 (May 2003).

Mauve, M., Widmer, J., Hartenstein, H., A Survey on Position-Based Routing in Mobile Ad Hoc Networks, *IEEE Network* **1** (6): 30–39 (Dec., 2001).

Nasipuri, A., Castaneda, R., Das, S. R., Performance of Multipath Routing for On-Demand Protocols in Mobile Ad Hoc Networks, *Mobile Networks and Applications, Vol. 6, No. 4*, pp. 339–349 (Aug. 2001).

Ozan, K. T., Gianluigi F., ed., *Ad Hoc Wireless Networks: A Communication-Theoretic Perspective*, John Wiley & Sons (2006).

Ramasubramanian, V. et al., SHARP: A Hybrid Adaptive Routing Protocol for Mobile Ad Hoc Networks, *Proc. 4th International Symp. on Mobile Ad Hoc Networking and Computing* (MobiHoc 2003), Annapolis, MD (June, 2003).

Rheingold, H., Smart Mobs: The Next Social Revolution, *The Power of the Mobile Many*: 288, MAS 214, Macquarie University (2002).

Royer, E., Toh, C., A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks, *IEEE Personal Communications* **6** (2): 46–55 (April, 1999).

Shields, C., Jain, V., Ntafos, S., Prakesh, R., Venkatesan, S., Fault-Tolerant Mobility Planning for Rapidly Deployable Wireless Networks, *Proceedings of the IEEE Workshop on Fault-Tolerant Parallel and Distributed Systems, LNCS* (1998).

Stallings, W., *Cryptography and Network Security: Principles and Practice,* 3rd. ed. Prentice Hall, Upper Saddle River, NJ (2002).

Toh, C. K. ed., Ad *Hoc Mobile Wireless Networks: Protocols & Systems*, Prentice Hall Publishers (2002).

Zadeh, A. N. et al., Self-Organizing Packet Radio Ad Hoc Networks with Overlay (SOPRANO), *IEEE Communications Magazine* (June, 2002).

Zimmerman, P., *The Official PGP User's Guide,* MIT Press, Cambridge, MA (1995).

Ziolo, P. [1], Trauma and Transcendence: Psychosocial Impacts of Cybernetics and Nanotechnology, *Proceedings of the PISTA 2003 International Conference on Informatics and Systemics (AAAS)* - also available on the World Systems Analysis Archive - URL: http://wsarch.ucr.edu/archive/papers.htm and http://wsarch.ucr.edu/archive/papers/**ziolo**/PISTA03-paper.doc (2003).

Ziolo, P. [2], The Psychodynamics of Dominance and Submission, in *Power in Focus*, Durlabji, S. (ed.), Wyndham Hall Press, Northwestern State University, LA, pp. 119-161 (2004).