Project Cyber Dawn v1.0

April 17

2011

This document may contain proprietary and controlled unclassified information requiring protection from disclosure. Ensure proper safeguarding. The following notice may apply - "FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE – PROPRIETARY Any misuse or unauthorized disclosure can result in both civil and criminal penalties."

LIBYA

ليبيا

Protecting cyberspace is the responsibility of all nations; a safer cyberspace can promote freedom of action, democracy and prosperity.

حماية الفضاء الإلكتروني هى مسئولية جميع الأمم،
و أمانهُ يمكن تعزيز حرية التصرف و الديمقراطية
والازدهار.

THIS PAGE IS INTENTIONALLY BLANK

EXECUTIVE REPORT

Project Cyber Dawn is the result of a collaborative research effort of twenty-one individuals from the USA, Australia, Canada, Egypt, Italy, Tunisia and the UK. The Cyber Security Forum Initiative (CSFI) is a non-profit, worldwide organization with a mission to provide Cyber Warfare awareness, guidance and security solutions through collaboration, education, volunteer work and training to assist NATO partners in their common government, military and commercial interests. Today, CSFI is a community of nearly seven thousand cyber security and cyber warfare professionals from governments, militaries, private sector and academia.

Project Cyber Dawn: Libya collates, analyzes and reports on raw data and its interconnections that have been harvested from the public domain. Recent events are correlated with known historical data to provide an in depth view into Libyan Cyber Warfare capabilities and defenses.

In light of recent NATO actions to protect Libyan civilians, the primary media focus has been placed on the elimination of Libyan military equipment that has been, or could be used to suppress and oppress, through the use of lethal force, the civilian population. In this information age, this report provides a detailed look at the information technology status of Libya.

Through this analysis, CSFI can help the international community to understand not only Libya‗s potential to influence the balance of cyberspace, but also the physical repercussions of cyber-attacks originating from, and directed towards Libya. In light of the recent STUXNET virus attack on Siemens produced Supervisory Control And Data Acquisition (SCADA) systems, particular focus is given in later chapters to Libya‗s vulnerabilities to this genre of attack and the risks associated with this.

Early on, Project Cyber Dawn: Libya provides a picture of Libya‗s current Internet status with a historical view of it implementation, current cyber terrain and infrastructure and communications networks and dependencies. Recent civil unrest has been surrounded by outages to Libya‗s Internet connectivity, the timing of which coincides with heightened civilian casualty reports. A breakdown of known Libyan Government websites and their providers are provided. The collective analysis of these information points provides an indication to Libya‗s potential for information gathering and dissemination operations worldwide and shows recent government efforts to attempt to conceal military efforts against civilians by deliberately shutting down Internet connectivity to the country. To ensure a continual government controlled web presence, Libya uses international service providers in it's hosting many of which are located in the US.

Libya‗s cyber offensive and defensive capabilities clearly show a relative lack of security surrounding most of Libya‗s network and communications infrastructure, however given the rapid acceleration in IT growth, this is expected to become a key focus area in the near future. Although behind in offensive cyber security capabilities, the threat of cyber attacks from, or on behalf of Libya should not be ignored.

Government efforts to recruit cyber-mercenary groups have been successful with over 10 identified loyal hacking groups. Many of these have no geographical affiliation and as such are notoriously difficult to monitor and defend against. If left unchecked by the international community, Libyan cyberspace could provide a fertile ground for malicious software development, cyber-attacks against allies, and further cyber-activist recruitment.

A study of malware signatures and activity rates Libya as high (150+ DLI Score), indicating a relatively low security level and a significant risk of breaches and attacks. The type of risk is classified as severe indicating a high probability of data loss, malicious advanced persistent threat (APT) activity and propagation as well as multiple compliance failures. Ongoing monitoring during government controlled Internet shutdowns shows almost a 90% reduction in malware with activity focused within the Tripoli area. This indicates that some connectivity is maintained during these outages and that these systems may be vulnerable both new attacks and exploitation of current infections.

Chapter 3 of the report analyses IT investments in Libya and foreign partnerships and indicate overall sector expansion and growth prior to the recent unrest. Libya is adopting new communications infrastructures such as satellite broadband, submarine fiber optics and 4G mobile communications as they increase their investment in information technology education. Although Libya is poised toward rapid growth and progression, evidence suggests there is a risk of disruption as a direct consequence of recent events. In this current climate, there is a significant risk of cyber-attacks against Libya that may have far-reaching effects. It is likely that Libya will continue to progress at an increasing rate in their infrastructure and IT self-sufficiency in the coming decade.

The risk of targeted and focused attacks on a countries infrastructure and corporate knowledge is becoming more severe as an appreciation for information control and acquisition develops. Recent media has covered stories of such attacks and some experts have theorized that certain of these may have been state sponsored. Although Libya has limited internal cyber warfare knowledge, she has drawn heavily from forces outside her borders in the past and will likely continue to do so until the current generation of students develops the necessary expertise. Libya is at a critical period and it is recommended that the international community come together to encourage the development of acceptable behavior, protocol and standards for this rising generation of specialists.

The impact of a successful cyber-attack on Libya may have far reaching consequences. A single individual or small group has the potential, in a worst-case scenario, to gain a measure of control over the economies of allied nations whose economies have a level of dependence on Libyan oil production. Libya‘s lack of cyber security coupled with industrial automation presents a ripe target for attacks that are designed to gain control of, or sabotage critical infrastructure. Potential outcomes and are discussed with their local and global impact. The impact of infrastructure-targeted cyber-attack is not limited to the systems affected, or even trading partners who rely on the production of oil, or gas products. A successful attack against a refinery or electrical grid system has the potential to lead to a widespread fear of repeat attacks in other regions and cause an inflation surge in the global economy due in part to a loss of consumer confidence. Even if other systems were protected from these vulnerabilities, there remain questions of whether the general public will be trusting of these protections, and how effective nations will be in collaboratively responding to these threats.

CERTs (Computer Emergency Readiness Teams) are designed to provide cyber emergency channels for nations to respond to and defend against cyber-attacks. Although no internal CERT is in place, Libya is a full member of OIC-CERT (CERT of the Organization of Islamic Countries). There is no evidence to date that Libya has benefitted from this arrangement or possesses any cyber capabilities other than the external groups already mentioned. Previous behavioral patterns suggest that it is more likely in the event of an attack that Libya would solicit the assistance of Serbian professionals rather than OIC-CERT. Serbian, Tunisia and Malaysia all have functional CERTs that may assist Libya under such circumstances.

The short and long-term impact analysis of cyber warfare shows Italy as being the largest consumer of Libyan oil. Ireland, Italy and Austria all receive over 20% of their total oil from Libyan sources. Although this does not place the US at direct risk, there is a risk of a connected economic impact from allied nations whose economies would be affected by Libyan oil production.

It is hoped that the analysis and research presented in this report will increase awareness of cyber warfare as both a threat to be aware of, and an effective tool that if used appropriately, may expedite the resolution, or reformation to a post-conflict and stable Libya by a reduced loss of civilian life and minimal negative impact to global economic stability.

EXECUTIVE SUMMARY

Project Cyber Dawn was created for the purpose of educating both our local communities and world governments on the current cyber security position of Libya. Libya‘s current state of unrest, the use of the Internet and cyberspace from actors on both sides of the conflict and Libya‘s quest to significantly increase its IT capabilities in order to attract foreign investment has created an environment in Libya primed for cyber-attacks. This document seeks to explore these areas and takes a unique approach in research by incorporating Data Link Intelligence. That combined with information gleaned from open source documentation and Palantir software has provided this project with in-depth perspectives that can be utilized by government officials, research practitioners or others seeking information regarding how Libya utilizes cyberspace and the risks therein. Due to the new developments in the region, Libya stands out as a significant player in both the oil market and in the international community. By analyzing Libya‘s cyber capabilities, CSFI can help our international community to understand not only how Libya could possibly influence the balance in cyberspace but also the physical consequences of cyber-attacks originating from and directed toward Libya. Special focus has been given to exploring SCADA, an extremely relevant topic and highly related to potential gaps within Libya‘s infrastructure.

CSFI is cognizant of the potential vulnerabilities presented in this report and has taken measures to minimize the potential use of this document by state actors and non-state state actors in cyber operations by omitting certain sensitive elements. This informational report is based entirely on information found in the public domain and as such is unclassified. Project Cyber Dawn is the result of collaborative efforts from cyber security experts with various technical backgrounds. Twenty-one CSFI volunteers have worked intensely in the crafting of this report; CSFI would like to recognize their service and collaborative spirit. CSFI would also like to thank the efforts of those who serve in silence for the overall benefit of cyberspace. CSFI would like to give special thanks to our Middle Eastern based colleagues and their arduous research work in making this possible.

A special thanks to Palantir for allowing our project members to use their powerful software in the analysis of cyber intelligence. This report is purely informative and educational with data found in the public domain.

CSFI has used its best efforts to insure the accuracy of this report. However, the accuracy of the report cannot be guaranteed. The purpose of this report is educational.

PARTICIPANTS

These are the CSFI project members who participated in Project Cyber Dawn – Libya, without their hard work and dedication this report would not be possible:

Amr Ali, Egypt
Founder and CRADO/CSO, Databracket

Zubair Ashraf, Canada
Independent Security Researcher

Eric Bachelor, USA
STS1(SS), US Navy

Jeffrey S. Bardin, CISSP/CISM, USA
Chief Security Strategist, Treadstone 71, LLC Adjunct Professor, Utica College

Chris Blask, USA
VP Marketing, AlienVault

Justin Clarke, USA
Principal Technical Architect, Energy Sector Security Consortium

Larry Dietz, JD, USA
Information Security and Legal Advisor/Adjunct Professor, American Military University

Jim Harper, CSFA, USA
Harper Jones Digital Forensic Examiners, LLC

Karim Hijazi, USA
CEO/President, Unveillance

Tasha Jones, USA
Deputy Program Manager, ITT Corporation

Joel Langill, CEH CPT CCNA TUV FS-Eng, USA
Officer, CSFI Department of Critical Infrastructure (SCADAhacker.com)

Dhamir Mannai, PhD CISSP, Tunisia
Chief Information Security Analyst, Cyber Security Lab 27

Stefano Mele, Italy
ICT Law, Intelligence & Security

Dale C. Rowe, PhD CITP MBCS, USA/UK
Asst. Professor of IT, Brigham Young University

Christine S., USA
Information Assurance Engineer, Lunarline, Inc.

Ron Southworth, Australia
SCADA Systems Specialist

Paul de Souza, USA
CSFI Founder Director

Kevin Stevens, USA
Senior Threat Researcher, FTR Group Trend Micro

J. "oday" Tubbs, USA
CTO Unveillance

Connie Peterson Uthoff, CSFI OSINT, USA
Analyst

Pano Yannakogeorgos Ph.D, USA
Military Analyst, Air Force Research Institute

Table of Contents

1. Libya and the Internet 1

1.1 A historical background of how the Internet was established in Libya 2

1.2 Timeline of Early Stages of Libya's Unrest 3

1.3 Libya's Cyber Terrain 13

1.4 Cyber Infrastructure and Communications Networks 18

1.5 Government Websites and its Providers 20

2. Libya's Cyber Offensive and Defensive Capabilities 21

2.1 Introduction 21

2.2 A Call to Cyber-Jihad 23

2.3 Malicious Code Activity in Libya 24

3. Libya and IT Investments 29

3.1 Introduction and Background 29

3.2 Are Cyber-Attacks a Realistic Concern? 33

3.3 The Potential Impacts of Cyber-Attacks on the Libyan Oil and Gas Industry 35

3.4 Other Alternate Futures 38

3.5 Some Implications in Regards to Oil, Gas, and International Cooperation 38

3.6 CERT – A model for possibilities 41

3.7 Short and Long Term Consequences of Cyber-Attacks 43

3.7.1 Short and Long-Term Impact to the infrastructure and economy of Libya 43

3.7.2 Short and Long Term Impact on the Economy and Infrastructure of Others 44

4. Oil, Gas and SCADA 47

4.1 Introduction and Background 47

4.2 Vulnerabilities within Libyan SCADA Systems 50

5. Analysis 53

5.1 Creation of Social Networking Sites 54

6. Conclusions 55

6.1 About CSFI (The Cyber Security Forum Initiative): 55

Table of Figures

Figure 1-1 – CSFI Analysis of Libyan Internet Activity as it correlates to War Reports 9
Figure 1-2 – Ongoing Libya Internet Outages (Jan 25 – Feb 22, 2011) 10
Figure 1-3 – Libya Web Traffic (25 Feb – 4 Mar, 2011) showing disconnect on 3 March 10
Figure 1-4 – Libyan Internet Traffic by Application (25 Jan – 21 Feb, 2011) 11
Figure 1-5 – Renesys Traceroute Analysis into Libya (13 Feb – 22 Feb, 2011) 12
Figure 1-6 – Palantir Interconnections and Relationships among Libyan Government sites 14
Figure 1-7 – Palantir Entity Corellations 15
Figure 1-8 – Palantir Map of Libyan Government Sites 16
Figure 1-9 – Libyan IP Prefixes 16
Figure 1-10 – Libyan IPv4 Peer 17
Figure 1-11 - Prefix 41.208.64.0/20 from Feb 15th 2011 to Feb 26th 2011 (AS21003 – Libya) 17
Figure 1-12 - Prefix 41.74.64.0/20 from Feb 15th 2011 to Feb 26th 2011 (AS6762 – Italy) 18
Figure 1-13 - Submarine cable connections linking Libya to the rest of the World 19
Figure 2-1 – Palantir Investigative Dashboard depicting Hacking Entities in Libya 22
Figure 2-2 – Entity Threat Level based on Historical Evidence and Known Skill 22
Figure 2-3 - Libyan Malware Activity (February 1 – April 13) 25
Figure 2-4 – Libyan Malware Hourly Activity (Feb 17 – Apr 13) 26
Figure 2-5 – Malware Traffic Localization 27
Figure 2-6 – Global Mariposa Malware Signatures 28
Figure 3-1 – Libya's Population and Energy Production 36
Figure 3-2 – Road and Pipeline Infrastructure in Libya 37
Figure 3-3 – Libyan Oil Production vs. Consumption (2000-2010) 43
Figure 3-4 – Libya's Oil Exports by Destination (Jan 2010 – Nov 2010) 44
Figure 3-5 - Cruide Oil (including condensate and NGLs) imported from Libya (kb/d) 45
Figure 3-6 – Total Products imported from Libya (kb/d) 46
Figure 4-1 – Libyan Crude Oil as % of Total National Crude Oil Imports 48
Figure 4-2 - Refinary 50

Table of Tables

Table 1-1 - Early Days of Conflict (references for Table at end of Report) 7
Table 1-2 – Opposition and Government Fatalities 12
Table 1-3 – Libya's Main Internet Service Providers 20

Table 2-1 - DLI Threat Levels 24
Table 2-2 - Libyan Malware Activity Breakdown (Feb 1 - Apr 13) 26
Table 2-3 - Top 5 Malware Generating Hosts since March 3 27

1. LIBYA AND THE INTERNET

The Libyan crisis of 2011 and the uprisings in Tunisia and Egypt have demonstrated how the use of computers and the Internet can influence revolution and shape political futures. In these recent rebellions, protesters used cyberspace to rally for support, to campaign for democracy and to communicate to the outside world. Governments used/blocked the Internet to limit the power and connectivity of the people. In Libya, the ongoing civil unrest also affected world finance, shook investor confidence, drove up oil prices and may possibly negatively impact the international economy for years to come. In each example, the power of the Internet to shape change, both radical and unexpected, has clearly demonstrated that the computer can be used as a tool to connect individuals in dramatic ways that can and has transitioned lives and governments and the political fabric of the very world in which we live. Of equal significance, the international growing unrest, advances in IT, the increasing sophistication and number of hackers, outdated control systems connected to the infrastructure, and limited legal deterrence to launching cyber events are pressing issues facing the global community today with potentially alarming consequences if they are not addressed. Using Libya as a model, this report will explore some of those issues with the hope of providing knowledgeable insights to be used to address these threats and find solutions for a sustainable future.

The recent uprisings in Tunisia, Egypt, Bahrain and Libya, the ability for individuals to coordinate and assemble rapidly, made possible through the use of the Internet and social media platforms, significantly highlight how individuals, countries and governments now view and use cyber space as a vehicle for change, revolution, and control. Of equal relevance, during the same period of time, in February 2011, hackers suspected to originate from China attacked five oil refineries (Telegraph, 2011). The combination of the rapid spread of revolution across the Middle East, the attacks on the oil refineries and the nuclear facility in Iran, cyber events in Georgia/Russia and Estonia, as well as the strategic use of the Internet/computers in Libya from both opposition and government forces indicates that the computer is becoming a significant component in regards to political and revolutionary ambitions, that its role in strategy, attacks and control is increasing on both local and national levels, and that though the international community can witness the results of uprisings ignited through the use of social media, it is essential that careful attention is also paid to the covert actions of cyber attackers. Our infrastructure, economies, political systems and lives are put at risk by minimizing their immediate significance.

On February 17, 2011, Libya‘s citizens gathered in a revolution that remains unresolved to this day. Unlike Tunisia and Egypt, Libya was the first oil producing country in the Middle East to launch civil unrest. As a result, this situation has become important to look at in regards to how the Internet/computer has been used in this revolution and how it may continue to be used. This document reviews the history of the Internet in Libya, its communication systems, how social media shaped the early stages of revolution as well as how both forces used the Internet as part of their strategy. As part of this exploration, this document also reviews Libya‗s information technology sector, its cyber terrain, and the malicious code activity during the period of unrest. We also look at threats in regards to potential cyber-attacks on the Libyan oil and gas infrastructure, examine the concerns related to SCADA and how this may relate to and impact the global economy and international security. If there are threats to Libya, do those same threats exist for other areas of the world? What does this moment in history suggest about potential futures and the need for greater computer and Internet security?

1.1 A historical background of how the Internet was established in Libya

Even within the past decade, computers and the Internet have provided the world with significant advantages and have become an intrinsic part of everyday life. Whether we choose to turn on a laptop or not, global economies, governments, military institutions, the media and infrastructures depend on the efficiency, coordination and connectivity provided by computers and access to the World Wide Web. Over the past five years with the introduction of Facebook and Twitter, the Internet has become deeply woven into the social fabric of human interaction, connecting individuals in an instant to people across the globe and giving each other access to different cultures, perspectives. As reflected in the recent uprisings in the Middle East, it has become a tool to unite people in a common cause; in this case, revolution. To have a better picture of how quickly the Internet developed in Libya and to more fully comprehend the implications of Internet usage during the uprisings, it can be helpful to look at the history of the Internet in the region.

During the final months of 1998, overshadowed by the strained dialogue surrounding the Pan Am flight bombing, Libya introduced the Internet to its country in an official capacity only. Until the year 2000, there were very few actual on-line users; however, early that year, Libya began to make the Internet available to the Libyan citizens. Since that time there has been an almost tense relationship between development and control as access to the Internet has been seen as both an opportunity for national growth as well as a potentially threatening bridge to global communication and information. The following sections illustrate the challenges and promises related to the development of Internet usage and availability in Libya.

In 1995, a comparative study from International Perspectives found that The Socialist People's Libyan Arab Jamahiriya reported the lowest non-government IT penetration in North Africa. As a result of the UN trade sanctions in place during 1992, data from that period of time is limited; however, Libya reportedly had the highest GNP per capita (as a result of oil revenues) at the time, and the smallest population in North Africa. It seemed remarkable that despite the business development potential connected to access to the World Wide Web, Libya had no Internet connectivity (Danowitz, 1995).

Through these early years, Libya had a relatively modern telecommunications infrastructure with the capacity to provide service to approximately 10 million subscribers, the lines available were significantly less than that amount, providing only around 370,000 lines instead, an estimated 4.8 lines per 100 people. According to Danowitz et al, their research found that this reflected ―….the under-utilization of the telephone network by citizens and its heavy subscription by the government and military" (Danowitz, 1995). An example of how this government footprint stepped further into the lives of citizens and investors is illustrated in the regulation that requires citizens and foreigners to register computers, telephones, fax machines, and other communications devices owned by Libyan citizens with the government (Danowitz, 1995).

Despite Libya's slow start, the following years reflected a dramatic increase in Internet access. The Arabic Network for Human Rights Organization reported that in 1998, the number of Internet users in Libya did not exceed 100 people (The Arabic Network for Human Rights Organization (ANHRO), 2004). It further documented that by early 2001, the number reached 300,000 once Internet service was extended to the public. The number more than doubled by the mid-2003 and was estimated to be 850,000. In 2005, the amount of on-line users was rapidly reaching one million, a dramatic increase from 1998 when only a handful of individuals had access. With a population of around six million individuals, usage had grown to almost one sixth of the population (ANHRO, 2004). The future of Libya and the Internet looks promising based on business projections, but the current unrest may set the country back as it struggles for stability and recovery. The opportunity and challenges still exist, and time will reveal how quickly (or if) it can return to the course of growth and opportunity.

1.2 Timeline of Early Stages of Libya's Unrest

"In this important historical juncture which Libya is passing through right now, we find ourselves at a turning point with only two solutions. Either we achieve freedom and race to catch up with humanity and world developments, or we are shackled and enslaved under the feet of the tyrant Mu'ammar Gaddafi where we shall live in the midst of history… To connect with our people at home and abroad, and to deliver our voice to the outside world, we have decided to establish this website as the official window of communication via the World Wide Web" (Libyan Interim National Council, 2011)

This statement is located on the website that was constructed by the coalition interim government. Speaking out on-line against Gaddafi is a revolutionary act in Libya and highlights how important the Internet, a symbol for freedom and development to some, became during the conflict.

In respect to the use of the Internet during the crisis, a few specific characteristics became clear at this time. The first is that the rapid increase of online communication corresponded with action/protests from the citizens. Second, the Internet proved to be a tool for quick and massive organization reflected by a comment from an Al Jazeera reporter who said, "They are well organized and say that they will make Manama's Pearl Roundabout Bahrain's version of Egypt's Tahrir Square" (Fox, 2011).

And third, protesters were not the only ones to make use of the power of the Internet. Ghaddafi and his government forces strategically limited access to the Internet early in the revolution. This became a concern, not only for the citizens of Libya, but also for foreign business partners worried about future opportunities. Global citizens also became concerned about human rights violations and for the impact that civil unrest might have on Saudi Arabia, the oil market and the economies of some of Libya‘s trade partners, especially Italy.

As quickly as Internet usage exploded in Libya over the past few years, the impact of social media has caught on even more rapidly, spreading, as Malcom Gladwell might surmise, like a virus, becoming a tool for political change and the sharing of revolutionary ambition. The Jasmine Revolution in Tunisia (December 2010 – early 2011) demonstrated to the world the capacity for abrupt change and the use of the Internet as a powerful agent in that pursuit. Egypt reinforced this trend, and soon the fervor spread into Libya. Libya‘s ”cyber-activists” (Fox, 2011) made use of social media outlets Twitter and Facebook to organize their cause, calling for a ―Day of Anger” on Thursday, February 17, 2011, the anniversary of the 1987 public execution of nine men accused of treason. On Tuesday, February 16, 2011 Facebook was reported to have over 4,000 followers. By Wednesday, February 17, the number had more than doubled to 9,600 members (The Peninsula, 2011).

The following table lists some of the important events during the early stages of civil unrest in Libya as a means to track key events on both sides of the conflict. The table documents the following: for each day listed, there is a corresponding stage in the revolution, fatality reports, political statements and reactions both from within Libya and from the West, highlights of government control of the Internet with links to Internet traffic reports and finally reactions from the citizens as they work to find ways to communicate with each other and the outside world despite the limitations to access.

The following table offers some insights into the timing of the events from the internal Libyan actors to those supporting the cause (government and rebel supporters) from outside its borders. There are also larger implications that can be taken from this information as well. .Some of the interesting highlights are:

1) There are parallels between the civil war events and the use of social media. For example, prior to the conflict, on February 15th and 16th, membership for the cause on Facebook increased by over 5000 members. During periods of heightened conflict, the Libyan government shut down the Internet, however support groups from outside Libya were quickly prepared with alternate methods for citizens to communicate with the outside world. Arasmus kept detailed information in regards to daily reports and created a Google map to track events and reported the following, ―At the time of writing, the map has had over 314,000 views in 12 days. It has been shown on Al Jazeera English. It has been covered in at least the following 20 news publications: the Lede Blog at the New York Times, Zeit Online, Wired, Huffington Post, Newshour, The Guardian, Global Voices, Los Angeles Times, Wall Street Journal Blog, Kurier (Austria), La Stampa, Excite Italia, Le Post, Expresso, Prachatai (Thailand), Observa Internacionales, Mashable, The Register-Guard, American Public Media, WiredVision (Japan)” (Arasmus, 2011). Similarly, on March 1, 2011, The United Nations' Office for the Coordination of Humanitarian Affairs also created a map to

document events. Telecomix provided safe internet resources, Operation Libya White Fax provided another alternate path of communication and even the hacker group Anonymous sent a ‗note to the UN‘ on behalf of Libyan citizens.

These supporters responded within the first week, some the very day that the rebellion began and quickly had large numbers of followers. The heavier traffic and support from the external community correlates to a study by DHS on Social Networks and disasters. Its research indicates that Twitter is a good leading indicator of the effects of the disaster and also a good measurement of when the disaster is perceived to be over by the population (DHS, 2011). In this situation, support via the Internet seemed to be most pressing when A) there was limited or no other forms of communication to reach those inside Libya. With the absence of Media coverage, sites like Arasmus and the UN map took on new significance as there were few other resources available. This could be important models for future conflict or areas hit by disaster. B) When reports of causalities seemed to be at their peak.

Table 1-1 illustrates this correlation between events/revolution and the immediate response from the outside community. This is helpful for practitioners interested in tracking Social Networking and disaster/conflict.

2) The table also reflects an interesting gap between the timing of overt government response and the rate in which grassroots efforts coordinate and respond. Groups like Telecomix and others provided options for the rebellion almost immediately after Internet service was disrupted. Individuals both from inside Libya and externally mobilized, communicated and worked to find methods to provide information to the outside world in moments. Governments and institutions, bound by laws and procedures, move much slower, despite their best intentions, as seen in the table.

A valuable trend that is occurring, one that could become a viable tool in the midst of future conflict or disaster, is that the flexibility and resources the grassroots cyber community has, is a power within itself and can be used to compliment the aid and assistance from the larger international community. The outside support was consistent, immediate, and at the very least provided morale, access to information and vehicles for communication to the rebels, and served to be a link to the conflict until support from the larger community could be provided.

3) There is a correlation between the government shutdown of the Internet and periods of heightened fatalities, suggesting that Libya may have used the internet as a tool to shield the international community from events inside their country as well as a strategy in regards to military efforts and controls. Libya has worked diligently over the past years to meet international standards, to overcome a reputation of supporting terrorism, and to create a culture that encourages foreign trade and investment. To have the world witness a brutal confrontation with Libyan citizens would

undermine Libya‘s goals for development. Shutting down the Internet during times of heightened violence would prevent the immediate disclosure of those events.

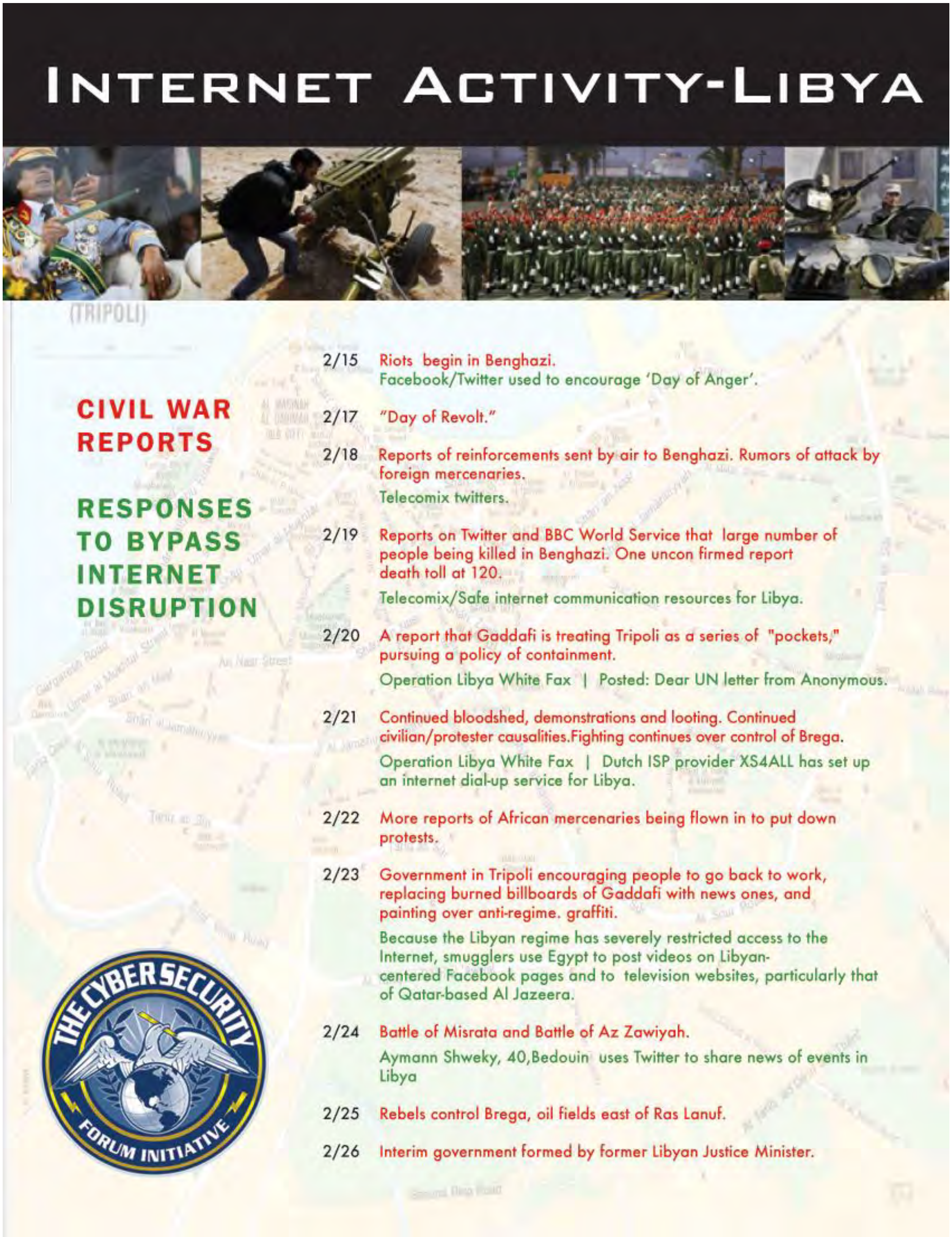
Renesys suggests that Libya took a different strategy than Egypt. Instead of initially shutting down the Internet completely, like ‗slowly turning off a faucet‘, there were slower periods of shut down and then the Internet was back on line again prior to shutting it off again in March (Renesys, 2011). It could suggest that the government believed they could suppress the violence right away as mercenaries were rumored to be on their way. Or it could have been a tactic to ease into the shutdown, giving the government forces more time to mobilize. It also could have provided the government brief access to the Internet while denying it to the rebel forces.

Renesys also suggests, as mentioned above, that shutting down the Internet completely might create international sympathy for the rebels which would not be a key strategy for Libya. ―Using denial of Internet access as a political weapon during crisis events is all about timing and messaging. Mubarak waited too long to implement his blackout, and then let it run past the point where the damage to the Egyptian economy and the cost of international outrage exceeded the dwindling benefits to the regime. In the end, all the Egyptian government accomplished was to attract the sort of sympathetic attention and message support from the Internet community that is pure oxygen to a democratic opposition movement" (Renesys, 2011).

Table 1-1 - Early Days of Conflict (references for Table at end of Report)

Date (2011)	Civil Unrest and Death Toll Reports	Political/Official Statements	Internet Activity	Traffic Report links - Libya	Responses to Bypass Internet Disruption
2/15	Riots begin in Benghazi		http://libyacrisismap.net/main	Internet Score Card	Facebook/Twitter used to encourage ‗Day of Anger‘
2/17	―Day of Revolt”	Interim Government established in Benghazi			
2/18	Reports of reinforcements sent by air to Benghazi. Rumors of attack by foreign mercenaries	Link to other timelines: http://www.globalsecurity.org/wmd/library/news/libya/2011/libya-110408-irin01.htm	Complete outage of Internet reported – 13 globally routed Libyan network prefixes w/drawn at 23:18 GMT	http://www.google.com/transparencyreport/traffic/?r=LY&l=EVERYTHING&csd=1296862200000&ced=1299281400000	Telecomix twitters
2/19	Reports on large numbers being killed in Benghazi. One report death toll at 120. February 17–20 Opposition: 332-479 Government: 163	Religious Scholars, Intellectuals and clan elders speak out against violence.	Internet outage - traffic volumes 60-80% below normal. Partial service restored Saturday morning, cut off again @ 2pm PT Two-thirds of Libyan routes came back to life at 6:01 UTC (8:01 local time), and the remainder were restored nine minutes later	http://blog.caida.org/best_available_data/2011/03/23/unsolicited-internet-traffic-from-libya/	Telecomix/Safe internet communication resources for Libya: http://www.werebuild.eu/wiki/Libya/Main_Page
2/20	A report that Gaddafi is treating Tripoli as a series of "pockets," pursuing a policy of containment		Partial shutdown of Internet	http://www.google.com/transparencyreport/traffic/?r=LY&l=YOUTUBE&csd=1296723600000&ced=1299142800000	Dear UN letter from Anonymous http://feb17.info/general/anonymous/

2/21	Continued civilian/protester causalities. Fighting continues over control of Brega February 17–25 300 Opposition In Tripoli	Gaddafi's son, Saif al-Islam calls for _general assembly Libya's Justice Minister resigned at ―excessive use of violence: against protesters Sec. of State Hillary Clinton, ―We join the international community in strongly condemning the violence in Libya."	Prefixes unreachable from 1am to just after 8am Sunday morning Al Jazeera pinpoints source of signal blockage to a Libyan intelligence agency building, south of the capital Tripoli.	http://www.google.com/transparencyreport/traffic/?r=LY&l=WEBSEARCH&csd=1297619832558&ced=1298748600000 http://www.monkey.org/~labovit/blog/	Operation Libya White Fax http://refuse.fr/blog/index.php?article6/operation-lybie Dutch ISP provider XS4ALL has set up an internet dial-up service for Libya. Use your modem to dial +31205350535 username: xs4all password: xs4all
2/22	Estimates of up to 4000 injured	Arab League suspends Libyan delegation from meetings	Routes seem impaired, but up	http://www.renesys.com/blog/2011/02/libyan-disconnect-1.shtml	http://www.arasmus.com/2011/03/01/mapping-violence-against-pro-democracy-protests-in-libya/
2/23	Government in Tripoli encouraging people to go back to work February 24–March 10 Opposition: 234-247 Government 65	Statement from President Obama —…suffering and bloodshed is outrageous and unacceptable…" Italy says total death toll over 1000	Libya Internet outages continue with a consistent 60-80% drop in traffic volumes. – Report on Traffic update for 2/22 http://www.monkey.org/~labovit/blog/	http://www.google.com/transparencyreport/traffic/?r=LY&l=WEBSEARCH&csd=1297619832558&ced=1298748600000	Because the Libyan regime has severely restricted access to the Internet, smugglers use Egypt to post videos on Libyan-centered Facebook pages and to television websites, particularly that of Qatar-based Al Jazeera.
2/24	Battle of Misrata and Battle of Az Zawiyah	Ahmed Ghadaf al-Dam defects to Egypt (Gaddafi aide)	Traffic in Benghazi slows	http://monkey.org/~labovit/blog//viewpage.php?page=libya_firewall_cracks	Aymann Shweky, 40,Bedouin uses Twitter to share news of events in Libya
2/25	Rebels control Brega, oil fields east of Ras Lanuf	Gaddafi appears in Tripoli Green Square			
2/26	Interim government formed by former Libyan Justice Minister	UN Security Council imposes sanctions against Col. Gaddafi		http://www.renesys.com/blog/2011/02/libyan-disconnect-1.shtml	



INTERNET ACTIVITY-LIBYA

CIVIL WAR REPORTS

RESPONSES TO BYPASS INTERNET DISRUPTION

2/15 Riots begin in Benghazi.
Facebook/Twitter used to encourage 'Day of Anger'.

2/17 "Day of Revolt."

2/18 Reports of reinforcements sent by air to Benghazi. Rumors of attack by foreign mercenaries.
Telecomix twitters.

2/19 Reports on Twitter and BBC World Service that large number of people being killed in Benghazi. One uncon firmed report death toll at 120.
Telecomix/Safe internet communication resources for Libya.

2/20 A report that Gaddafi is treating Tripoli as a series of "pockets," pursuing a policy of containment.
Operation Libya White Fax | Posted: Dear UN letter from Anonymous.

2/21 Continued bloodshed, demonstrations and looting. Continued civilian/protester causalities.Fighting continues over control of Brega.
Operation Libya White Fax | Dutch ISP provider XS4ALL has set up an internet dial-up service for Libya.

2/22 More reports of African mercenaries being flown in to put down protests.

2/23 Government in Tripoli encouraging people to go back to work, replacing burned billboards of Gaddafi with news ones, and painting over anti-regime. graffiti.
Because the Libyan regime has severely restricted access to the Internet, smugglers use Egypt to post videos on Libyan-centered Facebook pages and to television websites, particularly that of Qatar-based Al Jazeera.

2/24 Battle of Misrata and Battle of Az Zawiyah.
Aymann Shweky, 40,Bedouin uses Twitter to share news of events in Libya

2/25 Rebels control Brega, oil fields east of Ras Lanuf.

2/26 Interim government formed by former Libyan Justice Minister.

Figure 1-1 – CSFI Analysis of Libyan Internet Activity as it correlates to War Reports

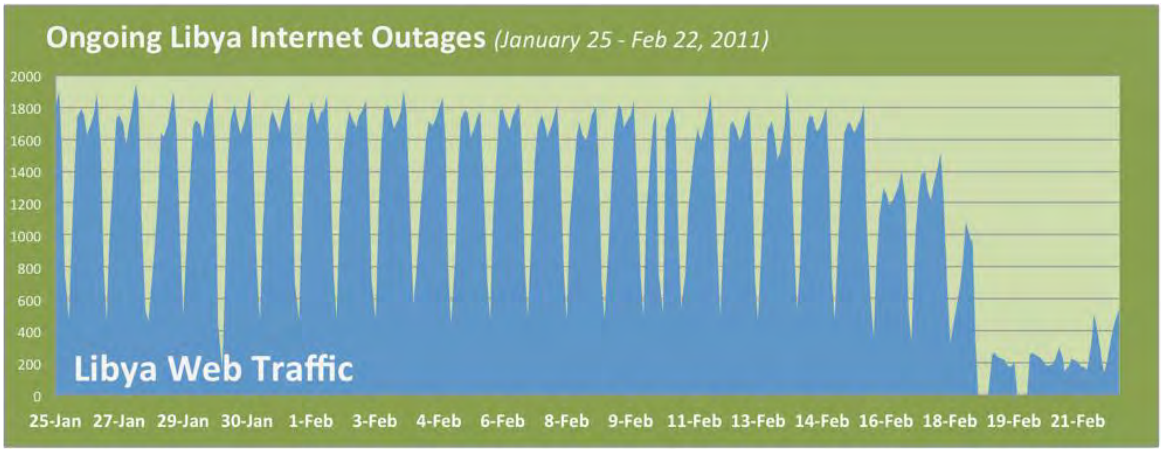
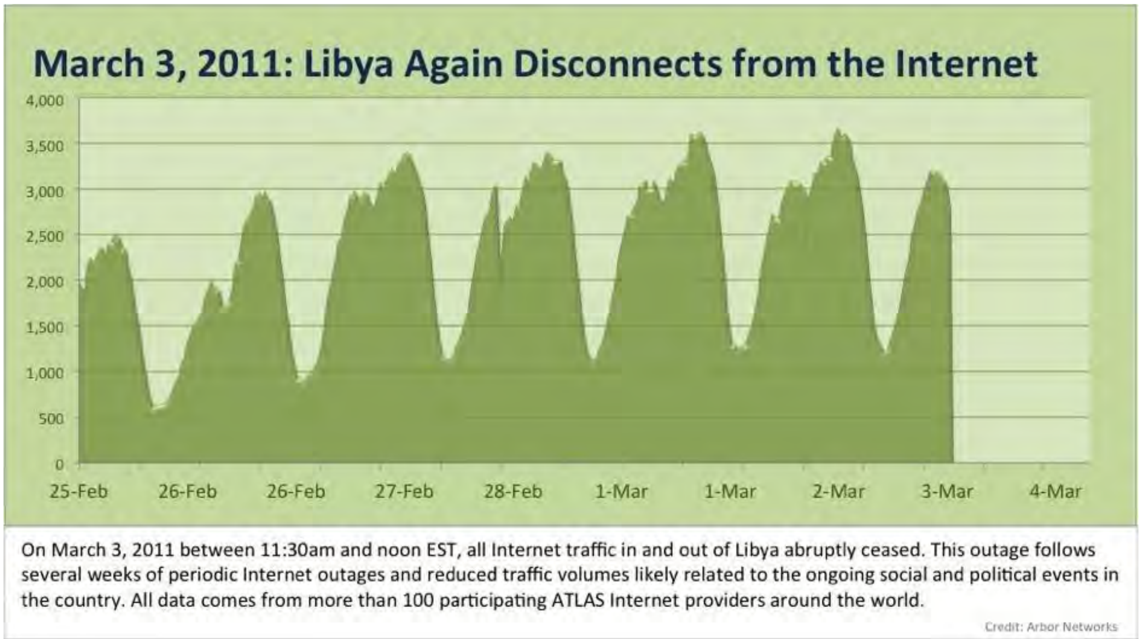


Figure 1-2 – Ongoing Libya Internet Outages (Jan 25 – Feb 22, 2011)

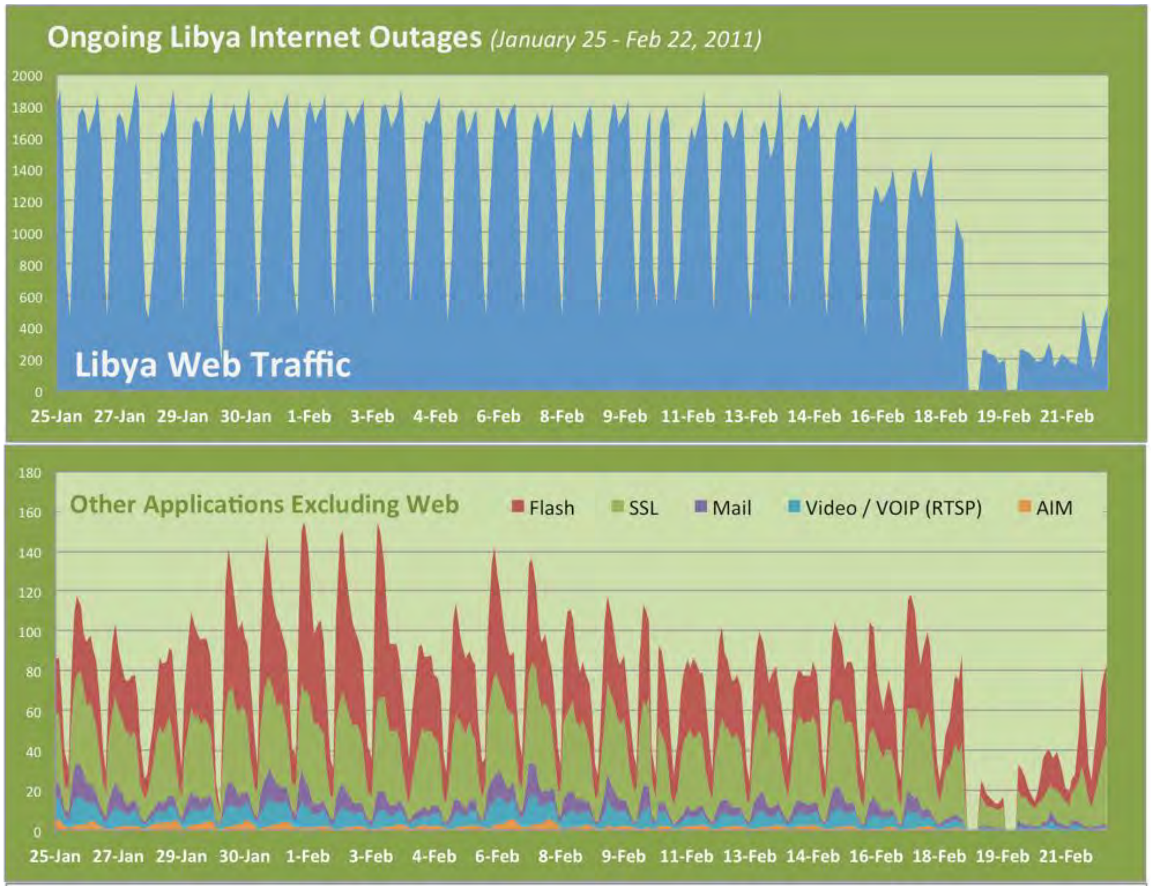
These reports reflect the Internet traffic in and out of Libya. According to these reports and the Unveillance reports on page 25, internet traffic was not completely shut down at first, –even though almost all traffic is blocked from traversing it. The BGP routes to Libya are still intact, which means that the Libyan ISP's border routers are powered on and the fiber optics are lit. In fact, we've identified a handful of isolated live IP addresses inside Libya, responding to ping and traceroutes, and presumably passing traffic just fine. Someone in Libya is still watching YouTube, even though the rest of the country is dark" (Renesys, 2011).



On March 3, 2011 between 11:30am and noon EST, all Internet traffic in and out of Libya abruptly ceased. This outage follows several weeks of periodic Internet outages and reduced traffic volumes likely related to the ongoing social and political events in the country. All data comes from more than 100 participating ATLAS Internet providers around the world.

Credit: Arbor Networks

Figure 1-3 – Libya Web Traffic (25 Feb – 4 Mar, 2011) showing disconnect on 3 March



A graph of a Libya traffic by application (TCP and UDP port groupings) over the month of February. The top graph shows only Web and the bottom the top five other applications. Beginning on Friday (February 18), Internet traffic suffered several multi-hour outages followed by a continuing 60-80% reduction in traffic impacting all Internet applications. While outage impacts all applications, disproportionate decrease in Web and AIM traffic. All data comes from more than 100 ATLAS ISP participants.

Credit: Labovitz, Arbor Networks

Figure 1-4 – Libyan Internet Traffic by Application (25 Jan – 21 Feb, 2011)

There is a correlation between the government shutdown of the Internet and periods of heightened fatalities, suggesting that Libya may have used the internet as a tool to shield the international community from events inside their country as well as a strategy in regards to military efforts and controls. Originally, in February, as indicated above, the Internet only had ‗multi-hour outages‘, suggesting that Gaddafi forces may have planned strategy specific to those times, that they underestimated the rebel forces and anticipated an end to fighting (on 2/23 the government in Tripoli encouraged citizens to return to work), they wanted to shield what they believed would be the bloodiest times of battle or they wanted to continue some traffic so as not to alienate/concern the international community, investors or foreign business partners. Regardless, watching Internet traffic to and from a country can be a good tool for political, military and intelligence analysts in gauging the potential intent of a government and the potential escalation of violence.

Table 1-2 – Opposition and Government Fatalities

Date	Opposition fatalities	Government Fatalities	Detail
February 17–20	332-479	163	First Battle of Benghazi
February 17–25	300	None reported	Tripoli clashes
February 18–*ongoing*	263-485	194-225	Battle of Misrata
February 24–March 10	234-247	65	Battle of Az Zawiyah
March 4–12	71-81	4-27	Battle of Ra's Lanuf
March 4	34-100	None reported	Explosion at an arms depot in Benghazi.

This data provided by Renesys is valuable because it measures the events in tighter periods of time than the others. For analysts, governments, or anyone conducting business within Libya, this information can be essential. Renesys further reported that, ―that the 13 globally routed Libyan network prefixes were withdrawn at 23:18 GMT (Friday night, 1:18am Saturday local time), and Libya is off the Internet. One Libyan route originated by Telecom Italia directly is still BGP-reachable, but inbound traceroutes appear to die in Palermo. A minority of our peers reports some surviving paths through the peering connection between Level3 and Telecom Italia, but traceroutes into those prefixes fail, suggesting that the Libyan cut off is complete" (Renesys, 2011).

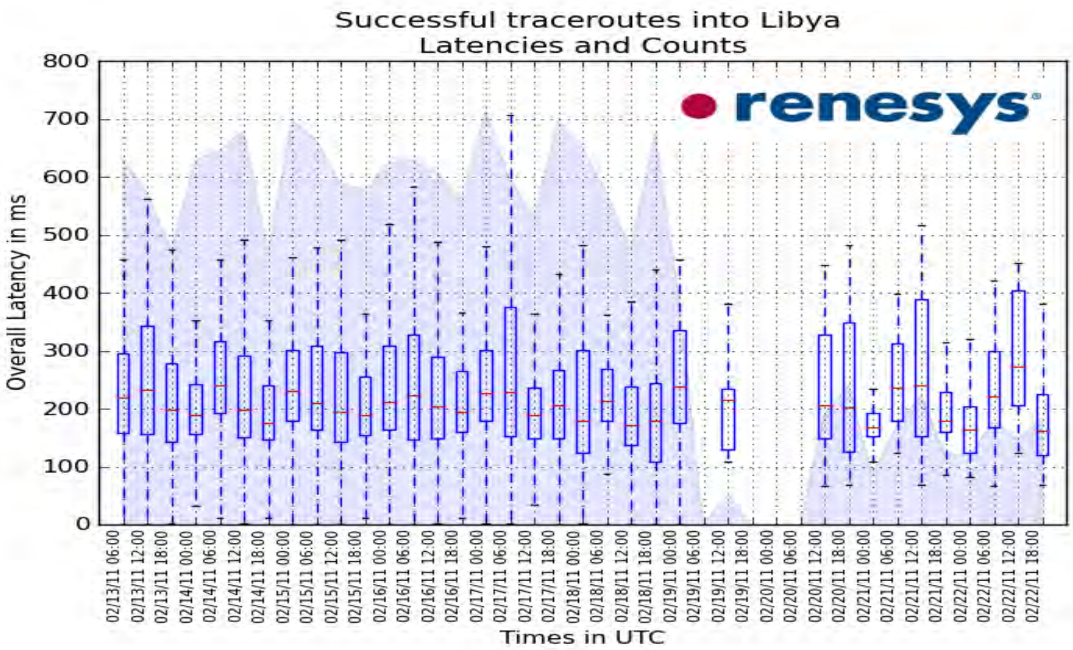


Figure 1-5 – Renesys Traceroute Analysis into Libya (13 Feb – 22 Feb, 2011)

A security advisor at Trend Micro commented, ―Every Libyan website (by this I mean sites hosted in Libya, www.bit.ly for example is still live) that I tested was unreachable, with traffic simply failing to get a response after the last hop on the internet backbone outside the Libyan address space. The best analogy

I can think of is that, although the figurative canal system is still in place to get traffic to the right destination, Libya simply pulled the plug and drained the water". (UPI, 2011).

1.3 Libya's Cyber Terrain

Libya's cyber terrain is mainly owned by the government with some interesting strategic relationships in regards to technology in the west. An interesting example of this is a company from California which handles a lot of the hosting services for Libya.

Figure 1-6 was developed by CSFI using Palantir software and shows the complex interconnections among Libyan government sites, their relationships and some of the locations hosting their sites. It is worth noting that there are many areas within the United States that provide hosting for these government sites such as those found in California, Texas, and Michigan.

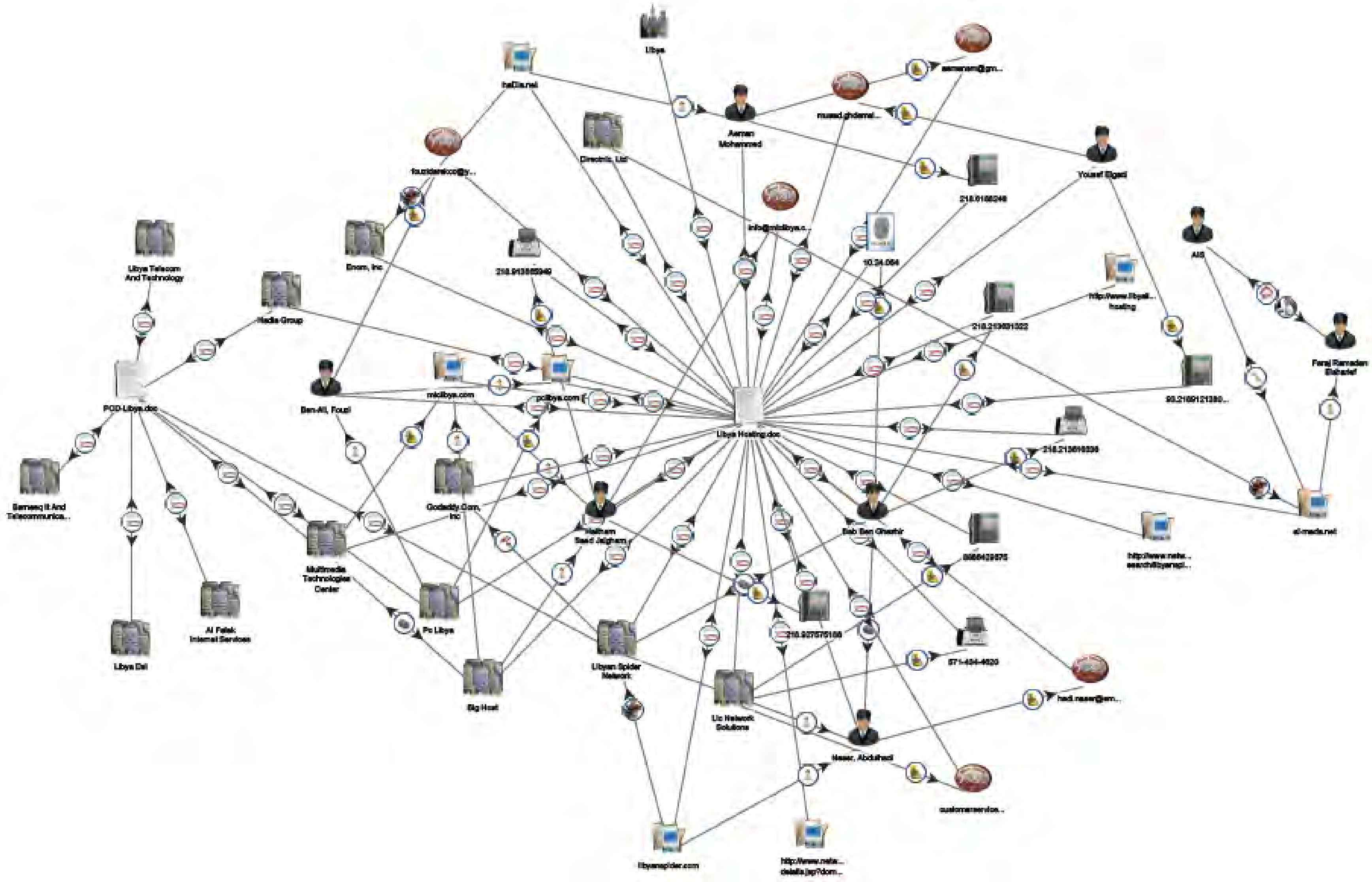
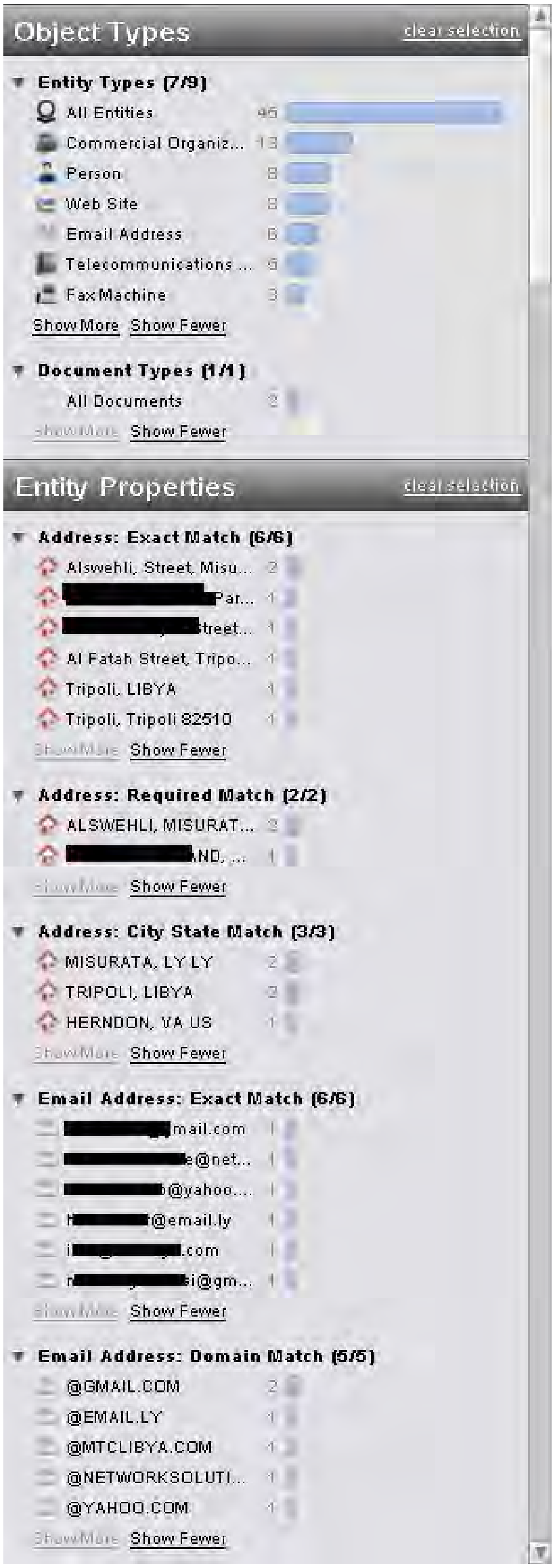


Figure 1-6 – Palantir Interconnections and Relationships among Libyan Government sites



Object Types

Entity Types (7/9)

All Entities	45
Commercial Organiz...	13
Person	8
Web Site	8
Email Address	6
Telecommunications ...	5
Fax Machine	3

Document Types (1/1)

All Documents	2

Entity Properties

Address: Exact Match (6/6)

Alswehli, Street, Misu...	2
[redacted]Par...	1
[redacted]treet...	1
Al Fatah Street, Tripo...	1
Tripoli, LIBYA	1
Tripoli, Tripoli 82510	1

Address: Required Match (2/2)

ALSWEHLI, MISURAT...	2
[redacted]ND, ...	1

Address: City State Match (3/3)

MISURATA, LY LY	2
TRIPOLI, LIBYA	2
HERNDON, VA US	1

Email Address: Exact Match (6/6)

[redacted]mail.com	1
[redacted]e@net...	1
[redacted]b@yahoo....	1
h[redacted]@email.ly	1
i[redacted].com	1
n[redacted]i@gm...	1

Email Address: Domain Match (5/5)

@GMAIL.COM	2
@EMAIL.LY	1
@MTCLIBYA.COM	1
@NETWORKSOLUTI...	1
@YAHOO.COM	1

Figure 1-7 – Palantir Entity Corellations

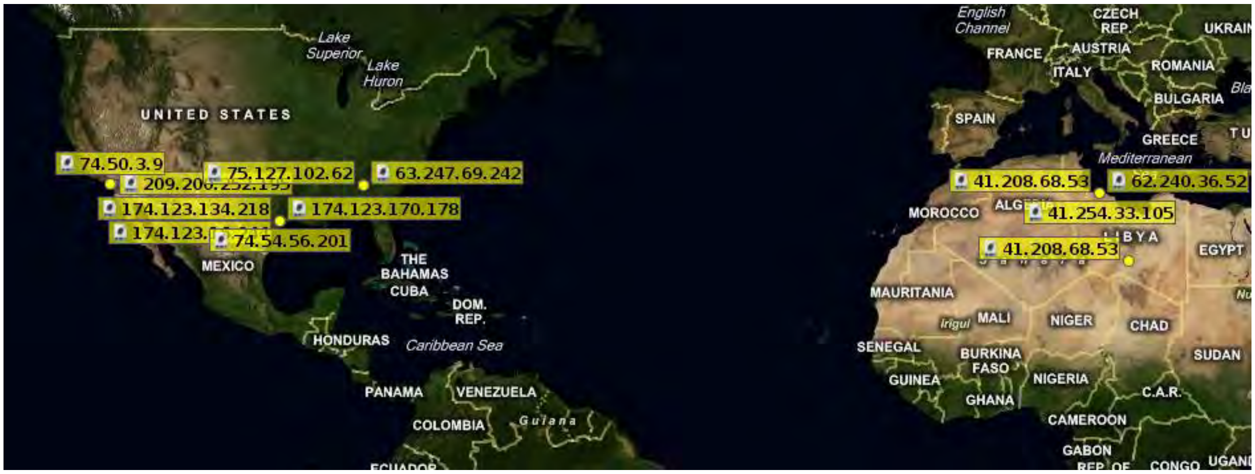
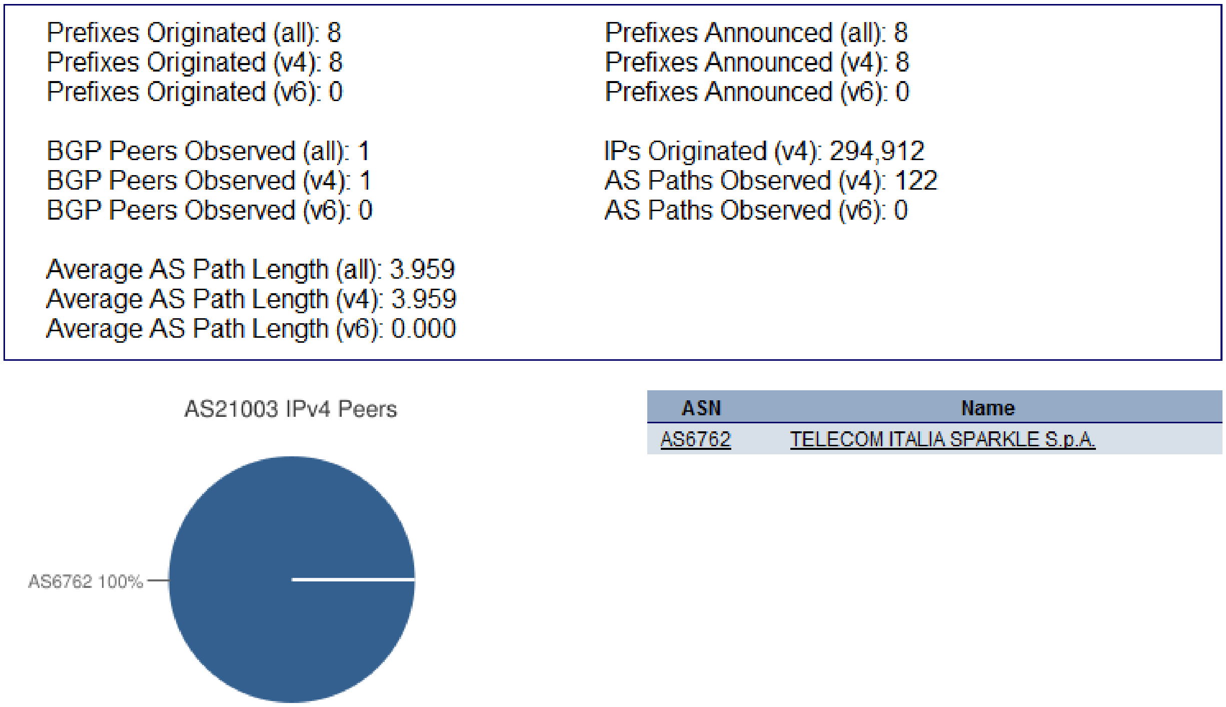


Figure 1-8 – Palantir Map of Libyan Government Sites

This map shows a good number of IP addresses in the US that have hosted or are hosting Libyan government sites.



Prefixes Originated (all): 8
Prefixes Originated (v4): 8
Prefixes Originated (v6): 0

BGP Peers Observed (all): 1
BGP Peers Observed (v4): 1
BGP Peers Observed (v6): 0

Average AS Path Length (all): 3.959
Average AS Path Length (v4): 3.959
Average AS Path Length (v6): 0.000

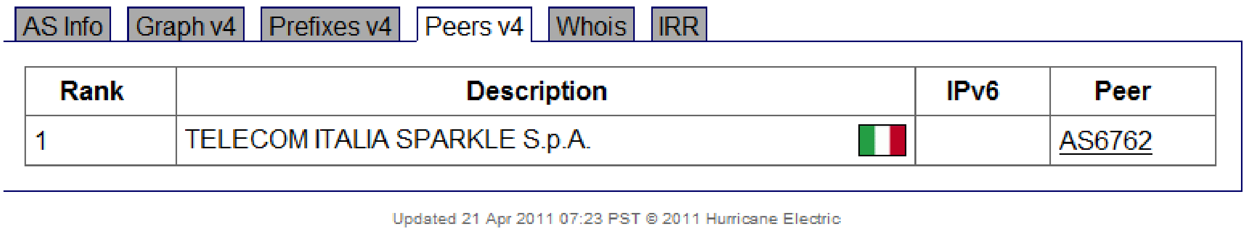
Prefixes Announced (all): 8
Prefixes Announced (v4): 8
Prefixes Announced (v6): 0

IPs Originated (v4): 294,912
AS Paths Observed (v4): 122
AS Paths Observed (v6): 0

ASN	Name
AS6762	TELECOM ITALIA SPARKLE S.p.A.

Figure 1-9 – Libyan IP Prefixes

Figure 1-9 shows all the IP prefixes for Libya with 122 Autonomous Systems paths observed and the main IPv4 peer to AS21003 (Libya) being AS6762 from Italy. Manipulation of AS21003 will directly affect Libya's cyber communications. (Source: http://bgp.he.net/AS21003#_peers)



Rank	Description	IPv6	Peer
1	TELECOM ITALIA SPARKLE S.p.A. 🇮🇹		AS6762

Updated 21 Apr 2011 07:23 PST © 2011 Hurricane Electric

Figure 1-10 – Libyan IPv4 Peer

Libya's allocated IP blocks:

# Country: LIBYAN ARAB JAMAHIRIYA
# ISO Code: LY
# Total Networks: 5
# Total Subnets: 299,008
41.74.64.0/20
41.208.64.0/18
41.252.0.0/14
62.68.32.0/19
62.240.32.0/19

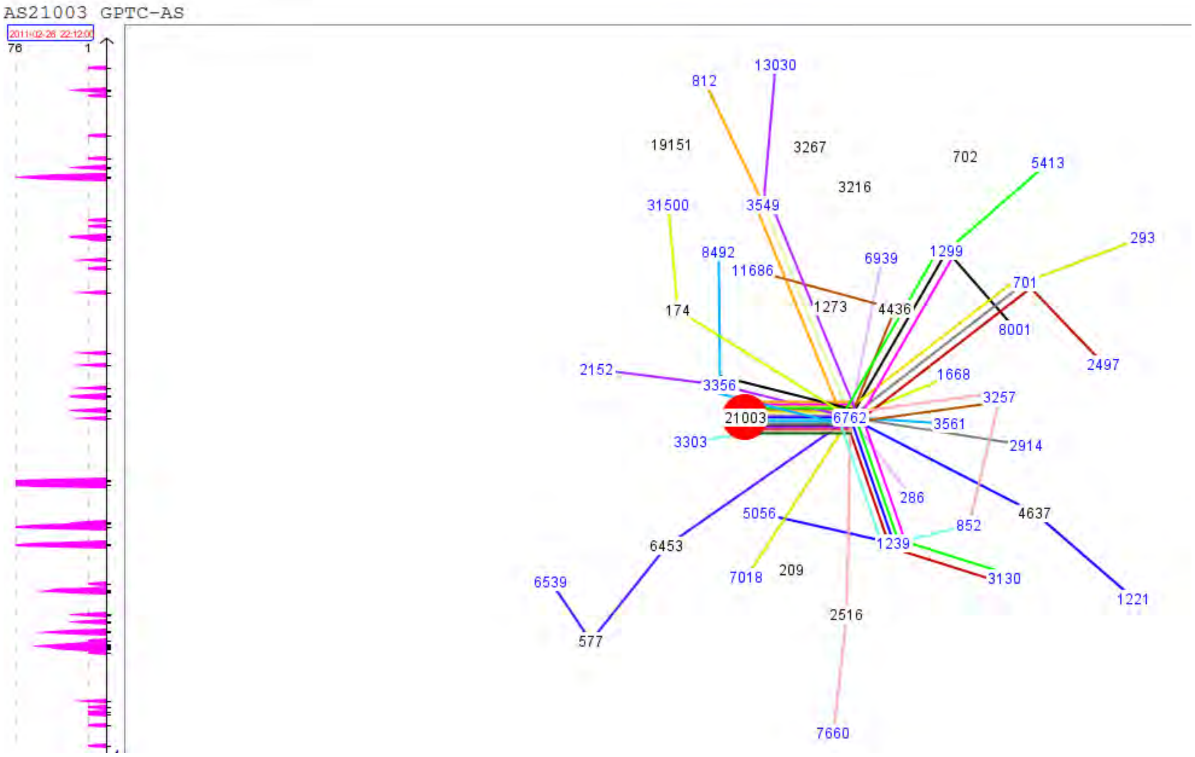


Figure 1-11 - Prefix 41.208.64.0/20 from Feb 15th 2011 to Feb 26th 2011 (AS21003 – Libya)

Figure 1-11 shows how the Libyan IP block 41.208.64.0/20 is routed through AS 21003 through several alternate routes during the days of physical unrest in Libya. (Source: http://bgplay.routeviews.org/)

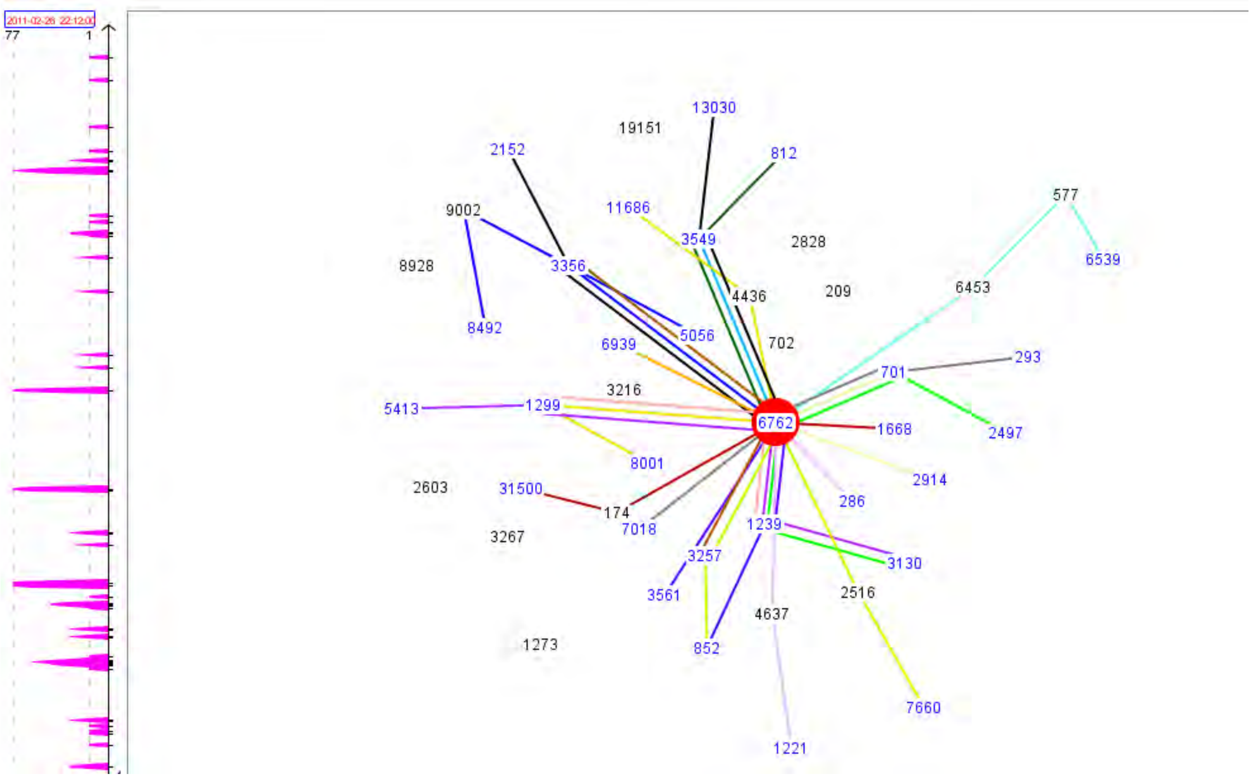


Figure 1-12 - Prefix 41.74.64.0/20 from Feb 15th 2011 to Feb 26th 2011 (AS6762 – Italy)

An interesting video of BGP route changes over time can be viewed at: http://www.youtube.com/watch?v=t4DsZyKk2zU

1.4 Cyber Infrastructure and Communications Networks

Understanding communications in Libya begins with the GPTC or General Post and Telecommunications Company. This state owned organization is responsible for overseeing all the postal and telecommunication services in Libya, including satellite telecommunications, mobile telephony (for example its partnerships with the Al Madar and Libyana Mobile Phone), fixed telephony and other Libyan internet service providers such as the Libyan Telecom & Technology Company (LTT). The power and influence Gaddafi's family has over communication in Libya is demonstrated by the fact that the president of the largest telecom company in Libya is Gaddafi's eldest son, Muhammad (Anima, 2011).

A report from Anima Investment Network states in regards to Libya's network, ―Libya has considerable network and transmission equipment compared to its population: nearly 180 telephone exchanges (main suppliers: Alcatel, Siemens, Ericsson), 13 earth stations providing the national connections via the ARABSAT satellite (the DOMSAT network), international connections and a VSAT network.

Figure 1-13 shows two of the submarine cable connections that physically link Libya to the rest of the Web (red ovals).

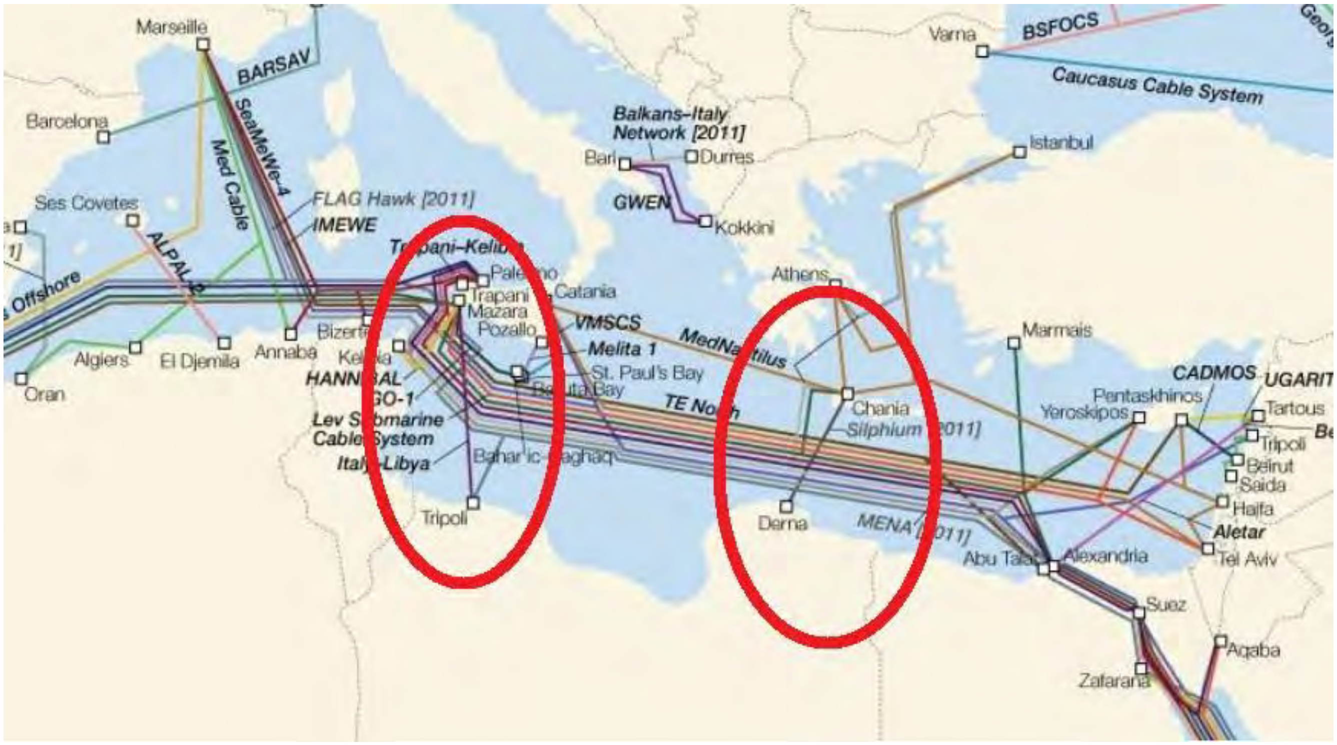


Figure 1-13 - Submarine cable connections linking Libya to the rest of the World

This is nearly 10,000 km of radio-relay systems and border-to-border connections, linking the Mediterranean coast from the Tunisian border to Egypt. It also provides more than 30,000 km of UHF radio bands, a 6500 km network of coaxial cables backing up the radio relay system and connecting 107 cities, set up by four Italian companies (Pirelli, SIRTI, CEAT and Telettra)" (Anima, 2011). The Thuraya Company offers satellite telecommunications to mobile users and, though headquartered in Dubai, is a subsidiary of GPTC and therefore governed by the same laws in Libya.

In 2005, the law that oversees the GPTC and its subsidiaries was put into effect by the General People's Committee. They created both the National Authority for Information and Documentation as well as the General Authority for Information and Telecommunications.

In 2009 when Libya lost its marine cables connection to Malta/Italy, they routed their Internet traffic through the marine cables of Tunisia. At that time period, also, Algeria routed most of its Internet traffic through Tunisia because of the breakdown of its under-sea cables that run between Annaba and Marseille.

1.5 Government Websites and its Providers

Libya Telecom and Technology (LTT) controls and moderates the Internet and telecommunications throughout Libya. This service was developed in 1997 and headed by the Gaddafi family. In 2004, it was placed under the GPTC (General Post and Telecommunications Company) in 2004 also run by the Libyan government. Though Libya has many Internet service providers, all of the traffic to Libya, flows through this one provider, who controls access to all others, so when the Internet was shut down, this was the body responsible for it. Just recently, the Libyan Interim National Council, the temporary governing body of the revolution, set up a website at http://ntclibya.org/english/about/ in order to bypass the outages and ‗connect with our people at home and abroad, and to deliver their voice to the outside world.‘ Table 1-3 is a list of some of the other government service providers followed by hosting services and their domain names. (Source: http://www.libyalinks.com/dir/libya-internet-service-providers)

Table 1-3 – Libya's Main Internet Service Providers

Service Provider	Description	Domain
Libya Telecom and Technology (Government)	Internet services, GSM network and VSAT connections. They provide news.	ltt.ly
Al Falak Internet Services (Government)	Provides networking and Internet services for businesses in Libya	alfalak.ly
Libya DSL (Government)	Internet service provider in Libya	libyadsl.com
Barneeq IT and Telecommunications (Government)	Offering satellite Internet connectivity services to users in North Africa and Middle East in addition to other Internet services.	barneeq.com
Global Telecom Services Company, Libya (Government)	Satellite broadband internet service provider in Libya and the entire North Africa region.	gtsc.ae
Libyan Spider Network (Government)	Offers hosting and web design services in Libya. Also provide .ly domain registrations.	libyanspider.com
Multimedia Technologies Center (MTC), Libya (Government)	Offers hosting and web design services, domains registrations, web hosting, live chat and more	mtclibya.com
PC Libya (Government)	IT experts and web design team, providing professional web development and web hosting services.	pclibya.com
Hadia Group (Government)	Web page design and hosting, advertising and printing in Libya.	hadia.net
Almada Info Systems (Government)	Web hosting and Design Company in Libya	al-mada.net
Ly Hosting (Government)	Offering a variety of web hosting solutions and packages	lyhosting.com
Libo Hosting (Government)	Offers several hosting solutions.	libohosting.net
Virtual Dimensions Inc. (Government)	Hosting and Internet solutions provider	vdilink.com
Libyano Web Hosting (Government)	(Government) offers a variety of flexible managed hosting solutions in Libya.	libyano.net

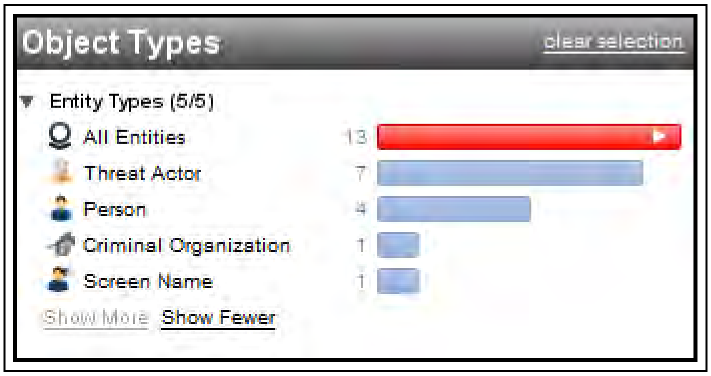
2. LIBYA’S CYBER OFFENSIVE AND DEFENSIVE CAPABILITIES

2.1 Introduction

Libya‘s IT and security industry are still not yet fully developed in comparison to countries like China and the United States, for example. For this reason, their ability to address cyber concerns, their methods and approaches are important to review. In 2005, Libya looked outside its borders (outsourced) for assistance in regards to suppressing on-line dissidents (ANHRO, 2006). It is possible that as Libya seems to lack the highly technical systems and experience that other countries have, an option in regards to cyber defense/offense is that Libya would either hire rouge hackers to exploit enemy systems or find the method internally to launch cyber-attacks against those they perceive as threats. This section discusses some concerns in regards to some of Libya‘s future cyber defense options as well as various hackers and groups known to support the country.

One of the concerns was that nations like Libya, which are normally incapable of competing either militarily or economically with larger international powers, could potentially leverage cyberspace and attack the critical systems of other state targets. Others worry that Libya may still have significant ties to terror groups or actors, such as private companies or criminal groups, with little or no-geopolitical connections, who could act as an intermediary in regards to launching cyber-attacks. It could even be possible that a Libyan sponsored terror group, with connections across the globe plan new "physical" attacks, calls to "cyber-jihad", proselytize, and create social bonds that are necessary for radicalization and recruitment.

In looking at these possibilities, CSFI did discover Libyan cyber supporters who do have access to reliable exploits in which to infiltrate a specific target, and also a working knowledge of cyber operations and how to automate these exploits. CSFI has identified more than 10 Libyan hacking groups that are both directly engaged in hacking activities in support of Libya and at least one publically verified group that claims ties to jihadist activities against the west. The most publicly known actor from these activists is iraq_resistance a.k.a. iqziad (Founder of Tarek Bin Ziad Group). Iqziad has been engaged in electronic jihad and is reported to be the creator of the ―Here You Have” Virus, which infected major corporations including Google, NASA, AIG and others. CSFI believes that the language used by iraq_resistance when writing the virus was VB6. Iqziad also claims to have created a ―virus” that ―deletes” AVIRA Anti-Virus from a Windows machine.



Object Types

▼ Entity Types (5/5)

All Entities	13
Threat Actor	7
Person	4
Criminal Organization	1
Screen Name	1

Figure 2-1 – Palantir Investigative Dashboard depicting Hacking Entities in Libya

These groups communicate through Yahoo Messenger, IRC channels and the standard Internet technologies with sporadic encrypted communication channels. Iraq_resistance, for example, was able to create a channel on YouTube to further his mission and recruit individuals.

It is also worth noting that the Libyan government may have recruited and influenced Serbian internet users to support Libyan President Gaddafi. Activists from Serbia have launched pro-Gaddafi movements on Facebook, Twitter, Myspace and other social networks, and Serbian hackers are trying to bring down the opposition's websites, according to the Libyan Youth Movement (LYM) (Speartip LLC, 2011).

The Libyan cyberspace may become fertile soil for malicious code development, cyber mercenaries, jihad recruitment, and the multiplication of hacking groups, especially if the international community does not step in to help regulate and stabilize their cyberspace. Many of these hacker groups are pro-Gaddafi due to religious and financial motives.

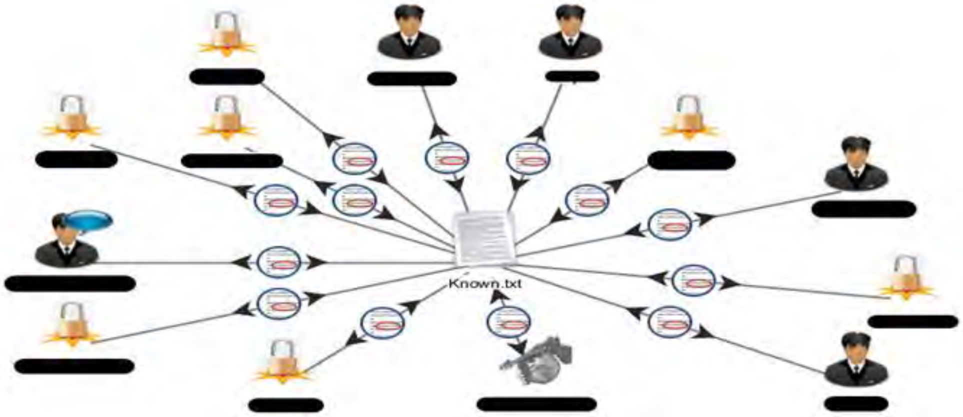


Figure 2-2 – Entity Threat Level based on Historical Evidence and Known Skill

2.2 A Call to Cyber-Jihad

The following is an example of how organized, pervasive and committed to cyber jihad some of these hacker groups are. Recently, the group Tariq bin Ziyad has posted a call for jihadist candidates on the osoud website. This information is relevant because it demonstrates an example of a terrorist/jihad group that supports Libya and is specifically using the internet to create cyber warriors for the purpose of launching on-line attack against U.S. systems. It also calls for members to communicate via the Internet via Yahoo Messenger and MSN, which has proven to be a powerful and instant method of coordination. As a pro-Libyan group, though a backdrop to recent events, they are a relevant piece of how allies to a cause, nation or government can become a serious cyber threat. Just as organized crime groups have hired hackers, it is possible that nation states could hire or distantly support jihad networks and launch cyber-attacks through them.

Here is a translation from Arabic of the call posted by the Tariq bin Ziyad Brigade:

Peace be upon you my brothers (اخواني عليكم السلام)

~~O~~ur group was established in the name of al- Tariq bin Ziyad, and the goal of this group is to infiltrate American systems that belong to the U.S. Army. The group is recruiting new members to enhance its capabilities and to increase its effectiveness. In order to join the Tariq bin Ziyad electronic jihad group, candidates must meet certain requirements and must also make a few pledges:

- The candidate must have the goal of electronic jihad and promises not to use the techniques and skills learnt here for any targets other that those belonging to the U.S. Army.
- Loyalty and respect for members of the group, respect for seniority and effectiveness; and only seniority and effectiveness gives way to leadership roles in the group and its subgroups.
- Intergroup meetings and communications is to be done using Yahoo Messenger and MSN.
- Problems and complaints shall be addressed to the General Commander of the Brigade.
- The level of expertise of the candidate is not important as they will be trained by the group, the learning is not difficult, but the tools taught are effective.
- It is imperative that candidates follow the guidelines and directives of the General Commander, and shall have full loyalty to him and work with devotion for the sake of God.
- Candidates must ignore and dismiss any misunderstandings between them, and to only compete against the enemy and not against each other.
- The swear-in and pledge of allegiance to the group shall be recorded and will be heard by the General Commander.

Finally, we ask for God‘s help and guidance, and we hope you will join this noble cause. We also thank the Administration of this forum [www. ousoud. net] for allowing us to post this call, and we will keep you posted firsthand with the results of this campaign.

To join us, please add the Yahoo ID [redacted]

Awaiting your joining the group,

Your brother General Commander of the Brigades Tariq bin Ziyad

(اخوكم القائد العام لكتائب طارق بن زياد)”

Iraq_resistance, tarek_bin_ziad_army (http://www.osoud.net/vb/showthread.php?t=30779)

Posted on June 10th, 2008 and last updated on November 22, 2008. The ousoud (Lions) web site claims to be an Arab, Islamic and International network that includes the best and most modern internet forums. Their slogan is ―Arab lions, our eyes are Arabian”

2.3 Malicious Code Activity in Libya

This particular portion of Project Cyber Dawn was completed in cooperation with Unveillance, a company specializing in Data Leak Intelligence, in order to give the audience a clear picture of malicious traffic within Libyan cyberspace. Unveillance works specifically to provide real time intelligence in regards to identifying (for the purpose of eliminating) computer attacks and botnets. In the wake of increased cyber-attacks aimed at governments, military institutions and the commercial space, this type of information is valuable in that it gives rapid updates and information concerning security breaches and threats (Unveillance, 2011). In regards to Libya, this information indicates how vulnerable Libya might be to cyber-attacks and provides a snapshot of its security level which could be valuable data for any government or industry.

According to the information gathered, Libya is a country with a Data Leak Intelligence (DLI) Score of 150+ (HIGH). The scale used for this model is:

Table 2-1 - DLI Threat Levels

DLI Score	Ranking
[<1]	Low
[1-25]	Guarded
[25-75]	Elevated
[75-150]	High
[>150]	Severe

As the DLI Score (the number on the left) declines, the greater the security and, as it would follow, the higher the DLI Score, the lower the security is for the particular company, government or country. According to Unveillance, ―The DLI Score allows a simple-to-interpret, comprehensive metric to instantly evaluate aggregated networks of a country, industry sector, sub-sector, corporation, government, university, and more. DLI Scores are updated near real-time as the security state of an organization improves or declines" (Unveillance, 2011).

Libya has a DLI Score of 150+ which according to this study, indicates that it has relatively low security and is open to breaches and attacks. This score is defined as ‗severe‘ with ―extreme number and/or severe threats identified with a high probability of data loss and malicious APT activity and propagation as well as multiple compliance failure" (Unveillance, 2011).

The data below has been collected in partnership with Unveillance. The graphics represent the analysis of thousands of network nodes in Libya

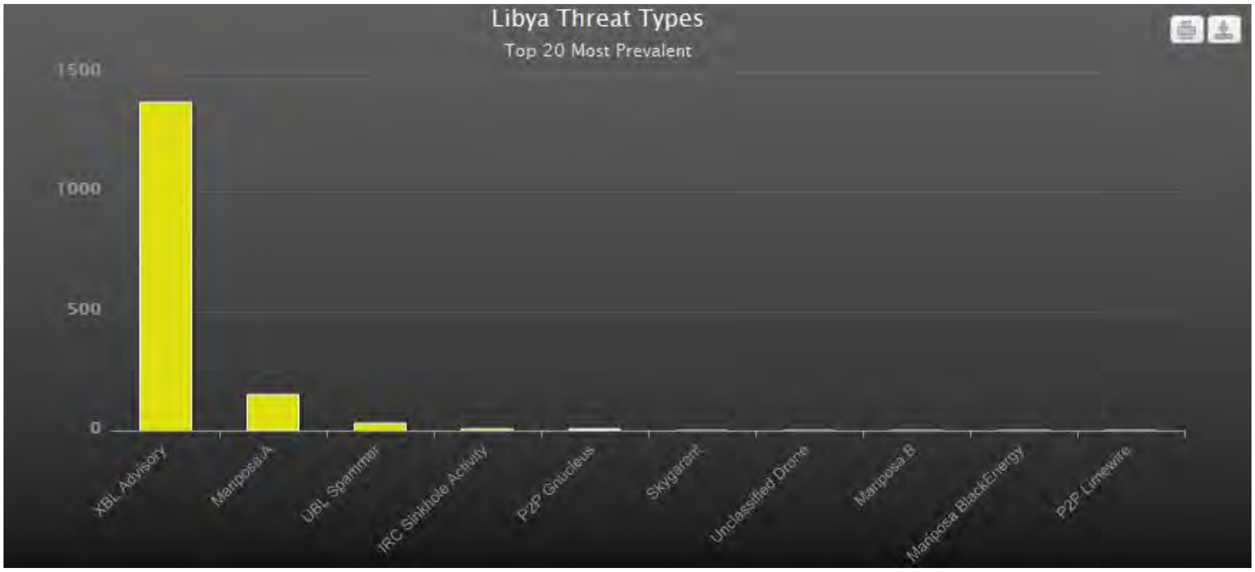


Figure 2-3 - Libyan Malware Activity (February 1 – April 13)

―In the midst of the 2011 Libyan uprising, coalition forces announced the launch of Operation Odyssey Dawn on Saturday (March 19).

The uprising began on or around February 15 and took a serious turn on February 17, picking up momentum in eastern Libya. Much like the uprising in Egypt, where the then standing Egyptian government attempted to use a complete shutdown on the Egyptian internet as a ploy to slow the growing revolution, the Libyan government appeared to be using the same playbook and reportedly began to shutdown portions of the Libyan internet.

Beginning on February 17, 2011, the landscape of malware activity normalcy began to dramatically shift with an increase of hourly counts of both unique public hosts and total malware events originating from sinkhole/tarpit-derived malware. During the first couple weeks of the uprising, the malware event activity dropped 61.63%, and unique host activity counts dropped 34.25% with a few periods of total silence lasting only a few hours. Starting on March 3, the overall malware event activity became very erratic, dropping a stunning 88.93% compared to activity up until and on February 17 with unique host counts dropping 70.03% over the same time period" (Unveillance, 2011).

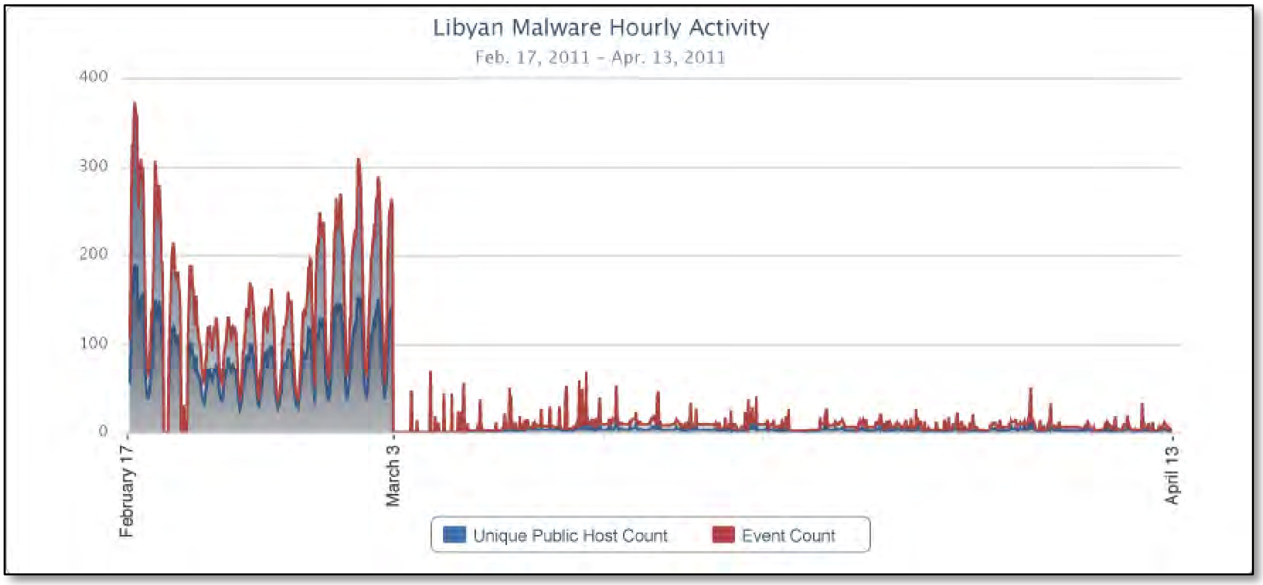


Figure 2-4 – Libyan Malware Hourly Activity (Feb 17 – Apr 13)

Dramatic differences in Event Counts, Unique Host Counts, and Average Events per Host are all evident post the February 17 timeframe.

Table 2-2 - Libyan Malware Activity Breakdown (Feb 1 - Apr 13)

Range	Events per Host Avg.	Unique Hosts	Total Events	% Change Post Feb. 17
Feb. 1 – Feb. 17	74.78	981	73,363	-
Feb. 17 – Mar. 3	43.64	645	28,153	61.63% reduction
Mar. 3 – Apr. 13	27.60	294	8,116	88.93% reduction

Following the March 3 internet shutdown by the standing Libyan Federal Government, all malware activity appears to be predominantly from hosts that are centered in or around Tripoli—evident in the map below.

This information not only reflects the high risk of cyber-attacks that Libya is vulnerable to, but it also reinforces the unique pattern that Libya had in regards to how it shut down the internet. This data would suggest that activity slowed between February 17 and March 3, but after that there was a severe decline in traffic. There were still events in the Tripoli area however, which would indicate that some sites still had connectivity.

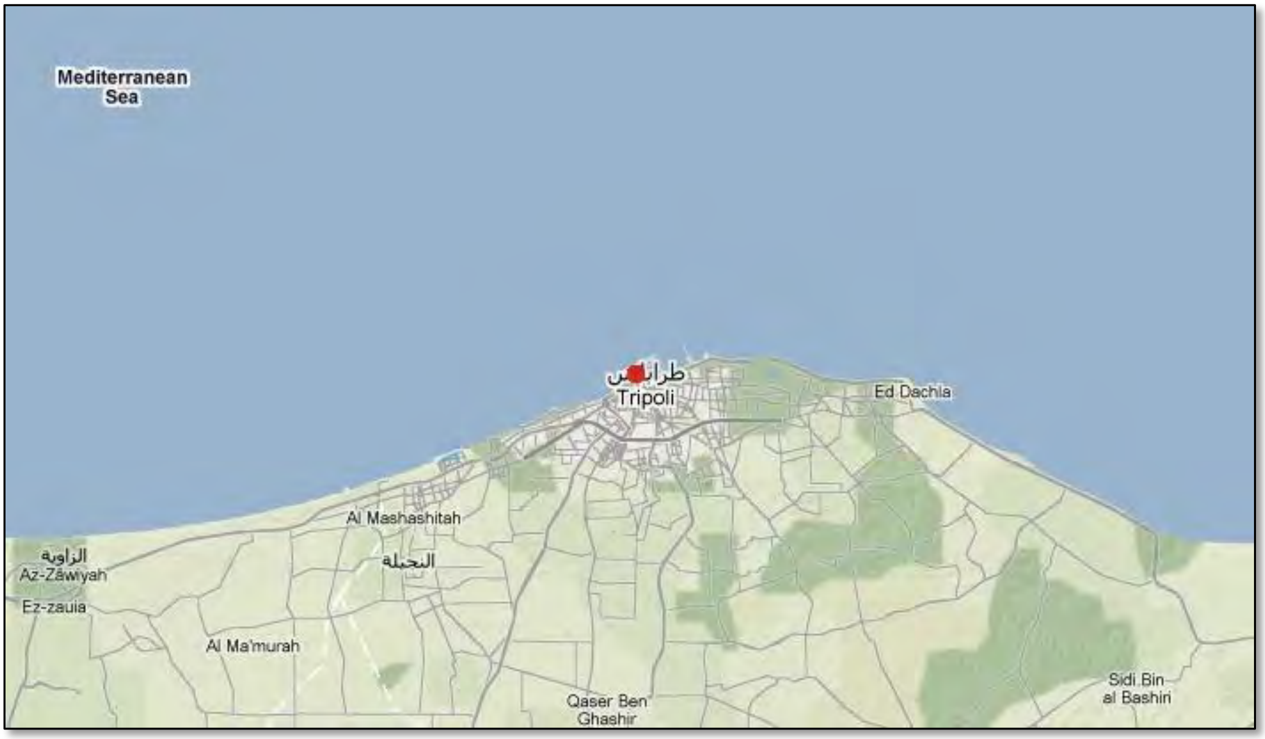


Figure 2-5 – Malware Traffic Localization

It is interesting to note that the top five hosts (out of a total of 294) generating the most malware traffic since March 3 make up 70.24%, or 5,701, of the total events since March 3. All of the top five hosts share the same IPv4 Prefix [redacted] and AS in AS21003.

Table 2-3 - Top 5 Malware Generating Hosts since March 3

IP Address	Hostname	IPv4 Prefix	Total Events	% Events Post Mar. 3
[redacted]	[redacted]	[redacted]	2,327	28.67%
[redacted]	[redacted]	[redacted]	1,524	18.78%
[redacted]	[redacted]	[redacted]	1,049	12.93%
[redacted]	[redacted]	[redacted]	548	6.75%
[redacted]	[redacted]	[redacted]	253	3.12%

Concentrating on the number one host/gateway by total events since March 3 ([redacted]), all events from the host are indicative of a Mariposa.A (Microsoft Win32/Rimecud) infection. Taking a quick look at the reverse DNS address of [redacted] reveals [redacted].ly.

It is not surprising that the host is infected with Mariposa as its derivative botnet is still quite alive and kicking, evident in the map below, which is a snapshot of all global malware activity with a signature of Mariposa within a two second range of data upon generating the dataset.

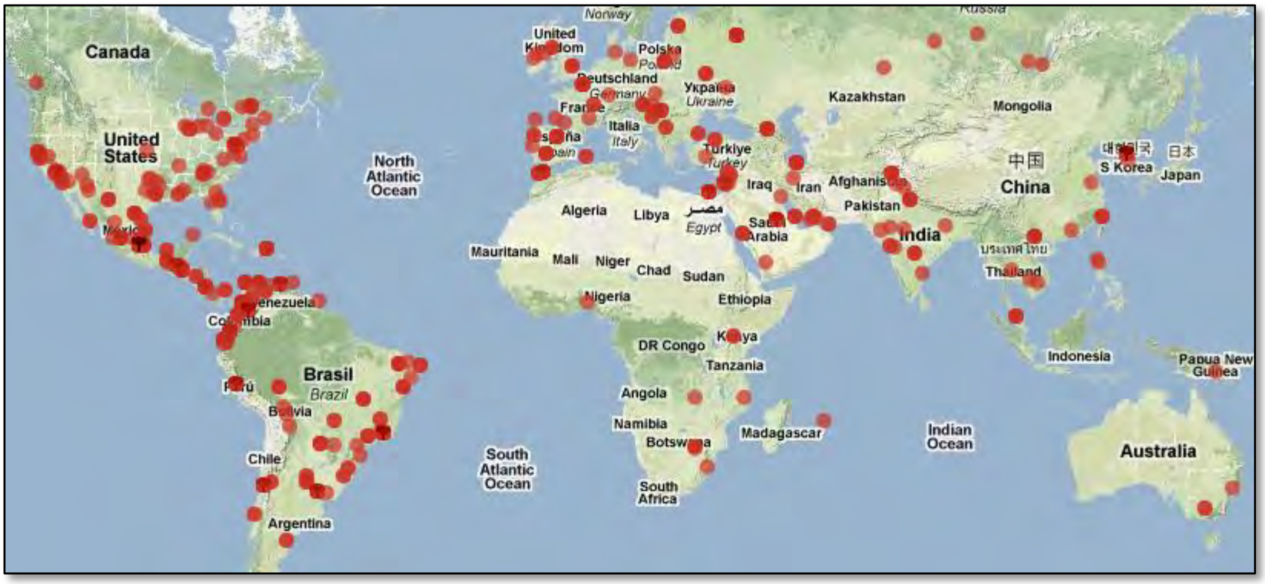


Figure 2-6 – Global Mariposa Malware Signatures

-Mariposa is Spanish for butterfly. In computer lingo, Mariposa is a botnet created by the Butterfly bot kit. Mariposa is typically spread via instant messaging (usually MSN/Live), peer-to-peer file sharing networks and as an autorun worm. Mariposa steals usernames and passwords and harvests email addresses from infected systems. Mariposa bots may also be directed to launch Distributed Denial of Service (DDoS) attacks" (Landesman, 2011).

Understanding Libya‘s security level in regards to the types of attacks and where they are located is significant in assessing how secure other areas of Libya may be and taking steps to mitigate the threats.

3. LIBYA AND IT INVESTMENTS

3.1 Introduction and Background

Though Libya has not always been on friendly terms with the international community, was on the terrorist watch list and was pursuing a nuclear program despite having signed the Non-Nuclear Proliferation Treaty, at the end of 2003, Libya began making significant strides to become a viable economic force by investing in the growth of its infrastructure and increasing foreign business partners. As part of this goal, Libya has had to shift policies, denounce terrorist activity, get rid of its WMD program and cooperate with the other nations to demonstrate its commitment toward trade, trust and transparency. In order to attract new business ventures, Libya became determined to build its IT sector and also started to increase communication networks and provide access to the Internet as part of encouraging ties with the international community. By taking steps to become a more open economic partner, Libya also became exposed to the risks that accompany increased internet access and computer use including cybercrimes and attacks.

Over the years, Libya has continued to make progress toward its goal of creating viable global business partners and developing its It sector. Some notable dates include:

- September 20, 2004 -, President George W. Bush signed an Executive Order ending IEEPA related economic sanctions This made it possible for U.S. companies to invest in and conduct business in Libya.
- In 2008, The Libyan Investment Authority, a government run business that oversees government investments was formed. This fund is particularly important because it ~~c~~ontrols at least $70 billion in fixed assets and reserves. It has invested the bulk of its money in European banks and businesses, including Dutch-Belgian bank Fortis, Italian bank Unicredit, the Pearson publishing empire, Italian defense firm Finmeccanica SpA, an oil-production sharing agreement with BP and even a slice of the Italian soccer team Juventus" (Huffington Post, 2011). In regards to seeking opportunities to advance the IT sector, Baram reported that "some of the advantages that Layas saw the U.S. having over European competitors for contracts in Libya are the weakness of the dollar compared to the euro, as well as U.S. access to more advanced technology" (Huffington Post, 2011).
- November 2008, ThurayaIP, in partnership with the General Post and Telecommunications Company in Libya, started to install terminals to be used in key areas across the country including government agencies, international companies within the region, gas and oil companies—an indication of Libya's commitment to continued growth (Thuraya, 2011).
- In 2010, HP announced plans to open IT sales and support locations in Libya just shortly after Vodafone and Libya's national mobile company, Almadar Aljadid, entered a joint non-equity

Partner Market agreement to provide foreign businesses opportunities, better support and connectivity (TechnoLibya, 2011).

It is expected that in 2011, Libya will list at least 30% of Al Madar and Libyana, originally 100% owned by the Libyan Government, on the stock exchange. They are just two of 20 expected firms to go public this year. (Libya News and Views, 2010)

These are just a few examples of how Libya has been pushing to increase advancement in the IT sector as well as foreign investment and partnerships, but there are others. According to one report, ~~In~~ternational companies (Alcatel, Siemens, Ericsson and Nokia in particular) are already doing business in Libya. Many opportunities in Internet and data processing are available to small businesses. For example, some $15 million will be spent to install a data-processing network connecting Libyan banks. Demand for equipment and services relating to ICT in the public sector is growing in the framework of an ongoing master plan for networking strategic public services and the private sector, in particular foreign oil companies, which need appropriate infrastructure to carry out their projects." (Anima, 2011)

Other foreign tech companies that have had a strong presence in Libya include LG, Alcatel Lucent, Samsung and Huawei, and the numbers and interest from foreign markets has increased since Libya, in a push to increase competition in the wireless market and to encourage growth, actively sought bids from foreign companies. As a result, tech giants like HP and Vodafone have created new partnerships with Libya One.

Partnerships with foreign firms are common in Libya, and many are mandated by recent changes in the laws regarding foreign investment opportunities. For example, one component relative to doing business in Libya is that recent changes in the law require that many investments in the country pursue a joint venture. So, not only does a foreign company need to find an internal partner, but it should also be aware the implications of such a partnership (US & Foreign Commercial Service, 2008).

The following is a list of 913 It companies doing business in Libya. The second is a list for connecting buyers with Chinese suppliers. This contains the type of Libyan business, the company name and a contact person.

A list of 913 Information Technology companies doing business in Libya:

http://www.adcbuae.com/directory/information_technology_companies_in_libya.html

A list of Libyan Companies, types and contact person (for Chinese suppliers)

http://www.made-in-china.com/global-company-index/Libya-5024-1.html (Made in China.com, 2011)

Some examples of foreign and domestic information technology companies and their range of services and customers include:

- Altaqnya
    - Libyan ITC market leader 2006
    - Partners: EMC, Keymile, Aastra
    - Projects: BOCD, Wehda Bank, Libyana Mobile Phone, LITC, Bank of Sahel & Sahara, Libyan Petroleum Institute, Veba Oil, Ras Lanof Oil, etc.
- Getronics Middle East
    - Information, Communication and Outsourcing Professional IT services
    - Headquarters Dubai – Office in Libya, UAE, Egypt
- Iratlel Group – Italy
    - Designs and installs multi service networks
    - 2 largest contracts with Libya, presence in Libya
- Ai-Ada Mutkan Networks
    - IT, Communications, Electric Systems
    - Security, Banking, Systems
    - 4 Locations in Tripoli and 4 in Benghazi
- Al-Manteq Company for Information Technology
    - IT company in Tripoli, Libya
    - Provides computer hardware and accessories, printers and maintenance services
- Al-Malak Information Technology
    - Software, hardware and information technology solutions in Libya
- **Microsoft Libya**
    - Local representative office of Microsoft international software company in Libya.

Further examples of dynamic partnerships that demonstrate Libya‘s push to drive technology as well as to create an economy that supports networking, foreign investments and connectivity are:

- Alada Smart Infrastructures – Building smart infrastructures and communication systems
- Nokia Siemens Networks and MoreMagic Solutions – Partnering w/LPTIC in mobile payment solutions
- Al Jeel Al Jadeed will be a distributor of Thuraya IP and Marine Services – Postpaid services
- SLIIT will set up a campus in Libya (Sri Lanka Institute of Information)
- Omnix International – BIM solutions
- Phoenicia Group rolls out BGAN Satellite Internet Technology in Libya
- Green Future Limited contracted by telecoms owned in part by LAP, the Libyan African Investment Portfolio to Rwanda, funded in part by the Chinese government

- IMS Libya is the result of a powerful alliance between Libyan Post, Telecommunication & Information Technology Holding Company (LPTIC) and Intelligent Mechatronic Systems Inc (IMS)
- Submarine Cable Partnership – WIOCC is a uniquely created African investment company, owned by 14 major telecom operators in Africa, including Libya. They receive funding from various global development finance institutions such as World Bank, AFDB, AFD and KFW (WIOCC, 2011)
- Huawei Marine to construct ―Silphium" fiber optic submarine cable under Mediterranean Sea linking Libya with Greece – This is the second large project Huawei has had with Libya in the past two years

The WIOCC cable partnership referenced above involves the creation of The EASSy cable, a 10,000 km fiber-optic submarine cable, the largest to serve the African continent. Joe Sloan, who represented the project financiers, the IFC and the World Bank said the completion of the EASSy submarine cable represents a major step forward in bringing the countries of the Eastern African Region closer together and closer to the rest of the world. ―The arrival of EASSy and low-cost access to the global communications network is a potential ‗game changer', which should benefit the region in the fields of business, medicine and education, and lead to improved employment opportunities" (IT News Africa, 2010).

A recent report by JBB Research indicated that Al Madar plans to adopt LTE and rush right into 4G, which, combined with the partnerships and push for information technology growth, puts Libya in a position primed to become a full global participant in the fields of IT, international business partnerships and thus connectivity (TechnoLibya, 2011).

Libya is also investing capital in its education, especially in the area of IT. Many foreign organizations have been encouraged to seek opportunities in regards to exchange programs, IT development, training and computer related equipment sales in the area of education. Libya announced in 2008 that it would spend over 5 billion dinars (a little over 4 billion U.S. dollars) for the advancement of learning with a concentration in the field of IT. In February 2011, just prior to the riots, Libya began distributing approximately 150,000 laptops to school aged children (Libya Investment, 2011).

Though Libya seems poised to push forward in the technology market, the recent unrest has caused some uncertainty and concerns with international business partners. From Abu Dhabi, 25th February 2011: ―Thuraya Telecommunications announced today that its mobile satellite communication services have been subjected to harmful and intentional interference in Libya over the past 7 days. The interference has affected both data and voice communications over Libya and some surrounding areas" (Thuraya, 2011). Microsoft too, has voiced concern over the recent disappearance of one of their employees working in Libya. In regards to the oil industry, ―Royal Dutch Shell has declared its decision of pulling away its workers from the troubled zone. The shares of BP have also suffered due to the political unrest, though it has only exploration business with the country. Italian oil and gas company, Spanish oil and gas company, U.S. independent oil and gas company Marathon Oil and Hess have either suspended oil operations, or are taking definite measures to reduce the percent of loss through its distributed operations in the war torn regions of Libya" (Best Growth Stock, 2011).

Another setback for Libya, as a result of the conflict, the United States has put a block on some of Libya's assets, –U.S. President Barack Obama's executive order freezing $30 billion in assets of Muammar Gaddafi, his family and the Libyan government could impact several U.S. banks and private equity firms, including Goldman Sachs, Citigroup, JPMorgan Chase and the Carlyle Group. The Obama administration described it as the largest seizure of foreign funds in U.S. history" (Huffington Post, 2011).

The current instability in the region, Libya's past tainted with links to terrorism and terror groups, volatility that comes with potential regime change, a ripe oil market, and Libya's push to develop and create new opportunities for information technology all create an atmosphere in the region ripe for increased cyber-attacks on its systems for the purpose of spying, hacking, stealing vital company information or finding and exploiting vulnerabilities in its infrastructure. It's newly opening borders will offer promise and challenge as Libya is forced to reconsider some it's policies and internal controls in order to foster business growth and opportunities for its citizens. Libya has grown substantially and with a rapid pace over the past years, almost compensating for its slow emergence into the market. These next ten years, depending on the aftermath of the recent unrest, are projected to reflect equal, if not more progression. This will be an important country to watch in terms of cyber development and IT capabilities, foreign markets, global stability and growth for Libya's infrastructure.

3.2 Are Cyber-Attacks a Realistic Concern?

As the uprisings in the Middle East have been drawing international attention, quietly in cyberspace, Chinese hackers were launching attacks against oil refineries. They were successful in breaching five. The attacks seemed focused on commercial gain, stealing drilling information, information about operations and equipment, bids and other financial records. Of particular concern, however, much like with the attacks on Google in 2010, these were focused, –coordinated, covert and targeted" and started sometime in 2007 (Telegraph, 2011). There may be some connections to a state or business sponsored attack as the hits all came during Bejing working hours. Attacks that have been on-going for three or four year without detection, suggest there may be more gaps experts do not know about, and other vulnerabilities that are currently under attack.

This past event is another clear example that attacks on critical areas such as oil refineries are possible and realistic. Today, governments are blocking Internet traffic as a part of conflict strategy. Soon strategy – or perhaps currently, as demonstrated by the oil attacks - may involve damaging the critical infrastructure of an opponent or hiring rogue hackers to weaken financial systems, destroy an electrical grid or shut down oil production. Brazil, Iran and the ‗Night Dragon‘ attacks have announced that cyber events against global infrastructures are not future concerns, they are happening now.

In regards to cyber protection for Libya, there are a handful of mercenary hackers and hacker groups that claim allegiance to Libya; however, their focus has been primarily on defacing websites, attacking perceived or real threats or as in the iraq_resistance, launching cyber-attacks against the United States Army and affiliates. Gaddafi seems to lack internal state supported hackers and Libya has a limited (though growing) IT sector. As Unveillance discovered, Libya‘s security is severe‘ with ―extreme number and/or severe threats identified with a high probability of data loss and malicious APT activity and propagation as well as multiple compliance failure" (Unveillance, 2011), so drawing upon internal reserves may not be the best option for Libya in regards to security. An article from 2005 mentions that Gaddafi has reached out beyond his borders in the past to Russia and Pakistan in order to address issues with anti-Libyan rhetoric and demonstrations on the Internet (Eid, 2005). The author, Gamel Eid writes, ―Oppositional websites, human rights websites, forums, news websites, and even literary websites—all of which are based abroad—soon followed in appearance. According to the groups behind these websites, the Libyan government has appointed one of the closest friends of the Libyan President Moussa Kosa to monitor oppositional websites and attempt to limit their growth. Moussa Kosa summoned experts from Russia, Poland and Pakistan to help block these websites. He forced owners of net cafes to place stickers on computers that warn visitors from logging onto websites deemed oppositional" (Eid, 2004). Though there is limited information in regards to these experts, Libya has a pattern of hiring forces outside of its borders for assistance as part of its strategic defensive capabilities.

Though many of Libya‘s cyber defense/attack resources seem to come from outside of Libya, recently there has been a push to provide school age children with laptops. 150,000 were distributed over the last year. There is also a tech school developing in Libya. This suggests that in the future Libya will be armed with access to greater talent and cyber savvy citizens. How this may affect the global community remains to be seen, but it would most likely be a prudent next step to quickly develop international consensus in regards to cyber activity, language, laws and accepted behaviors long before these cyber students develop into cyber specialists. That does not help Libya today.

This is a critical period for Libya in regards to securing its infrastructure, which, as a result of the current instability in the region, is at risk internally as well as externally. Libya differs from Tunisia and Egypt as it is an oil producing country; this political uprising has also been about controlling the oil. Internally, Gaddafi and the protesters have battled over oil, and in early April, the rebels gained enough control to deliver oil to an undisclosed location. This is just one indication of how volatile Libya remains in regards to its oil and gas infrastructure. Regarding cyber security, without a comprehensive plan for defense, Libya still remains vulnerable to penetration from cyber-attacks originating from outside its borders as well as those from within. It is clear that the computer has become a tool and a method for revolution and control in this particular conflict. It is not unreasonable then to wonder how it may continue to be utilized as the situation unfolds. Could knowledgeable rebel hackers attack the oil infrastructure? If Gaddafi does leave, would a mercenary hacker group launch a cyber-onslaught against Libya?

Georgia/Russia, Estonia, Iran, and Brazil have all experienced the effects of cyber-attacks in specific and focused ways. In February, 2011, Chinese hackers attacked five oil refineries and were successful. The reality remains that the world is experiencing successful attacks against nations and infrastructures of varying degrees and purpose. The question is, are the world governments prepared to address the threats related to these growing trends? Is Libya?

The next few sections will examine some of the potential threats to the Libyan infrastructure, will look at mock attack scenarios and how these attacks could potentially devastate Libya and harm some of the other actors in the international community.

The following pages will also give specific attention to SCADA and how vulnerable this area is in relation to security within Libya as well as the rest of the world. Recently in Iran, when one of its nuclear facilities was compromised by a worm, it became clear that cyber-attacks are developing at a rate faster than some of the vital areas of concern are being updated. The conversations today about supervisory control and data acquisition systems (SCADA) and the STUXNET worm are extremely relevant and highly related to potential gaps within Libya‘s infrastructure, leaving the oil and gas industry exposed as well as potentially critical infrastructures around the world.

3.3 The Potential Impacts of Cyber-Attacks on the Libyan Oil and Gas Industry

Much like with Georgia/Russia, the trend represented in the Middle East is that conflict and the computer are increasingly interconnected and that cyberspace is an important element in regards to conflict strategy. The lines too, have become blurred in regards to the threat level associated with the actor launching an attack. Threats are no longer contained to nation against nation or coalition against a nation. One hacker or a small group, located across the globe is an equal if not more dangerous threat, as their motives and methods may lie further under the intelligence radar. This introduces other possibilities which include ‗hacker for hire' in which a state or organization may hire a skilled operative to create and launch attacks.

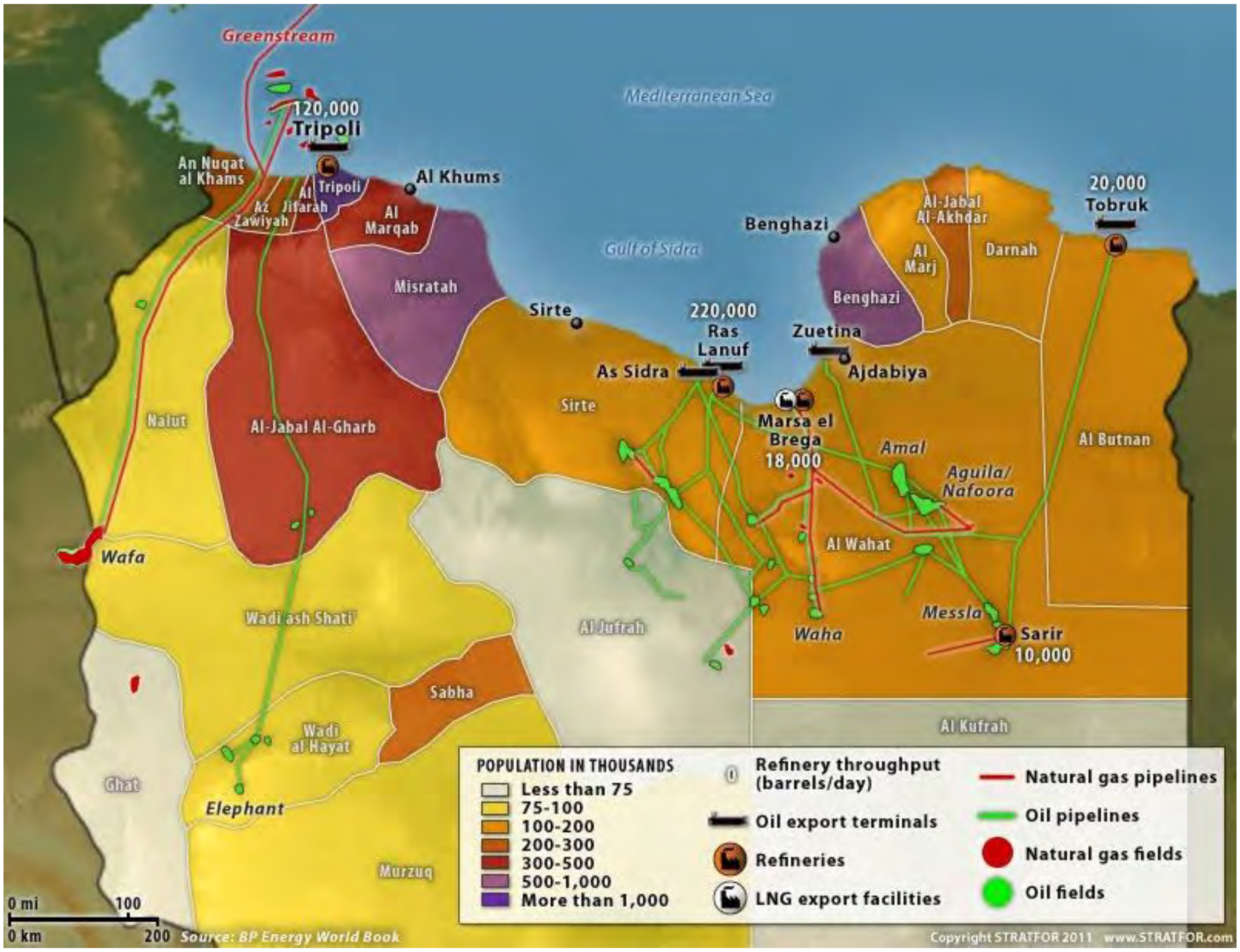


Figure 3-1 – Libya's Population and Energy Production

In regards to the Libyan Civil War and its vulnerability to cyber-attacks against its infrastructure, this report will explore three scenarios as a model for what could occur. Scenario analysis is an approach that can help individuals to visualize various outcomes and possibilities for the purpose of making informed well-rounded decisions. It is a method used by competitive intelligence professionals, businesses; military and political analysts and can open up thinking, discussion of a wide range of potential futures and provide added tools in which to plan how to address worst-case challenges if they should arise.

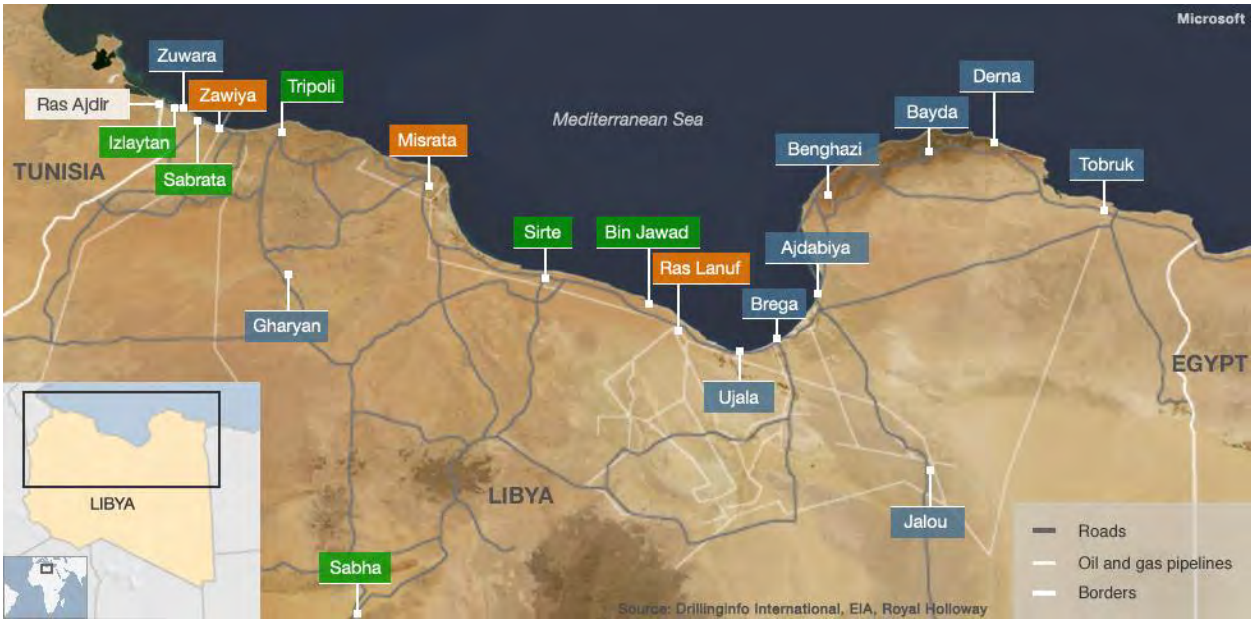


Figure 3-2 – Road and Pipeline Infrastructure in Libya

<u>**Scenario One**</u>: In this scenario, the Gaddafi regime has crumbled. Gaddafi and his supporters have lost control of Libya and a new government is in place. Either Gaddafi, or someone close to him, refuses to watch others reap the benefits of Libyan oil, so Serbian (maybe) hackers are hired to cripple the infrastructure in Libya from within. The aim is to control the oil fields, pipelines and energy sector. The weapon of choice: the STUXNET worm or something similar. The attackers would assume control of the Libyan oil industry and critical power and electric stations.

Vector of Attack: STUXNET worm to gain control of systems.

Another possibility is that Gaddafi has already put systems in place so he can take control remotely. Like Russia, Libya may collect all Internet data on citizens and internal information/controls on businesses and telecoms, and Gaddafi may still have allies willing to help him out.

Potential areas of vulnerability: Siemens has been noted to be a gap in security since the discovery of the Stuxnet worm. –Specifically, the malware uses the Siemens default password of the MSSQL account WinCCConnect to log into the PCS7/WinCC database and extract process data and possibly HMI screens” (Dow, 2010). Siemens is well integrated into the Libyan infrastructure and could be a first line of attack for an actor seeking an area to exploit. In 2010 Siemens Libya started projects in the industry and energy sectors. (Ahlia Cement Company, Great Man Made River Project, Renovation of gas/power supplies at Benhazi, Misurata and Zwitina power plants) (Siemens, 2011).

Vector of Attack: Stuxnet worm to gain control of systems

Scenario Two: The conflict is over, and a new government in place. This cyber-attack against Libya is not done to cripple Libya as much as it is done by rogue hackers, perhaps Al Qaeda or a nation-state as a test or to send a message. The real targets could be larger countries, such as the United States or China or the oil industry as a whole. Libya is just a pilot to prepare for larger enemies. Since Libya has been in turmoil and will be unsettled and in transition for a while, it will not be focused on quality checks to the infrastructure. With a transitional government, finding and exploiting gaps in the infrastructure may be easier here as opposed to a larger target. Hackers would aim at critical space such as power generators, air traffic control systems, oil, gas, electrical grids and the water and sewer lines. Similar approaches could follow the attempts in Brazil, Georgia, Iran and the Korean DDoS attacks.

The following blog outlines some of the components to STUXNET:

http://www.symantec.com/connect/blogs/distilling-w32stuxnet-components

3.4 Other Alternate Futures

Other interesting alternate futures to apply to a wider more complete scenario analysis or future studies can be found at https://www.recordedfuture.com/rf/?ts=1303084571962 and http://blogs.forbes.com/energysource/2011/03/28/europe-and-the-endgame-scenarios-for-intervention-in-libya/?partner=relatedstoriesbox

3.5 Some Implications in Regards to Oil, Gas, and International Cooperation

One essential question in each of these scenarios is could these attacks impact oil and gas prices? This a fundamental issue in regards to global economic security. Conflict and confusion can and often does impact buyer and investor confidence and thus, the stock market; however, oil and gas prices are part of a much larger discussion and can be difficult to sort out even by experts. Regardless, it can be helpful to look at certain key points in regards to this issue as well as other implications related to an attack on Libya‘s infrastructure as well as how this could affect other countries.

As reflected in the recent spikes in the market, oil prices did increase during the early stages of the Libyan crisis; however these leaps seemed connected to the perception of the risk associated with the conflict rather than the real, direct impact to oil reserves in the world. If the case of a cyber-attack, if the threat could be immediately contained or minimized so that the world could see that the attacks were limited to Libya and not the oil fields of the world, then most likely prices would leap, but eventually stabilize. If not, if the perception or reality was that the attackers had the ability to freely attack any and all national infrastructures, compromising global oil reserves, then prices would most likely be impacted for a long time, but, at that point, international security would be threatened and the attack could be tantamount to a declaration of war on a global scale as opposed to a regional or national scale. Perception and scale would dictate much of how the world would respond.

If the attack was not announced or if it could be contained and shut down, the country that would be primarily harmed would be Libya. First, Libya may not recover well from its 2011 crisis in regards to oil trade. Some experts compare the current events to the situation with Iraq after it attacked Kuwait. Both countries suffered in regards to oil production for years to follow. Also Libya would most likely be impacted the hardest by any attacks to its infrastructure because oil accounts for 95% of Libya‘s export revenue and 80% of the government earnings (Frayer, 2011). Italy and Europe would also be affected as one fourth of Italy‘s oil demand is supplied by Libya, but there are enough world oil resources to prevent a global oil or gas crisis. Other trade partners would be affected eventually and the opportunities for investment from the foreign market could also be compromised.

In looking at the United States, it is not dependent on oil from Libya. Currently, a fifth of Libya‘s oil production has been halted (Frayer, 2011) and though prices of oil have increased, the United States still has significant reserves. Furthermore, again in regards to oil and gas prices, the nation with the most oil is Saudi Arabia with reportedly more than 250 billion barrels. Iraq, Iran, Kuwait and the UAE and Canada also hold large reserves. (Canada has the second largest amount in the world). Other countries with oil include Venezuela, Libya, Indonesia, Mexico and Nigeria, Brazil, China and some EU nations (Gethard, 2010).

Oil is usually purchased and sold on the futures market through the NYMEX, Globex or through the Intercontinental Exchange (Gethard, 2008). Pricing can be impacted by OPEC, and other shifts in the market. Instability can impact pricing, but again is often as a result of perception or confidence rather than availability of supplies (Fell, 2011).

It would take time and money to address cyber-attacks against the Libyan infrastructure, however the implications of the attack in regards to its scale, its success, the ability to track the attackers, the type of attack, the legal, international and global policy issues that would be impacted would most likely be of greater significance and would be a top concern in regards to national and global security than potential slight increases in oil or gas prices. However, it is important to consider if there is a major breach to the oil or gas industry and it seemed likely that the world reserves were vulnerable, then not only would pricing and future availability be a concern, but it would be essential to have the means to immediately triage/assess the damage and potential future risks to Libya and the rest of the world.

One immediate step would be to determine the current threat to global oil reserves, infrastructures, financial sectors and nations. Could the actor/hacker repeat an attack elsewhere, is it systematic and controlled and does the international community have the necessary tools in regards to disaster mitigation, the ability to immediately protect other vulnerable areas, locate the attack, then respond accordingly in order to contain the threat and deter possible future events? This type of threat has local, national and global implications and as reflected earlier, actors are moving quicker than state and national governments, who can be slowed down by varying degrees of bureaucracy.

Another concern in this regard is that nations on a local and international level are not prepared to address the many issues surrounding cyber-attacks whether they are launched against individuals, institutions, businesses, infrastructures or nations. Today, a majority of cyber events cross international borders, exponentially complicating the time, effort and coordination to address and limit attacks of any kind, not to mention on an electrical grid or nuclear facility. This is important to look at in relation to Libya, who, in the past has hired support from other countries to address cyber concerns. How would it respond to a major attack against its oil or gas infrastructure? Gaddafi‘s forces have already demonstrated the extent they will go to protect these areas. It could be possible that Libya, without a significant number of sophisticated IT resources, would hire cyber mercenaries to locate and eliminate the source of the attack. What would be the repercussions of such an attack? Could this type of response become the norm for some countries or eventually develop into state-sponsored cyber terrorism?

The following example does not represent an attack against a grid or infrastructure, but it is included to illuminate some of the challenges the international community faces in regards to prosecution and deterrence in relation to cyber-attacks. This is relevant to the discussion at hand because without a structured plan of recourse, legal or policy remedies, if key sites in Libya or anywhere in the world are targeted, then it very possible that the country attacked will find other methods to protect itself, which in relation to the cyber space could be potentially detrimental.

One example of the challenges in regards to deterrence and prosecution involves the Mariposa botnet, the type of malware discussed earlier in this study. This was an attack launched for financial gain; however the situation can be applied to attacks against critical infrastructures as well in regards to deterrence and international coordination and cohesion. Brian Krebs blogged that in March,2010 three of the individuals responsible for creating and distributing the Mariposa botnet were apprehended in Spain. They ~~s~~tole directly from victim bank accounts, using money mules in the United States and Canada, and laundered stolen money through online gambling Web sites” (Krebs, 2010). Unfortunately, ~~In~~ Spain, it is not a crime to own and operate a botnet or distribute malware. So even if we manage to prove they are using a botnet, we will need to prove they also were stealing identities and other things, and that is where our lines of investigation are focusing right now” (Krebs, 2010). At that time, Spain had signed the Council of Europe‘s cybercrime treaty, but Spanish legislators had not passed the corresponding cybercrime laws in Spain, illuminating another gap in deterrence and prosecution.

Targets included those in the U.S. and Canada, but the law (or lack thereof) protects the perpetrators in Spain, just one of the challenges that the international community faces today. On the very basic level, there still lacks common language in regards to cyber incidents, so it begs the question how will the world nations coordinate quickly on deeper more pressing issues in a timely and relevant manner?. There lacks a cohesive, but necessary approach. Hackers and cyber-attacks will not wait for law and policy makers, governments and institutions to work together.

In most countries, the gain of cyber sabotage far outweighs the costs and hackers may assume if they do get caught, they will not face prison time. This extends to political hackers, jihad hackers and state sponsored actors. To look at another possibility in relation to Libya, in the past they have hired external hackers (outsourced), from Russia or Pakistan to control problems with Libyan cyber dissidents. If Libya were to return to a terrorist sponsored state following the potential overthrow of Gaddafi, then, as a result of their limited IT functions, they, and other smaller nation states may become aggressors in this growing threat landscape, from stealing intellectual property and national secrets to launching covert attacks on power facilities and electrical grids. These are essential concepts to prepare for today.

Recent reports have indicated that the national infrastructures of the United States and China may be at risk. The true concern is that the world is not ready to witness or experience a true example of cyber warfare aimed at the Libyan infrastructure, China, the United States or any other country for that matter. Oil and gas prices are a significant concern to the international economy, but our global security is threatened on a more crucial level when individuals, governments or terror groups have and can demonstrate the power to cripple a nation‘s infrastructure.

3.6 CERT – A model for possibilities

If a cyber-attack is launched against a critical area of Libya‘s infrastructure, one potential resource that Libya has at its disposal is CERT, (Computer Emergency Readiness Team). Based on its history of hiring hackers and mercenaries to address cyber problems, it remains to be seen whether Libya would rely on assistance from CERT or not. According to the Carnegie Mellon Website, ―CERT is an organization devoted to ensuring that appropriate technology and systems management practices are used to resist attacks on networked systems and to limiting damage and ensure continuity of critical services in spite of successful attacks, accidents, or failures" (Carnegie Mellon, 2011). Cert was developed in was formed by the Defense Advanced Research Projects Agency (DARPA) in November 1988 after the ‗Morris Worm‘ attacked and disabled the Internet.

The only CERT centers in proximity to Libya are in Tunisia (TunCERT) and Egypt however; it is likely that Tunisia's CERT, TunCERT, is probably NOT an option at all for Libya. Libya has not developed a structured approach to Cyber Security and though Libya uses U.S. based hosting for its "sensitive" sites it is most likely that Libya will rely on a few hired cyber security companies to fend off attacks. For example, Serbian companies currently hired for hacking activities will likely also be the "CERT" of Libya.

Libya is a full member of the OIC-CERT (CERT of the Organization of Islamic Countries, (http://www.oic-cert.net) a "consulting" forum based in Malaysia, but with no real technical activity. Libya is not in the steering committee of OIC-CERT, (http://www.oic-cert.net/mmb_listofmembers.html) however, Libya is represented in OIC-CERT by its Centre for Economic Information and Documentation, Ministry of Economy, Trade and Investment.

OIC-CERT is supposed to provide cyber emergency channels among member countries; however there is no trace or indication of it doing that. The CERT of the country of Malaysia, however, is very active and technically-able. Its headcount exceeds 240 people. (OIC-CERT, 2011).

Bullet points in regards to OIC-CERT (OIC-CERT, 2011).

- In June 2005, The formation of CERT among Organization of The Islamic Conference (OIC) member countries was proposed during the Annual Meeting of Islamic Development Bank (IDB) Board of Governors at Putrajaya, Malaysia.
- Amongst its other mandates, the meeting was tasked to initiate the establishment of a Task Force in cooperation with leading OIC member countries to establish an "OIC CERT"
- On July 27th, 2006, the first "OIC-CERT" Task Force meeting was held in Kuala Lumpur, Malaysia (CyberSecurity Malaysia) and Tunisia (National Agency for Computer Security - ANSI) have been appointed as the protem Chairman and Secretariat, respectively. The ANSI runs TunCERT (CERT member), which is one of the best in the region.
- In June 2008, the Organization of The Islamic Conference (OIC) has approved and accepted the Resolution on "Collaboration of Computer Emergency ResponseTeam (CERT) Among the OIC Member Countries". The Resolution was approved during the 35th Session of the Council of Foreign Ministers of the OIC Meeting in Kampala, Uganda (on 18 - 20 June 2008).
- In May 2009, the Organization of The Islamic Conference (OIC) has accepted the Resolution on "Granting the Organization of the Islamic Conference-Computer Emergency Response Team (OIC-CERT) an Affiliated Institution Status". The Resolution was during the 36th Session of the Council of Foreign Ministers of the OIC Meeting in Damascus, Syrian Arab Republic (on 23 - 25 May 2009)

Again, in reference to Libya, even though it is not a founding member, has become a full member of OIC-CERT. However, this is not very significant operationally given that Libya has no CERT and does not seem to be likely to rely only on CERT in the event of an attack. It is possible that Libya is assisted by the Malaysia and Tunisia CERTs in addition to Serbia's CERT. As part of Libya's cyber pattern, in the case of a cyber-attack on Libya, it's most likely to solicit the assistance of Serbia professionals to help fend-off the attacks.

It is also worth noting that the U.A.E. countries have just signed a MoU with CERT to enhance the cyber-attack mechanisms of their cyber space. The MoU includes Dubai's port operator (DP World), which has teamed up with the UAE Telecommunications Regulatory Authority (TRA), represented by the UAE Computer Emergency Response Team (aeCERT), to defend against cyber-attacks on mission critical systems.

3.7 Short and Long Term Consequences of Cyber-Attacks

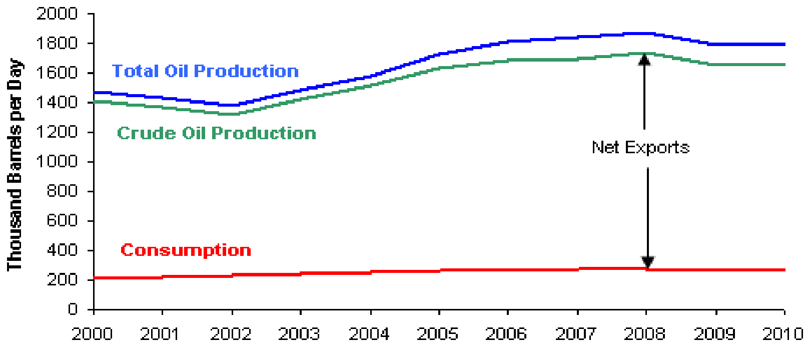
To more specifically understand the impact of an ―offensive” initiative against Libya‘s oil infrastructure in relation to the economy, it is important to consider it from the following perspectives:

- Long-term impact to the economy of Libya
- Short-term impact to the infrastructure of Libya
- Long-term impact to the economy of Others
- Short-term impact to the infrastructure of Others

3.7.1 Short and Long-Term Impact to the infrastructure and economy of Libya

Oil related exports, both of crude oil and refined products, account for nearly 95% of Libya‘s exports and more than 80% of their fiscal revenue. Without oil exports, Libya will obviously suffer long-term consequences from the reduction of revenue. Of equal, if not greater significance, is the almost immediate impact to the local infrastructure that would result from the curtailment of much of their refined products. Most refineries are not able to store more than a few days‘ worth of product, which means that within one to two weeks, inventories within local cities will begin to dry up. Libya does not possess the necessary natural gas distribution network within the country to efficiently use gas for the production of electricity. The majority of the power plants require fuel oil, which is supplied from the refineries. As fuel oil supplies are depleted, generating capacity begins to drop. Diesel and motor gasoline also begin to decline, and the transportation system effectively shuts down. This then impacts second-tier aspects of the economy, preventing goods and services from being manufactured, sold, and distributed.

This may also create deeper layers of social instability and insecurity, which can lead to additional aggressive actions within the country.



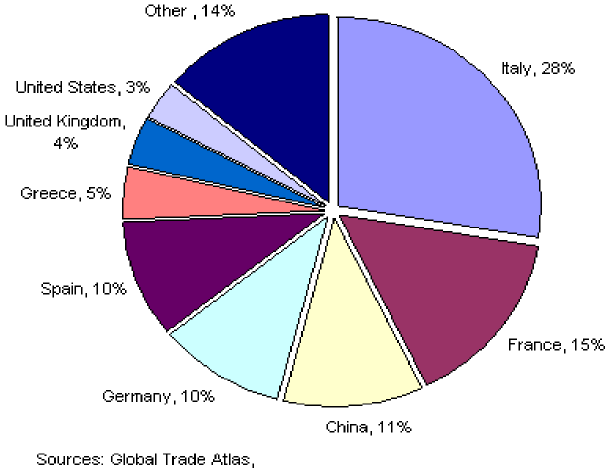
Source: EIA
Note: 2010 is a preliminary estimate based on Jan-Nov available data

Figure 3-3 – Libyan Oil Production vs. Consumption (2000-2010)

This figure shows production versus consumption rates for Libya. (Obtained from EIA) Based on information regarding the current situation within the oil production facilities, Libya‘s production rates have already dropped to almost those of consumption.

3.7.2 Short and Long Term Impact on the Economy and Infrastructure of Others

As previously mentioned, refineries are designed to operate with a specific crude oil blending, making it very difficult to significantly change a particular refinery‘s feedstock based on the sudden removal of a particular grade. Libya currently has nine export grades of crude oil, ranging from API gravities of 26.0˚ (heavy crude) to 43.3˚ (light crude). Most of the light crude is destined for European markets, while the heavier crudes target Asia. The chart below shows where Libya currently exports oil.

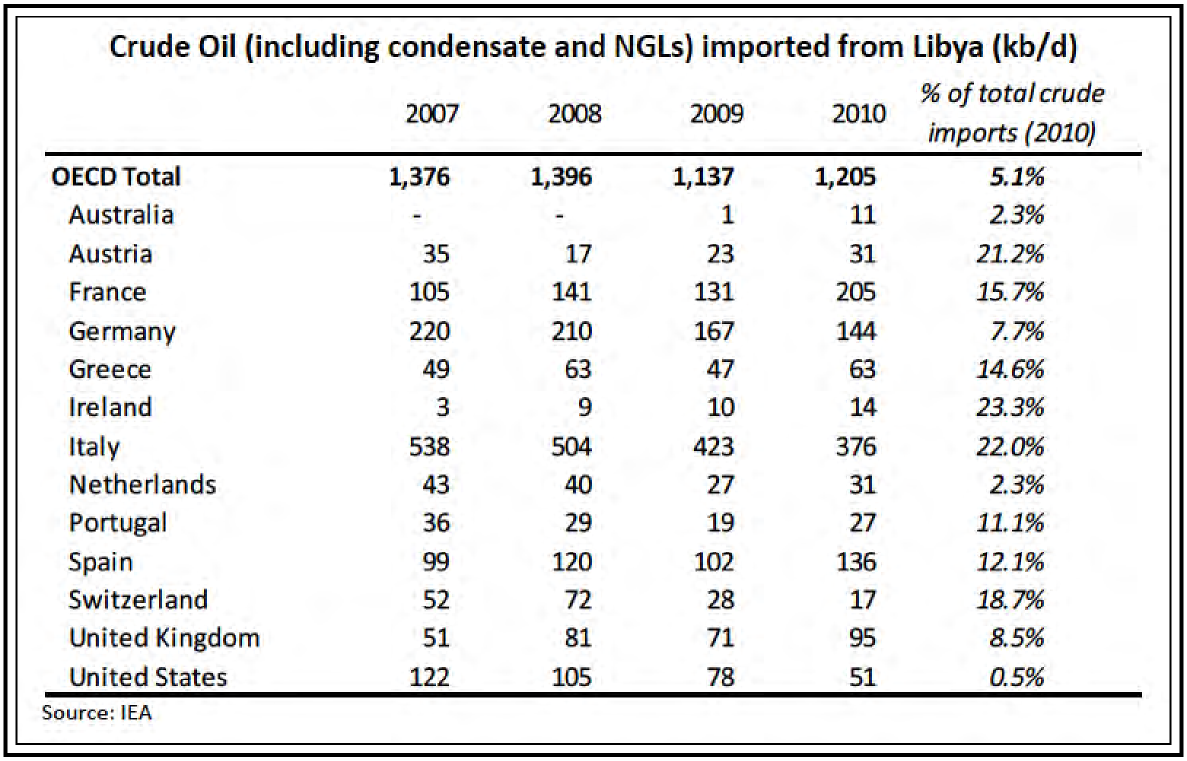


Sources: Global Trade Atlas, EIA, IEA, FACTS Global Energy

Figure 3-4 – Libya's Oil Exports by Destination (Jan 2010 – Nov 2010)

Italy is at the greatest risk of economic impact due to a sudden drop in crude oil imports from Libya. Libya is also a direct producer and distributor of refined products in Italy, Germany, Switzerland, and (since early 1998) Egypt through Tamoil. In Italy, Tamoil Italia, controls about 5% of the country's retail market for oil products and lubricants, which are distributed through around 2,200 Tamoil service stations.

To more thoroughly understand the implications of the sudden loss of crude oil to a particular country, it is necessary to understand the actual impact the supply of Libyan oil has on a particular country‘s oil infrastructure. The chart below shows the percentage of oil sourced from Libya as a percentage of all oil consumed within the country.



Crude Oil (including condensate and NGLs) imported from Libya (kb/d)

	2007	2008	2009	2010	*% of total crude imports (2010)*
OECD Total	**1,376**	**1,396**	**1,137**	**1,205**	***5.1%***
Australia	-	-	1	11	*2.3%*
Austria	35	17	23	31	*21.2%*
France	105	141	131	205	*15.7%*
Germany	220	210	167	144	*7.7%*
Greece	49	63	47	63	*14.6%*
Ireland	3	9	10	14	*23.3%*
Italy	538	504	423	376	*22.0%*
Netherlands	43	40	27	31	*2.3%*
Portugal	36	29	19	27	*11.1%*
Spain	99	120	102	136	*12.1%*
Switzerland	52	72	28	17	*18.7%*
United Kingdom	51	81	71	95	*8.5%*
United States	122	105	78	51	*0.5%*

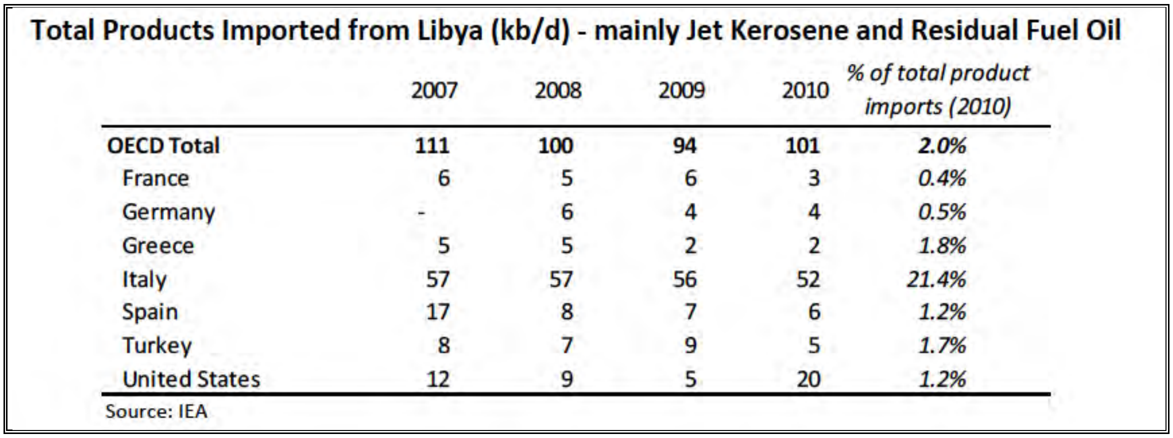
Source: IEA

Figure 3-5 - Cruide Oil (including condensate and NGLs) imported from Libya (kb/d)

This data confirms that not only Italy, but also Austria, France, Greece (already in economic stress), Ireland, and Switzerland would see potential consequences to their already sensitive economies.

Libya and Italy currently have multiple energy relationships, including the 32-inch Greensteam Pipeline, which begins in Wafa and continues to Mellitah where it turns subsea under the Mediterranean Sea, surfaces in Sicily and continues through Italy ending at their northern border.

Most of the countries impacted by Libyan sourced crude oil have means of refining crude oil into higher value products used as part of everyday lifestyles. Italy, however, also has a huge dependence on Libya for the supply of their refined products. The following table shows that over 20% of Italy‘s consumption of refined products is supplied from Libya.



Total Products Imported from Libya (kb/d) - mainly Jet Kerosene and Residual Fuel Oil

	2007	2008	2009	2010	*% of total product imports (2010)*
OECD Total	**111**	**100**	**94**	**101**	***2.0%***
France	6	5	6	3	*0.4%*
Germany	-	6	4	4	*0.5%*
Greece	5	5	2	2	*1.8%*
Italy	57	57	56	52	*21.4%*
Spain	17	8	7	6	*1.2%*
Turkey	8	7	9	5	*1.7%*
United States	12	9	5	20	*1.2%*

Source: IEA

Figure 3-6 – Total Products imported from Libya (kb/d)

4. OIL, GAS AND SCADA

4.1 Introduction and Background

Libya is a member of OPEC (the Organization of Petroleum Exporting Countries), and though it is not the largest producer of oil, it does hold the largest proven oil reserves in Africa. ―According to the 2008 BP Statistical Energy Survey, Libya had proved oil reserves of 41.464 billion barrels at the end of 2007 or 3.34 % of the world's reserves" (MBendi, 2011).

Other statistics in regards to Libyan oil production include the following from MBendi.com:

―Libya is Africa‘s major oil producer and one of Europe‘s biggest North African oil suppliers. Supplies from North Africa to Europe destinations have the advantage of being both timely and cost effective. According to the 2008 BP Statistical Energy Survey, Libya produced an average of 1847.7 thousand barrels of crude oil per day in 2007, 2.2% of the world total and a change of 0.5 % compared to 2006. Libya‘s economy is based on oil, and exports contribute between 75% and 90% of State revenues.

According to the 2008 BP Statistical Energy Survey, Libya had 2007 proved natural gas reserves of 1.49 trillion cubic meters, 0.84% of the world total, while producing 15.2 billion cubic meters, 0.51% of the world total, in the same period" (MBendi, 2011).

In addition, ―NOC controls the whole of the downstream sector together with its numerous subsidiaries and overseas arms, Umm Jawwaby Oil Services and OilInvest with its two subsidiaries of Gatoil and Tamoil. The Umm Jawwaby Oil Services acts as the Libyan National Oil Company‘s procurement arm based in London. Libya is a direct producer and distributor in Italy, Germany, Switzerland and Egypt. In Italy, Tamoil Italia, based in Milan with approximately 2,100 service stations, controls about 5% of the country‘s retail market for oil products and lubricants" (MBendi, 2011).

According to a report dated 06 April 2011 on oilprice.com, the suggestion ―that much of the fear that Libya oil export could be offline 'for years' or even ‗indefinitely‘ seems to be somewhat hyperbole" (MBendi, 2011).

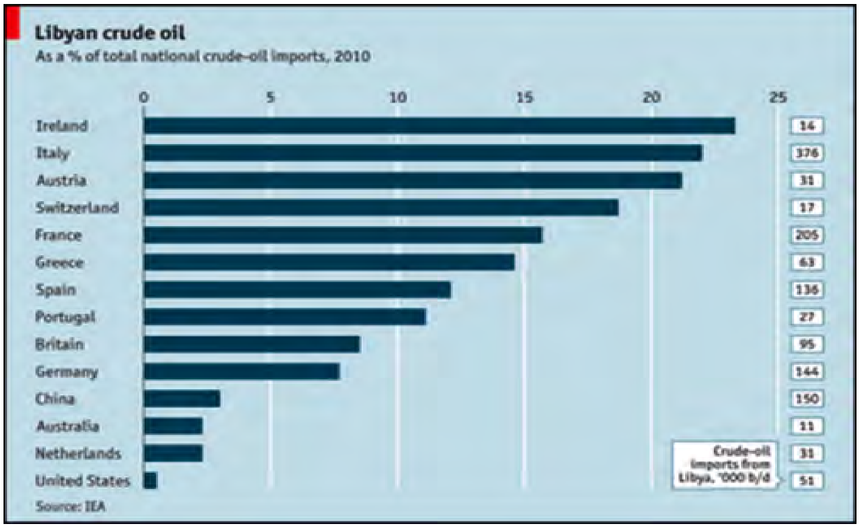


Figure 4-1 – Libyan Crude Oil as % of Total National Crude Oil Imports

Continuing from that article, ―if you look at the production level relative to the world‘s, you‘d realize Libya‘s production is about 1.7 million barrels per day (bpd), accounting for less than 2% of the world‘s 88 million bpd of oil. Out of the 1.7 million bpd, Europe is Libya‘s top crude customer with 11 countries importing about 1.1 million bpd (see chart below)" (The Economist, 2011).

As stated, oil and gas are the primary sources of revenue for Libya; however, they do not produce enough to directly affect the United States. Despite that fact, many of the countries that could be negatively impacted by a successful attack against the Libyan infrastructure are U.S. allies, which could strain those country's economies and as a result, eventually possibly the United States.

Despite the impact, it is also important to recognize that some attacks may be motivated by money, others by the desire to create chaos, and some may be driven for more clandestine purposes. Potential actors could be Chinese hackers like ‗Night Dragon‘, hacker groups, members of organized crime groups who are seeking advantage via the Internet, state sponsored hackers or industrial spies to name a few. Target and motivation are important components to cyber-attacks against a system or infrastructure, and as the economy expands, the desire to find lucrative targets for the purpose of either financial or political gain or motivation will also grow. For example, industrial systems are a constant target, and given time and money, access can be gained to almost any system. This became apparent with the STUXNET attacks. Today, any company using SCADA devices (this particular device type referenced as an industrial tool) could and would be potential targets, if for no other reason than to cause chaos and mayhem.

Other Notes on the Oil Industry in Libya as indicated by Wikileaks: (Wikileaks, 2008).

- State-Owned Zwara Oil Refinery Company Has Appointed HSBC as Financial Adviser: Zwara Oil Refinery Company (Zorco) plans to develop a 200,000 barrels-a-day crude oil refinery

- Chinese CNPC to Bid for Verenex Asset in Libya: China National Petroleum Corporation (CNPC) is bidding for Canadian energy firm Verenex Energy in a transaction valued at as much as $300 million; adding a successful bid would broaden CNPC"s assets in Africa. Indonesia"s state oil firm, Pertamina, had announced its interest to participate in the Libyan oil area of the Canadian energy company Verenex. [Reuters, 12/15/2008]
- Hess Discovers Oil in Libya Sirte Offshore: In Libya, well A1-54/01, which is located 38 miles offshore in the Sirte Basin, was drilled to a depth
- Turkish Petroleum Overseas Company Pre-Qualifies More than Ten Companies to Provide Drilling Services: A prequalification notice had been issued, and the companies in the running, all based in Libya
- NOC Announces AGOCO Oil Discovery: The National Oil Corporation (NOC) announced that the state-owned oil company Arabian Gulf Oil Company (AGOCO) made an oil discovery in the Ghadames Basin. The well is located approximately 500 kilometers south of Tripoli
- Libya Gains $5.4 Billion Dollars from Altering Oil Deals: The NOC reported earnings of $5.4 billion U.S. dollars in additional oil revenues from changes to contracts with foreign companies ENI, Petro-Canada and two consortiums led respectively by U.S. Occidental and Spain‘s Repsol last year.
- New Oil and Gas Discovery by Australian Woodside: NOC announced that an exploratory well drilled by Woodside in the Ghadames Basin, 900 kilometers South of Tripoli, produced oil and gas when tested.
- Shell Awards Seismic Contract: The UK/Dutch Shell Group has awarded a seismic contract to BGP, the geophysical division of Chinese oil company China National Petroleum Corporation (CNPC), for a survey on the gas exploration block 89N in the onshore Sirte Basin. It is considered a difficult area to work in due to the potential risk from landmines
- Libya to Invest in Oil Refinery in Egypt: Libya will invest in an oil refinery and a number of construction projects in Egypt under a deal signed in December 2008, during a visit to Tripoli by Egyptian President Hosni Mubarak. Aside from the refinery, Libya will also build service stations as well as an industrial and residential complex in Egypt. The two countries are also working towards establishing a free exchange zone on their border.

4.2 Vulnerabilities within Libyan SCADA Systems

Before looking at specific vulnerabilities, it is important to understand some of the structure of the Libya O&G industry, covering initial exploration and production (E&P) activities, through distribution, refining, and transport. The E&P business within Libya consists of not only state-owned, but also several joint ventures established in recent years with major international oil interests following the removal of the United Nations bans in 2003 (followed by the lifting of United States bans in 2004). Some of these relationships include active production wells for both crude oil and natural gas, while others have not yet been fully developed.

Figure 4-2 - Refinary

With a large number of players in this space, it is likely that there is an equally large compilation of supervisory control and data acquisition systems (SCADA) from numerous vendors spanning several years of revisions and platforms.

The area most vulnerable to a cyber-attack, which could impact not only the Libyan‗s prime source of income, but also the primary source of energy to the country, would be a focused attack on their petroleum refining facilities. Without refined products, it is difficult to fuel the trucks, tanks and planes needed to wage any effective war campaign.

Libya has the capability to refine just less than 380,000 barrels of crude oil per day, coming primarily from the Sarir and Mesla fields, both located in eastern Libya. Of this capacity, it is primarily processed through two refineries: Ras Lanuf at 220,000 BBL/D and Az Zawia at 120,000 BBL/D. Both refineries were initially built as straight-run or ―topping" refineries, due to the high quality of the crude oil feedstock. Az Zawia was commissioned in 1974 and Ras Lanuf in 1984. Based on these dates, the initial control system would have most likely been based on pneumatic-type instrumentation. In 1986, President Reagan issued a full ban of direct imports and exports with Libya. In 1992, the United Nations began to impose bans on the sale of oil equipment to Libya. Though this did not directly include the sale of automation equipment, it could be implied that little new automation technology was made available to Libya as a result of these bans.

The Ras Lanuf Refinery underwent an upgrade in 1995 to add a catalytic cracking unit (reformer) and naphtha hydrotreater to increase output of gasoline and lighter products. Since the embargo was still in force, it could be assumed that any new instrumentation was based on older, pneumatic technology offering little –digital” infrastructure.

In 2004, President Bush lifted many of the economic sanctions with Libya, allowing trade to once again resume. This appears to be when Libya began to undertake significant upgrades to their refining infrastructure, beginning with an automation upgrade at the Az Zawia Refinery, which included significant improvements to the control system infrastructure, including upgrades to distributed control systems (DCS), emergency shutdown and burner management systems (BMS), and real-time plant-wide data historians.

Beginning in 2009, a five-year program to upgrade the Ras Lanuf Refinery was also initiated, following the creation of a joint venture at this refinery between Libya and the UAE. This project is expected to cost $2 billion, and will include not only mechanical upgrades to the facilities, but also complete integrated control system upgrades.

Information gathering has uncovered that the Ras Lanuf Refinery has undergone smaller, standalone automation projects in recent years. These upgrades provide the keys to the vulnerabilities that now exist within this refinery and provide a means to impact the operation of the control system and the plant under control.

First quartile oil companies are resistant to implement appropriate security controls within the control system networks to prevent or detect an –inside” attack, since they believe that all threats will originate from outside the isolated and trusted control system environment. STUXNET demonstrated in 2010 the power of an inside attack and how it is able to effectively operate uninhibited when launched from the inside.

Further information has shown that these refineries possess equipment that is vulnerable to attacks, mainly due to the fact that it is highly unlikely that any of these systems have been properly patched, either for what was discovered during the STUXNET disclosure or as part of a normal maintenance activity.

STUXNET exploited the Siemens SIMATIC PCS7 control system and the S7-315 and S7-415 PLCs that it controlled. Research has uncovered that there are potentially vulnerable S7-315 PLCs installed within the demineralization plant used to treat boiler feed water in 2002. Refineries depend on steam for both its heat value and the ability to generate electricity (though many refineries in the Middle East do not depend on steam for electric generation due to the abundance of refinery and natural gas). Refineries cannot operate without steam.

Other references have also confirmed that there are [redacted] controllers used on the gas turbines that comprise the power plant of the refinery. These PLCs were likely installed before the Reagan embargo and could likely still be in service. These become vulnerable targets for attack considering they were likely integrated in recently years to a human-machine interface (HMI) type architecture through the simple addition of Ethernet communication modules.

Finally, references have been found to projects implemented since [redacted] that utilize [redacted]. [redacted] version [redacted] was released in [redacted] and runs on either [redacted] platforms – both unsupported and vulnerable to a complete compromise via cyber-attack.

This information confirms the likelihood of able, vulnerable equipment within the Libyan refineries. A cyber-attack would be among the easiest and most direct means to initially inject into the systems if unable to gain physical engineering attacks against the facility. Numerous client-side attack vectors exist that support payloads capable of compromising SCADA application platforms.

5. ANALYSIS

The current situation in Libya presents both threats and opportunities. The threats are those that accompany any region in the midst of civil unrest: a changing unsettled environment, opposing forces who may seek retribution in the following years, a flood of weapons to the region and mixed allegiances pave the way toward an unpredictable future. It is still not apparent who will control Libya in the days to come or how the military and government will be structured following the expected overthrow of Gaddafi's regime.

Libya is also ripe with opportunity. Some suggestions include the following:

- Infiltrate existing Internet technology that will assist in influencing collection methods.
- Deploy advanced information technology sensors to assist in information gathering.
- Leverage the passive collection of malicious traffic emanating from compromised public IPs. It would transform raw data into actionable intelligence and metrics that feeds into the over cyber intelligence profile of Libya
- Sensors could track financial movements, military changes/purchases, diplomatic communications, Chinese government activities within Libya, extremist penetration and expansion, and oil production/pricing information and fluctuations.

Other suggestions include:

- Rebuild their infrastructure to accommodate their new era of free communication, that way all infrastructure blueprints and details will be known before hand and adding/taking away from it will not be a problem.
- Get {EG,TU}-CERT involved will be beneficial as it will help with the "trust" gap. (it's more about trust than culture in the MENA region)
- For governments - maintain a database for countries of interest that collect information about each piece of the critical infrastructure
- Being part of OPEC, Libya already has connections with "like" countries with oil/gas production. Encourage those countries to assist in bringing the o/g facilities in Libya to what is considered 'modern'. This would include not only the controlling devices (think SCADA here), but also how those facilities communicate (wireless/cellphone/satellite and potentially landline/DSL).
- By encouraging the 'local' neighbors of Libya to assist with updating, we as a country might very well show/indicate that we have confidence in our allies and friends in the region. This would hopefully be a significant move perceived, not only 'locally' within Libya and the Middle East, but around the world.

IT: invest a concerted joint coordination and collaborative effort involving federal and commercial institutions to research, trace, access, and analyze state run Libyan investments and fund flows. We would suggest a strong focus on the states sovereign wealth fund controlled by the Libyan Investment Authority (LIA). Efforts to freeze LIA assets are reported to have already transpired in the US, Canada and the UK. However, the details of all of the sovereign wealth funds' investment interests are unknown and the portion of funds continuing to flow presents an opportunity for non-favorable political figures to fund malicious cyber acts and manipulate the transition of power. This fund is significant because of pro-Qaddafi supporters involved in the fund and the known opaque and reported "haphazard" operational practices utilized to execute the fund.

5.1 Creation of Social Networking Sites

The opportunity exists to establish two different social networking sites each dedicated to one side of the conflict. The potential for using traditional cyber jihadist favorite tools such as vBulletin could serve as an intelligence collection mechanism for site participants. Each site would brandish propaganda sympathetic to each cause as a method to attract and identify those loyal to Qathafi's regime and the rebels.

6. CONCLUSIONS

CSFI has looked at raw and organized data related to Libya‘s cyber security posture and threat levels. We have expanded and gotten granular on many aspects of the state actor of Libya, including kinetic effects caused by military action. Our final conclusion focuses on three elements: scope, scale and severity. Our scope was concentrated on Libya‘s defensive and offensive capabilities in cyberspace. From a CND (Computer Network Defense) perspective, Libya‘s ability to protect, monitor, analyze, detect and respond to network attacks, intrusions, disruptions or other unauthorized actions is minimal. Libya has a massive number of compromised network systems, no national cyber security strategy, and older technology. This dangerous security posture in cyberspace can be taken advantage of by state actors, rogue nations and hacking groups. At the moment, one of Libya‘s few defensive measures would be to cut connectivity, as they do not have the capability to fight through an attack. CSFI would like to alert the international community about the many oil refineries in Libya running a large compilation of supervisory control and data acquisition (SCADA) systems from various vendors spanning several years of revisions and platforms. Well-coordinated cyber-attacks against their oil refineries can not only damage their oil production but also affect the global oil market.

From a CNA (Computer Network Attack) perspective, Libya‘s ability to disrupt, deny, degrade, or destroy the information within computers and computer networks should be taken into consideration as a medium severity threat level with natural conditions to scale into something more serious. Their current offensive capabilities are not too well organized by their government or supporters; however, due to their weak defensive posture, a great portion of their nation‘s network systems could be hijacked and exploited by other actors and transformed into an effective weapon.

CSFI recommends the United States of America, its allies and international partners take the necessary steps toward helping normalizing Libya‘s cyber domain as a way to minimize possible future social and economic disruptions taking place through the Internet.

6.1 About CSFI (The Cyber Security Forum Initiative):

Website: www.csfi.us

The Cyber Security Forum Initiative (CSFI) is a non-profit organization with a mission "to provide Cyber Warfare awareness, guidance, and security solutions through collaboration, education, volunteer work, and training to assist the US Government, US Military, Commercial Interests, and International Partners." CSFI was born out of the collaboration of dozens of experts, and today CSFI is comprised of a large community of nearly 7000 Cyber Security and Cyber Warfare professionals from the government, military, private sector, and academia. Complimentary to our collaboration efforts, CSFI is engaged in creating Cyber Warfare training materials to promote a stronger background for our men and women in uniform and also throughout the DOD community.

References:

ADCB UAE Business Directory. 2011. Information Technology Companies in Libya. http://www.adcbuae.com/directory/information_technology_companies_in_libya.html (accessed April 8, 2011).

Anima Investment Network. 2011. Country Perspectives Libya: Telecom & Internet, http://www.animaweb.org/en/pays_libye_telecominternet_en.php (accessed April 4, 2011).

The Arabic Network for Human Rights Organization. 2004. The Internet in an Arab World: A New Space for Repression? Libya, the Internet in a Conflict Zone. http://www.anhri.net/en/reports/net2004/libya.shtml (accessed April 5, 2011).

Baram, Marcus. 2011. Libya's Billions Invested in U.S. Private Equity. Big Banks. Huffington Post Online (March 1, 2011). http://www.huffingtonpost.com/2011/03/01/libya-investment-portfolio-us-banks-equity_n_829964.html (accessed April 20, 2011).

BestGrowthStock.com. 2011. Escalated Violence at Libya Effect Global Oil Supply. (February 24, 2011). http://www.bestgrowthstock.com/blog/2011/02/24/escalated-violence-at-libya-effect-global-oil-supply/

BusinessWire. 2005. Ericsson Mobile Softswitch to Expand Al Madar Network in Libya. (September 27, 2005), http://www.allbusiness.com/media-telecommunications/internet-www/5077484-1.html (accessed April 8, 2011).

Carnegie Mellon, Software Engineering Institute. 2011. The CERT Faq. http://www.cert.org/faq/cert_faq.html (accessed April 20, 2011).

Danowitz, A.K., Y. Nassef and S.E. Goodman. 1995. *Cyberspace in the Sahara, Computing across North Africa. International Perspectives Communications of the ACM* Vol. 38, No. 12, pp 23-28 (December 1995), http://som.csudh.edu/fac/lpress/devnat/general/nafrica.htm (accessed April 7, 2011).

DHS. 2011. Human Factors Behavioral Science Projects: *Social Network Analysis for Community Resilience Project.* Project Manager: Michael Dunaway. http://www.dhs.gov/files/programs/gc_1218480185439.shtm#21 (accessed April 18, 2011).

Dutta, S. and Irene Mia. 2010. Global Information Technology Report 2009-2010. World Economic Forum -Insead, The Business School for the World http://docs.google.com/gview?url=http://www.weforum.org/pdf/GITR10/GITR+2009-2010_Full+Report+final.pdf&chrome=true

Eid, Gamal. 2004. The Internet in an Arab World: A New Space for Repression? Libya, the Internet in a Conflict Zone. The Arabic Network for Human Rights Organization, http://www.anhri.net/en/reports/net2004/libya.shtml (accessed April 5, 2011).

Fell, Charlie. 2011. Crude Oil & Stock Prices. (18 March 2011), www.charliefell.com/indexphp/articles/2-general/139-crude-oil-a-stok-prices?amp (accessed April 6, 2011).

Frayer, Lauren. 2011. Could Gaddafi Sabotage Libya's Oil Fields*? AOL News (*23 February 2011), www.aolnews.com/2011/02/23/could-moammar-gadhafi-sobatage-libyas-oil-fields/ (accessed April 6, 2011).

Gethard, Gregory. 2008. How Does Crude Oil Affect Gas Prices? *Investopedia,* http://www.investopedia.com/articles/economics/08/crude-and-gas-prices.asp (accessed April 6, 2011).

Hawkes, Rebecca. 2011. Jazeera Names Libyan Spy Agency as Jamming Source. (February 22, 2011). Radio TV News. http://www.rapidtvnews.com/index.php/2011022210508/al-jazeera-names-libyan-spy-agency-as-source-of-jamming.html

Itp.net. 2008. LTT to bring WiMAX service to Libya with Alcatel-Lucent deal: Libya Telecom and Technology (LTT) WiMAX service due to launch in September for business and residential users (May 5, 2008), http://www.itp.net/518453-ltt-to-bring-wimax-service-to-libya-with-alcatel-lucent-deal (accessed April 6, 2011).

IT News Africa. 2010. WIOCC-EASSy Cable Ready for Business (July 23, 2010). http://www.itnewsafrica.com/2010/07/wiocc-eassy-cable-ready-for-business/comment-page-1/ (accessed April 7, 2011).

Krebs, Brian. 2010. Mariposa Botnet Authors May Avoid Jail Time. (March 4, 2010). http://krebsonsecurity.com/2010/03/mariposa-botnet-authors-may-avoid-jail-time/ (accessed April 9, 2011).

Landesman, Mary. 2011. Mariposa Botnet. About.com http://antivirus.about.com/od/virusdescriptions/p/mariposa.htm (accessed April 21, 2011).

LibyaInvestment.com. 2011. Libya Distributes 150,000 Laptops. (February 15, 2011). http://www.libyaninvestment.com/index.php?option=com_content&view=article&id=153520&catid=42&Itemid=168 (accessed April 10, 2011).

LibyaLinks.com. 2011. Libya Hosting. http://www.libyalinks.com/dir/libya-hosting (accessed April 5, 2011).

LibyaLinks.com. 2011. Libya Internet Service Providers. http://www.libyalinks.com/dir/libya-internet-service-providers (accessed April 5, 2011).

Libyan Interim National Council. 2011. http:ntclibya.org/english/about/. (accessed April 15, 2011).

Libya News and Views. 2010. (December 23, 2010) http://www.libya-watanona.com/news/n2010/dec/1210nwsc.htm (accessed April 11, 2011).

MadeinChina.com. 2011. Free List of Libyan Companies. http://www.made-in-china.com/global-company-index/Libya-5024-1.html (accessed April 8, 2011).

MBendi. 2011. Oil and Gas in Libya, an Overview. http://www.mbendi.com/indy/oilg/af/lb/p0005.htm (accessed April 7, 2011).

Murchu, Liam. 2011. Distilling the W32.Stuxnet Components. http://www.symantec.com/connect/blogs/distilling-w32stuxnet-components (accessed April 9, 2011).

MyFoxDetroit.com. 2011. Libya Prepares for a Day of Anger, (February 16, 2011), http://www.myfoxdetroit.com/dpps/news/libya-prepares-for-day-of-anger-dpgonc-20110216-gc_11915839 (accessed April 9, 2011).

http://oilprice.com/Energy/Crude-Oil/Oil-Supply-Crisis-From-War-in-Libya-Free-Trade-Begs-to-Differ.html
OIC-CERT. 2011. http.//www.oic-cert.net (accessed April 20, 2011)

OTEGLOBE. 2010. Construction of the ‗Silphium' cable across the Mediterranean, (June 12, 2010), http://www.oteglobe.gr/index.php?option=com_content&task=view&id=143&Itemid=135&lang=en (accessed April 7, 2011).

Sibley, Jeff. 2010. Malware Affecting Siemens WinCC and PCS7 products (STUXNET) http://www.automation.siemens.com/WW/forum/guests/PostShow.aspx?PageIndex=1&PostID=225690

(accessed April 11, 2010).

Siemens. 2011. http://www.usa.siemens.com/entry/en/index.htm?stc=usccc020189 (accessed April 11, 2011).

Speartip, LLC. 2011. Serbian Hackers Support Gaddafi. March 2011. http://www.speartip.net/2011/03/serbian-hackers-support-gaddafi/ (accessed April, 17, 2011).

Stewart, Scott. 2011. Will Libya Again Become The Arsenal Of Terrorism? Stafor. (March 10, 2011). http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=14041:stratfor-will-libya-again-become-the-arsenal-of-terrorism&catid=49:National%20Security&Itemid=115 (accessed April 10, 2011)

The Peninsula. 2011. Clashes as Libya Braces for Day of Anger. (February 17, 2011). http://www.thepeninsulaqatar.com/middle-east/142870-clashes-as-libya-braces-for-day-of-anger.html (accessed April 11, 2011).

TechoLibya. 2010. HP to Expand In Libyan Market. (November 22, 2010). http://www.technolibya.com/internet/hardware/hp-to-expand-in-libyan-market.html (accessed April 10, 2011).

TechnoLibya. 2010. Vodafone and Almadar Aljadid Sign Strategic Partnership, (February 23, 2010) http://www.technolibya.com/ (accessed April 10, 2011).

TechnoLibya. 2010. LTT to Double ADSL and Add Extra 5gigs on Libyamax (October 7, 2010). http://www.technolibya.com/communications/ltt-to-double-adsl-and-add-extra-5gigs-on-libyamax.html (accessed April 8, 2010).

The Unjust Media.com (2010). http://theunjustmedia.com/Islamic%20Perspectives/Jan11/The%20Reality%20and%20the%20Role%20of%20the%20Jihadist%20Media.htm In English (search using www.ayna.com)

Thuraya. 2011.Thuraya Telecom Services Affected By Intentional Jamming In Libya. (February 25, 2011). http://www.thuraya.com/userfiles/files/Media%20Releases/2011/thuraya-telecom-services-affected-by-intentional-jamming-in-libya.pdf (accessed April 9, 2011).

http://www.v3.co.uk/v3-uk/news/2031675/libyan-authorities-cut-internet-civil-war-looms#ixzz1K29zC8xy

Unveillance. 2011. www.Unveillance.com. (accessed April 20, 2011).

Unveillance. 2011. http://www.unveillance.com/trends/ (accessed April 20, 2011).

UPI.com. 2011. Libya Pulls Plug on Internet. (March 4, 2011). http://www.speartip.net/2011/03/serbian-hackers-support-gaddafi/ (accessed, April 9, 2011).

U.S. & Foreign Commercial Service and U.S. State Department. 2008. Doing Business in Libya, Country Commercial Guide For U.S. Citizens. http://pdf2me.com/preview/doing-business-in-libya:-2008-country-commercial-guide-for-us-...-219898.html (accessed April 11, 2011).

Wikipedia. 2011. Europe India Gateway. http://en.wikipedia.org/wiki/Europe_India_Gateway (accessed April 8, 2011).

Wikipedia. 2011. Libya Telecom and Technology. http://en.wikipedia.org/wiki/Libya_Telecom_%26_Technology (accessed April 9, 2011).

Wikipedia. 2011. Muhammad Al-Gaddafi. http://en.wikipedia.org/wiki/Muhammad_al-Gaddafi (accessed April 7, 2011).

Tables, Graphs and Maps

First Stage of Libyan Civil Unrest Table
References:

Arasmus. 2011. Mapping Violence against Pro-Democracy Protests in Libya. (accessed April 3, 2011).
We-Re-Build. 2011. Libya Main Page. http://werebuild.eu/wiki/Libya/Main_Page (accessed April 2, 2011).
Libya Crisis Map. 2011. Social Media Mapping for Common Operational Datasets. http://libyacrisismap.net/ (accessed April 4, 2011).

Wikipedia. 2011. Libya Civil War 2011. http://en.wikipedia.org/wiki/2011_Libyan_protests (accessed April 5, 2011).

Labovitz, Craig. 2011. Middle East Internet Scorecard. *Arbor Networks*. (February 12-20,2011), http://asert.arbornetworks.com/2011/02/middle-east-internet-scorecard-february-12-%e2%80%93-20/ (accessed April 6, 2011).

Labovitz, Craig. 2011. Craig Labovitz Blog. (February 28, 2011). http://www.monkey.org/~labovit/blog/ (accessed 3, 2011).

Google Transparency Report. 2011. Libya all Products. http://www.google.com/transparencyreport/traffic/ (accessed April 7, 2011).

We Re-Build. 2011. Libya Main Page – Telecomix/Safe Internet Communication Resources for Libya. http://www.werebuild.eu/wiki/Libya/Main_Page (accessed April 4, 2011).

Dear UN. 2011. Letter from Anonymous. http://feb17.info/general/anoymous
Operation Libya White Fax. 2011. http://refuse.fr/blog/index.php?article6/operation-lybie (accessed April 3, 2011).

Renesys.com. 2011. Renesys Blog –Libyan Disconnect (February 18, 2011). http://www.renesys.com/blog/2011/02/libyan-disconnect-1.shtml (accessed April 3, 2011).

McCullagh, Declan. 2011. Libya‘s Internet Hit with Severe Disruptions. http://news.cnet.com/8301-31921_3-20035079-281.html (accessed April 2, 2011).

Emile. 2011. Unsolicited Internet Traffic Reports From Libya, *According to the Best Available Data,* (March 23, 2011) http://blog.caida.org/best_available_data/2011/03/23/unsolicited-internet-traffic-from-libya/ (accessed April 3, 2011).

Internet Traffic Maps

Credit: Arbor Networks – From site: McCullagh, Declan. 2011. Libya‘s Internet Hit with Severe Disruptions. http://news.cnet.com/8301-31921_3-20035079-281.html (accessed April 2, 2011).

Credit: Traceroutes Data – From site: Renesys.com. 2011. Renesys Blog –Libyan Disconnect (February 18, 2011). http://www.renesys.com/blog/2011/02/libyan-disconnect-1.shtml (accessed April 3, 2011).

Wikipedia. 2011. Timeline of reported deaths per event. http://en.wikipedia.org/wiki/Casualties_of_the_2011_Libyan_Civil_War (accessed April 9, 2011).

Libyan Government Sites Graph
Graph Developed by CSFI using Palantir Software
Hacker Network Illustration s and Object Types Graphs

Graphs Developed by CSFI using Palantir Software
Libya‘s Population and Energy Production Maps
Stratfor. 2011. Libya‘s Population and Energy Production Map. *BP Energy World Book*. www.stradfor.com (accessed April 4, 2011).

Drilling Info International. 2011. EIA. Royal Holloway.

Libya‘s Oil Production and Consumption Graph: EIA

Libya‘s Oil Exports By Destination: Global Trade Atlas, EIA, IEA, FACTS, Global Energy

Crude Oil and Total Products Imported From Libya Graphs: IEA