1-2013

Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution

John Scott-Railton

Irregular Warfare Studies
number 3

CENTER ON IRREGULAR WARFARE AND ARMED GROUPS

Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution

John Scott-Railton

U. S. Naval War College

COVER

Anti-Mubarak protester takes
picture in Cairo, February 2011.
Photo by Peter Macdiarmind/Getty Images

Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution

Irregular Warfare Studies

In 2008 the U.S. Naval War College established the Center on Irregular Warfare and Armed Groups (CIWAG). The center's primary mission is to bring together operators, practitioners, and scholars to share academic expertise, knowledge, and operational experience with violent and nonviolent irregular warfare challenges. We are committed to making this important research available to a wider community of interest and across Joint Professional Military Educational (JPME) curricula. Our goal is to support the needs of civilian and military practitioners preparing to meet the challenges of a modern, complex international security environment. CIWAG publishes two separate series of case studies as a part of the center's expansive, ongoing effort of workshops, symposia, lectures, research, and writing.

The **Irregular Warfare Studies** are a collection of case studies that examine the use of irregular warfare strategies by states and nonstate actors to achieve political goals. These cases address a wide variety of irregular challenges on the spectrum of political violence and competition that encompass current-day or historic armed groups and conflicts, as well as the use of other irregular strategies and means to achieve political goals, including gray-zone activities, economic coercion, information operations, and resource competition.

Center on Irregular Warfare and Armed Groups

U.S. Naval War College
686 Cushing Road
Newport, Rhode Island 02841

Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution

John Scott-Railton

CENTER ON IRREGULAR WARFARE AND ARMED GROUPS

U.S. NAVAL WAR COLLEGE

Center on Irregular Warfare
and Armed Groups (CIWAG)

U.S. Naval War College
686 Cushing Road
Newport, Rhode Island 02841

Published 2021
Printed in the United States of America

ISBN: 978-1-935352-54-9 (paperback)

This publication is cleared for public release and available on the CIWAG webpage at: https://usnwc.edu/ciwag

For more information contact: ciwag@usnwc.edu.

Suggested citation:
Scott-Railton, John. 2021. *Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution.* CIWAG case study series 2013, ed. Richard Crowell, Marc Genest, and Andrea Dew. Newport, RI: U.S. Naval War College, Center on Irregular Warfare and Armed Groups.

For Sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-00001

ISBN: 978-1-935352-54-9

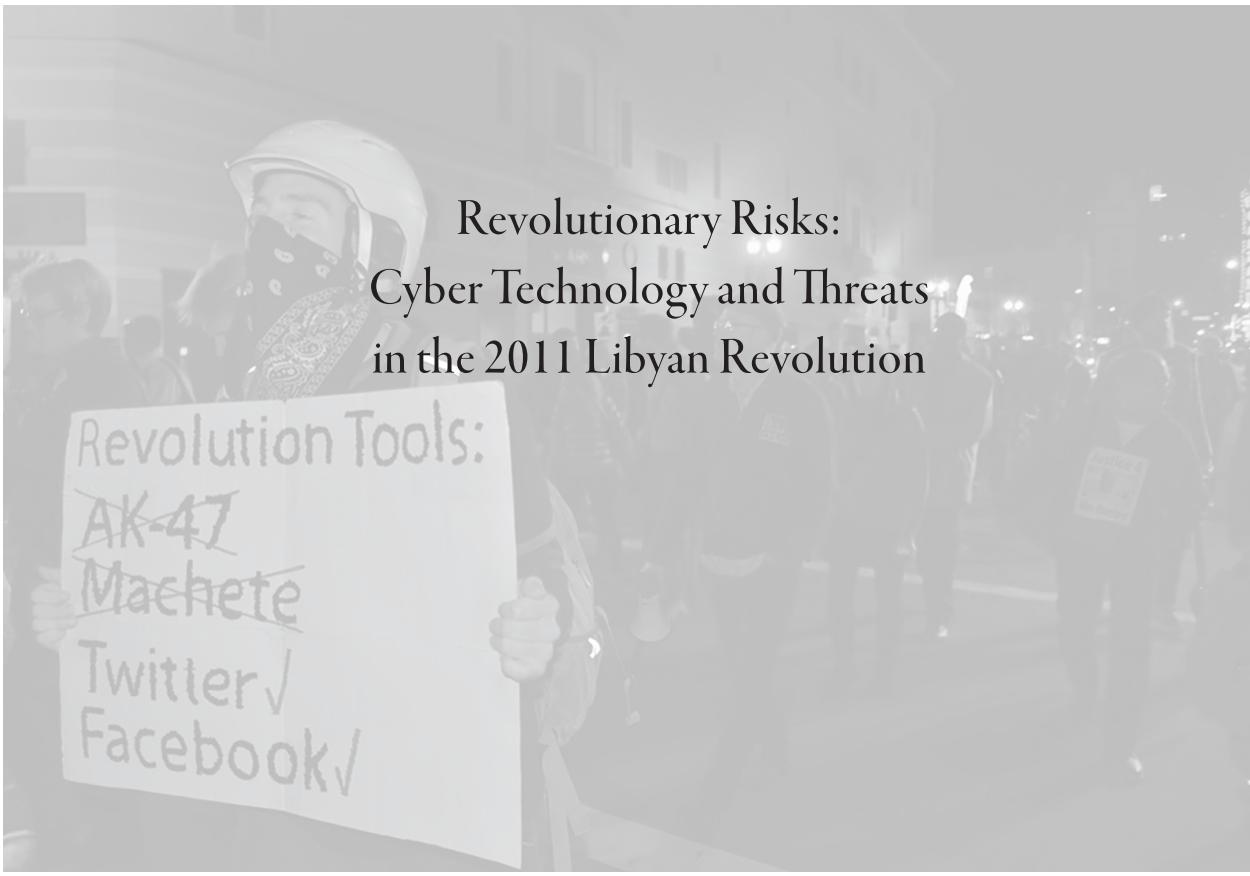
Contents

List of Figures *(Charts, Graphs & Illustrations)*

Acknowledgments

I'd like to thank Morgan Marquis-Boire (Google, and Senior Technical Advisor, Citizen Lab, University of Toronto), for the malware analysis and identification featured in the report, as well as helpful comments and discussions; Matthieu Aikins for insightful conversations and perspective arising from his fantastic work for *Wired* on the Libyan government's surveillance infrastructure, as well as threats to journalist security covered in the *Columbia Journalism Review*; Russ McRee (Microsoft) for initial malware analysis and discussion as the project developed; and Professor Richard Crowell (Naval War College) for extremely helpful dialogue throughout the writing process. I also want to thank Professor Crowell along with his colleagues Dr. Marc Genest and Dr. Andrea Dew for the early encouragement (and persuasion) to see the value to others in pursuing this unconventional project in a field far outside my own; Ron Diebert (Citizen Lab, University of Toronto) for feedback and discussion of themes of state-sponsored attacks; and John Pollock (Contributing Editor, *MIT Technology Review*) for sharing his thoughts and useful concepts as well as invaluable and detailed feedback on an earlier draft. My gratitude also goes to the many Libyans who offered thoughts, observations, commentary, malware samples, and other material to help me understand what they fought for, and bravely lived through. Thanks also to many others, too numerous to mention, who've dialogued with me about the ideas and topics in this study. Finally, special thanks to Janet Parkinson (Naval War College) for responsive, careful editing, encouragement, and patience.

Humbly dedicated to Muhannad Bensadik (KIA, Ajdabiya, March 12, 2011) and Mohamed Nabbous (killed in Benghazi, March 19, 2011).



Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution

Message from the Editors

Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution is the story of how the author and selected colleagues adapted existing information communication technology to help the Libyan opposition, counter the Libyan Arab Jamahiriya government's shut down of communications to outside the country in 2011. The case study is built from experience and contacts, stemming from recorded audio calls, and supplemented with after-the-fact conversations and open-source research.

At the time of writing, John Scott-Railton was a doctoral student at UCLA, and a Research Fellow at the Citizen Lab, University of Toronto. This research focuses on the free flow of information, particularly in conflict zones, and understanding threats to secure communications. Government attempts to subvert and control the flow of information during internal crisis also have direct application to evolving concepts of disputed informational control and denial within contemporary cyber conflict.

Scott-Railton's foray into irregular information conflict came via Egypt, as Mubarak's regime shut down the Internet to keep the world from seeing events in Tahrir Square and other areas around the country. He and several friends outside Egypt called into the country for information, then instructing an increasing circle of contacts inside Egypt to call cell phones outside Egypt. These calls were then recorded and the content tweeted or posted on other social media. Realizing that faster and more accessible connectivity was needed, the author formed @jan25voices, a network of associates whose information surrounding the conflict eventually reached millions of people, and providing grassroot support that gave a voice to Egyptian people on the street. They skillfully used both connectivity and content to outmaneuver government forces to ensure a flow of information out of the country, and past the Internet shutdown. The audio and video content coming from inside Egypt had an emotive effect that brought European and global audiences to support the opposition with money, connectivity, content, and support.

This group of tech-savvy innovators have provided a wealth of knowledge on how information content and code (software) are used in contemporary civil conflicts. Their successful denial of government informational control led to freedom of action for the opposition in the 2011 conflict. This also led to military support from the U.S. and NATO that ultimately allowed the opposition to defeating the Gaddafi regime, and the eventual election of a new government.

This is a study in the theory and practice of information warfare within a civil conflict. It tells how cyber technology was used in support of the ouster of the world's longest reigning dictator, and is deliberately not written with military jargon, but written with the civilian user in mind.

Although it is our hope that *Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution* will be a useful historical study, it's important to note that due to the complexity of civil unrest and interaction in Egypt, across North Africa, and throughout the Levant, this research is focused on the events in Egypt during 2011. The author also observed similarities between Libya and the civil war in Syria, correctly predicting that the Syrian regime would add malware and hacking to their electronic operations.

CIWAG provides this case study in the **Irregular Warfare Studies** series to assist those interested in conducting research on the use of information communication technology, social media, and cyber control in contemporary conflict.

Andrea Dew
CIWAG, Co-Director

David A. Brown
CIWAG, Co-Director

Figure Intro 1 Map of Libya

Opposition Technology and Its Vulnerability to Pro-Regime Attacks

Steve Rhoades, *Revolution Tools—Facebook Twitter,* https://www.flickr.com/photos/ari/8126756699, licensed under CC BY-NC-ND 2.0.

In the besieged city of Misurata during the 2011 Libyan revolution, Ali was using a two-way satellite Internet link to browse Google Earth, scrolling the blue marble, zooming, and precisely marking areas around the city.[1] Considering the constant stream of shelling, this might have seemed like an odd time to be working on a program commonly associated with recreational mapping and Earth viewing. Yet he was using Google Earth for a purpose more in line with the program's original design: imagery intelligence and targeting.[2]

Misuratis wanted to encourage NATO to intensify airstrikes, especially against areas where Gaddafi's forces had established supply routes, including some streets within the urban fabric of the city. Communicating with and organizing large volumes of coordinates from fighting groups that weren't

always equipped with GPS units was a problem, especially as the data had to pass through multiple hands on their way to the Misuratis' NATO contacts. To organize and keep the targeting information accurate, Misuratis turned to Google Earth.

Ali and others would receive information from fighting groups on Misurata's different fronts, sometimes as a coordinate, sometimes as a verbal description of a location that he and his team knew and could find by browsing. They would confirm the location with Google Earth and drag a pin to mark the position, label it, and take a screenshot. The team compiled sets of these files and sent them by e-mail to a contact associated with Libya's National Transitional Council and other groups outside Libya that were in direct contact with NATO.

The approach was clever, and simple. Yet, as with so many of the ways that the Libyan opposition leveraged the Internet and various free tools, electronic actors acting on behalf of the Gaddafi regime identified its use and attacked opposition computers by exploiting key human vulnerabilities in how the information was transmitted. Using hijacked e-mail and Skype accounts, pro-government electronic actors developed and circulated spear phishing attempts that encouraged recipients to execute files with names like gadaffigooglemaps, natocontacts, and gaddafimaps. These files actually contained remote-access Trojans: If a user double-clicked on the file, he or she downloaded a piece of malicious software designed to take control of the computer and exfiltrate information like keystrokes and screen captures, making it possible to capture credential information and ultimately to hijack users' accounts. Ali's e-mail account, like many others, was eventually hijacked, probably through this mechanism.

The 2011 Libyan revolution was marked by the intensive use of cyber technology. This case study reviews some of the roles that the technology played in the conflict, beginning with the Gaddafi regime's shutdown of the Internet. It highlights how the Libyan opposition reconnected itself and how connectivity was leveraged for a wide range of strategic and tactical aims. It also describes how the opposition was attacked electronically, underlining the vulnerabilities inherent in using common online tools during a military conflict.

By early February 2011, both Tunisia and Egypt had undergone revolutions, surprising much of the world. Many interpreted the speed and scope of these transformations to be at least in part a product of the potent ability of Internet connectivity to enable and accelerate disruptive social transformation.

Sandwiched by Tunisia and Egypt, the leadership of the Libyan Arab Jamahiriya[3] (LAJ) under the longstanding dictatorial regime of Muammar Gaddafi appears to have taken a similar view about the dangers of the Internet, even as the first discussion of a potential Libyan uprising began. From the first days of the uprising, the LAJ undertook a range of measures, from a total Internet shutdown to electronic attacks against the Libyan opposition's use of social media and communications. These attacks, although sometimes incurring substantial costs for the opposition, were not able to effectively deny it access to Internet connectivity or to fully degrade its many uses. Libyans quickly restored their own Internet access, completely bypassing the regime's networks and piercing the blackout with thousands of individual connections.

The blackout decisively pushed Libyans toward decentralized ways of connecting, such as two-way satellite Internet, almost totally bypassing the Libyan government's expensive and sophisticated network monitoring equipment and effectively ending the LAJ's ability to control Internet access. Yet evidence suggests that the Gaddafi regime remained aware of the Internet's importance throughout the conflict. Facing an adversary whose connections were no longer passing through their networks (and thus observable or vulnerable to disruption), the Gaddafi regime and electronic actors acting in support of it embarked on a set of campaigns to blunt the Internet's power and, in some cases, exploit connection vulnerabilities to regain their ability to spy on the opposition.

The Libyan opposition made extensive use of the Internet and various online tools for many tasks, including fighting battles, nominating targets to NATO, and coordinating logistics. Libyans used social media tools like Facebook, YouTube, and Twitter to broadcast an increasingly sophisticated stream of images, news, and information to the online public. The impact of these activities was amplified by conventional media's intense reliance on online sources.

This case study highlights how family networks meshed with social networking to create responsive and highly situationally aware clearinghouses for information. Central to the role of the Internet in the 2011 Libyan revolution was the role that it played in connecting Libyans as individuals and groups not just to the Web but also to transnational networks of diaspora Libyans and their supporters. These networks engaged in advocacy and other communications activities and provided a key backbone to the revolution, coordinating everything from aid to weapons.

The story of the role of the Internet in Libya's 2011 revolution is fascinating; much of it still needs to be documented and preserved. This case study addresses two issues that form part of this larger story:

1. What strategic roles did Internet communications tools and technologies play in the 2011 Libyan revolution, and how were they used by the opposition?
2. How did the LAJ and its supporters try to use these tools, and what were their effects?

Question 1 is answered by laying out and examining these tools and activities deployed by the opposition to restore and maintain connectivity and to use it strategically for public and private communications activities.

To answer question 2, the case study lays out information about efforts by the Gaddafi regime to disrupt, degrade, exploit, and otherwise compromise the Libyan opposition's use of the Internet, beginning with best-available information at the time of writing about the regime's monitoring and surveillance capabilities. The study further highlights how many of the tools used by the opposition, including social media, introduced substantial new risks, many of which weren't fully understood or mitigated during the conflict.

The effectiveness of some of these attacks illustrates the ways in which opposition practices introduced substantial new operational security challenges and vulnerabilities that do not appear to have been well understood during the conflict. The case study also highlights the role of pro-government electronic actors and the unique threats they posed to the Libyan opposition. It concludes with a discussion of the implications of these vulnerabilities and the emergence of such actors for other conflicts,

especially those in which direct and substantial foreign military assistance is not provided.

The subject matter is difficult, and much is still kept secret by the parties to the conflict. The organization of and privileging of certain themes and techniques over others in this study reflects the author's judgment about how to bridge gaps and provide a consistent picture. Geographically, too, the case study is limited by the author's greater familiarity with some locations (e.g., Misurata) than others. Some important details and themes have thus undoubtedly been overlooked.

This case study combines two sources of information to answer the guiding questions: open-source information, including news reports, articles, blogs, postings, and other publicly available material pertaining to the 2011 Libyan revolution; and information and materials provided by Libyan opposition members and supporters who were active participants in the revolution. The rationale for supplementing the research with direct dialogue with Libyan opposition members is simple: not only have many "private" elements of the conflict been incompletely documented, but now that Gaddafi and his regime are gone, Libyans themselves are looking forward, not back. Although memories remain strong, some of the details may be fading. This fusion of sources and approaches (a term used by the University of Toronto-based Citizen Lab) is an attempt to triangulate in on a story that is only partially written, much of it still held in the memories and on the hard drives of Libyans whose attention has turned toward their country's continued post-conflict reconstruction.

Notes

1. Personal communication with L1, Spring 2012.
2. Google Earth was originally developed from Keyhole Inc.'s EarthViewer 3D, an imagery intelligence platform.
3. Libya's official name from 1977–1986 was the Socialist People's Libyan Arab Jamahiriya; from 1986–2011, it was officially called the Great Socialist People's Libyan Arab Jamahiriya. In September 2011, the name was officially changed to Libya. The term "Libyan Arab Jamahiriya" and "LAJ" are used to refer to the Gaddafi-based Libyan government in this case study.

CHAPTER ONE

Libyan Internet Connectivity Before the Revolution

Country	Internet Users (ITU 2010)	Facebook Users (IWS/SB)	Internet Pen. (ITU 2010)	Facebook Pen. (IWS/SB)	Al Jazeera Pen. (AMC)
Tunisia	3.6 million	1 / 2.2 million	34.00%	15.8% / 20.5%	23.00%
Egypt	17 million	4 / 5.4 million	21.00%	5.1% / 6.8%	10.00%
Libya	350 k	182k / 300k	5.50%	2.8% / 4.6%	55.00%

Figure 1.1 Internet, Facebook, and Al Jazeera penetration rates in Libya, Egypt, and Tunisia[4]

The Users

The Internet was introduced to Libya in 1998, initially as a purely government service unavailable to the general public. Two years later, in 2000, Internet connectivity was first made available to Libyan citizens[5] and, by 2004, the number of Libyans with access to the Internet had grown dramatically. While the number of Internet users in Libya varies by source, Libya had more than 350,000 Internet users by 2009.[6] Compared to its neighbors Egypt and Tunisia, this number reflects a relatively low penetration rate. In 2010, for example, Egypt had an estimated Internet penetration rate of 21% and Tunisia 34%. Libya, in contrast, had only 5.5 % penetration rates for fixed users.[7] (See Figure 1.1)

The number of social media users in Libya at the beginning of the 2011 revolution was similarly small compared to neighboring Tunisia and Egypt. Facebook penetration in Libya was at either 2.8% or 4.6%, depending on estimates,[8] slightly lower than neighboring Egypt (5.1% / 6.8%), and substantially lower than Tunisia (15.8% / 20.5%). Twitter similarly reached less than 1% of the Libyan population in April 2011.[9] The relatively low penetration rate for Internet service is in contrast to both the penetration rates of Libyan state-controlled television (95%)[10] and Al Jazeera (55%).[11]

These numbers highlight a mathematical fact: information posted online in Libya could only directly reach a tiny fraction of its population.

The Internet Under the Libyan Arab Jamahiriya

In 2009, seven different Internet service providers (ISPs) offered connectivity to Libyans.[12] These providers were "subordinated" to the Libyan Telecom and Technology company (LTT), which was chaired by Gaddafi's son Mohamed Gaddafi. LTT maintained Libya's national Internet gateway through which all Internet communications entering or leaving the country passed. LTT, founded in 1997, was in turn owned by the state-owned General Post and Telecommunications Company (GPTC). GPTC also owned Libya's two mobile networks, Almadar and Libyana. This provided the LAJ with access to a centralized mechanism from which to monitor and ultimately block the Libyan Internet.

As the 2011 revolution began, according to the *Wall Street Journal,* the LAJ was actively seeking tools to supplement their monitoring apparatus with a more comprehensive filtering system.[13] Although the regime appears to have deployed a number of highly specific blocks of individual websites prior to the revolution, little evidence of a comprehensive filtering system was found during a 2009 study by the Open Network Initiative.[14] Libyans thus could connect to the Internet relatively freely, although they did so with little apparent knowledge of how comprehensively the LAJ was intercepting and monitoring their online behavior.

Discussion Questions

1. How did Libya's level of Internet penetration compare to its neighbors? Does this challenge the idea that the Internet could have facilitated an Internet shutdown?
2. How might Libya's centralized Internet infrastructure and governance have facilitated an Internet shutdown?

Notes

4. "Libya's Internet Penetration Rate Steadily Increasing," oAfrica.com, February 23, 2011, http://www.oafrica.com/statistics/libyas-Internet-penetration-rate/; "Al Jazeera Television: Viewers Demographics," Allied Media Corp, n.d., http://www.allied-media.com/aljazeera/al_jazeera_viewers_demographics.html
5. Project Cyber Dawn, Cyber Security Forum Initiative, April 17, 2011.
6. Libya, *CIA World Factbook*, CIA, 2012, https://www.cia.gov/library/publications/the-world-factbook/geos/ly.html
7. The number is likely lower than the actual number of those connected in Libya, since it doesn't track the use of mobile Internet devices.
8. "Libya's Internet Penetration Rate Steadily Increasing," oAfrica.com.
9. "TV, Twitter, Facebook and the Libyan Revolution," Informed Comment (blog), August 24, 2011, http://www.juancole.com/2011/08/tv-Twitter-Facebook-and-the-libyan-revolution.html
10. "TV, Twitter, Facebook and the Libyan Revolution."
11. "Al Jazeera Television: Viewers Demographics."
12. "Libya," Open Network Initiative, Aug. 6, 2009, http://opennet.net/research/profiles/libya
13. M. Coker and P. Sonne, "Life Under the Gaze of Gadhafi's Spies," *Wall Street Journal,* December 14, 2011, http://online.wsj.com/article/SB10001424052970203764804577056230832805896.html
14. "Libya," Open Network Initiative.

CHAPTER
TWO

The Net Goes Dark

The Internet Blackout

The exact calculus undertaken by the LAJ for shutting down the Libyan Internet is not publicly known. However, it is clear that LAJ leadership considered the Internet a serious threat and, in the wake of the January 25 Egyptian Revolution, began almost immediately to take steps that appear intended to address this risk. On February 13, 2011, Muammar Gaddafi issued a public warning to all Libyans: don't use Facebook.[15] During the same time frame, Gaddafi's regime had reportedly also arrested some activists who were known to use the Internet, possibly in response to reports of calls for protest on February 17.[16]

The threats didn't have the decisive effect that the LAJ may have hoped for. The first signs that a large popular uprising might be underway came on February 15, 2011, when hundreds of Libyans turned out in Benghazi to protest the arrest of Fethi Tarbel, a human rights activist and lawyer who had been involved in campaigning for the release of political prisoners. Interestingly, although calling for the resignation of key government figures, protesters' signs did not call for Gaddafi's resignation.[17] Tarbel was released following the protest, but a wave of protests had already begun.

The opposition movement grew throughout Libya, apparently taking its cue from neighboring Egypt, and the Gaddafi regime shut down the Libyan Internet twice for brief periods during the third week of February. The reasoning of key figures in the Libyan government that led to these first two cuts has never been made public. It is reasonable to assume that the decision was at least partly made in light of the key role that the Internet appeared to have played in the Arab Spring, as well as reporting in the early days of the uprising by Al Jazeera and others that highlighted Internet postings. At the time, many also speculated that the shutdown was intended to limit information about the crackdown unfolding against Libyan protesters.[18]

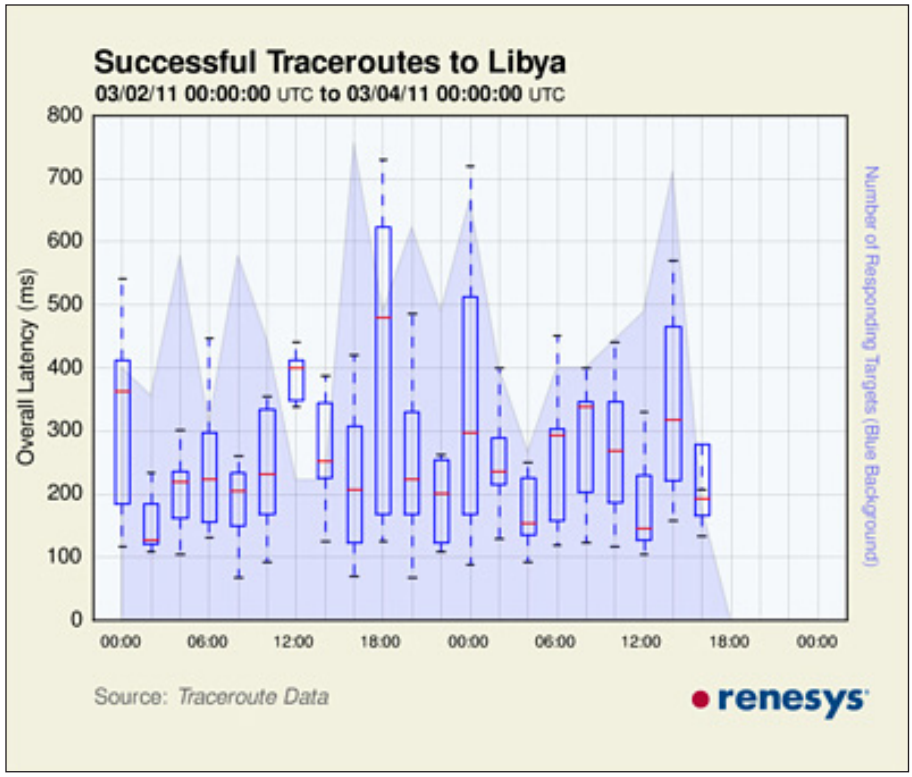


Figure 2.1 March 3, 2011, attempts to connect to hosts on the Libyan Internet (using a diagnostic tool) show a rapid decrease in the 12:00 and 18:00 UTC[19]

The first brief outage took place on February 18 and lasted 6.8 hours; the second, a day later, lasted 8.3 hours. Following the end of the second shutdown, a number of commentators noted that it seemed as if the Internet might have "returned," although it was noted that the return seemed more extensive in eastern Libya, not Tripoli, where many sites were still reported as inactive.[20]

While this return held true for the next two weeks, the optimism was premature. On March 3, at approximately 7:00 pm local time (EET), the LAJ deployed a more permanent shutdown.[21] This was observed in real time by the global Internet monitoring firm Renesys. As the cut began, attempts to access websites hosted within Libya began to fail. Renesys concurrently reported receiving reports from within Libya that Internet services, including browsing, were no longer working. It quickly became clear that a full Internet blackout had begun.[22]

Renesys noted that rather than disconnecting itself from the Internet, as the Egyptian government had done, the LAJ had instructed its network firewall to block almost all traffic, except for a small trickle. This probably indicated that the regime sought to maintain Internet connectivity for certain activities. Renesys concluded:

> The Internet is a valuable wartime resource, like a critical bridge over which supplies can flow. As long as you can deny it to your enemy, you don't blow it up — you keep it intact for your own use.[23]

The LAJ's approach was to place Libya's Internet on what Renesys called a "warm standby." This not only preserved the Internet for its own use but also softened the initial visibility of its block. Renesys continued:

> [The Egyptian web blackout had] signaled to the world that the Egyptian government considered itself out of options, ready to cut off internal communications and external dialogue, looking for a last chance to turn off all the cameras and clean out [Tahir] Square.[24]

It took most of the day before awareness of the blackout reached most international media. Citing the Renesys report, Joshua Keating of *Foreign Policy* blogged that the greater sophistication of the Libyan block compared to that used by Egypt may have reflected greater sophistication on the part of Libyan authorities. He suggested that Libya might have learned a lesson from the Egyptian experience and chosen a less immediately visible form of block.[25] From the point of view of Libyans, however, the LAJ "warm standby" had the same outcome as the Egyptian shutdown: the Internet was no longer accessible.[26]

Some speculated that the Gaddafi regime was also using jamming to block a satellite Internet service offered by LTT but managed outside Libya.[27]

The nature of the remaining Internet traffic (seen as blips on Google's Transparency Report in Figure 2.2) would become clearer much later in the conflict, as evidence emerged of groups like the Libyan Electronic Army and others acting on behalf of the regime from within Libyan networks. Some of these electronic attacks had IP addresses originating in Libya.[28] For the duration of this case study, these individuals and groups acting on behalf of the regime will be referred to collectively as pro-government electronic actors.

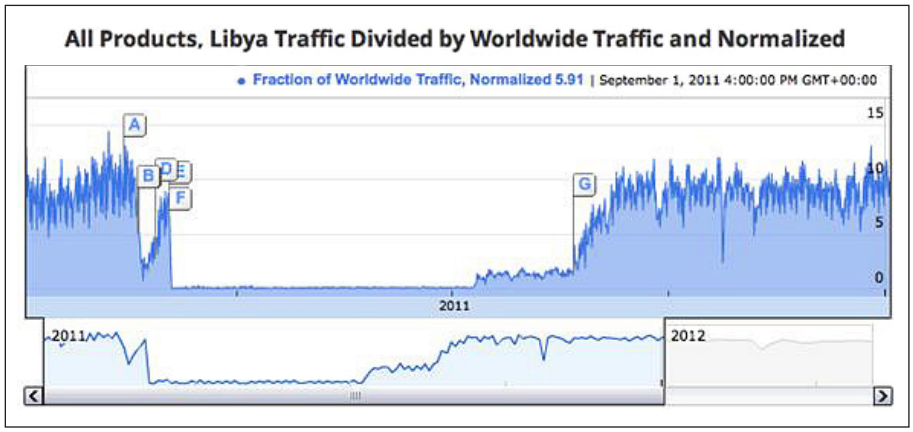


Figure 2.2 Google's Transparency Report reveals the almost complete block of Internet traffic to Google products beginning on March 3 "E" and "F"[29]

Simultaneous LAJ Attempts to Block Other Telecommunications

As the LAJ was working to cut Internet connectivity, it was also engaged in efforts to block other flows of information into and out of the country. Arabic-language television programming that reported on the uprising and that didn't hold to the LAJ line was a key target. Al Jazeera reported on February 17 that its program had been removed from the LAJ-owned cable networks.[30] Over the weekend of February 19, transmissions from two television satellites that served a wide range of news programming to Libya and the region were disrupted by jamming, according to the Lebanese Telecommunications Regulatory Authority.[31] And on February 21, Al Jazeera accused Libya of jamming its satellite transmissions in the region, and stated that it had conclusively identified the jamming as emanating from an LAJ intelligence services building south of Tripoli.[32]

Satellite telecommunications were not immune to LAJ disruption and denial efforts, which were likely targeted against the use of satellite telephones like the Thuraya handset, which were widely used in Libya. On February 25, Thuraya accused Libya of having engaged in a week's worth of jamming of the Thuraya-2 satellite that provided satellite phone and data connectivity to Thuraya devices within Libya.[33] Shortly thereafter, Thuraya announced that its technical efforts had restored voice services to much of Libya.[34] Nevertheless, users of Thuraya phones continued to experience substantial difficulty connecting throughout the revolution.

On March 3, the same day as the Internet shutdown took effect, Nic Robertson from CNN tweeted from Tripoli: "Security racheted up around #Tripoli, at same time, telephone internet access down."[35] Wireless and fixed-line telephone service interruptions didn't last in Tripoli, where some telephone services remained available throughout most of the conflict. The interruption of cell phone service was to become more permanent in eastern Libya, however, and wasn't reversed until over a month later, when Libyan opposition supporters with telecommunications engineering expertise separated Benghazi's wireless and fixed telephone networks from the Libyan national telephone network and made it autonomous.

Effects on Reporting

Attempts to limit the flow of information out of Libya extended to foreign journalists. Few foreign journalists were inside Libya when the conflict began, and the LAJ attempted to maintain this situation by refusing to issue visas to foreign journalists once the uprising began. A BBC World News editor, writing on February 20, 2011, highlighted the effect that this had on his organization's ability to effectively present the situation:

> The BBC and other news organizations are relying on those on the ground to tell us what's happening. Their phone accounts—often accompanied by the sound or gunfire and mortars—are vivid. However, inevitably, it means we cannot independently verify the accounts coming out of Libya. That's why we don't present such accounts as "fact"— they are "claims" or "allegations."[36]

The challenge that news organizations faced in establishing the authenticity of "citizen journalism" from Libya remained a theme of reporting throughout the conflict, and was probably satisfying to the LAJ. Nevertheless, as the conflict continued, news organizations developed deeper, more trusting relationships with on-the-ground sources, and many elements of the opposition developed media centers and more professional approaches to documenting conflicts, creating compelling products that made their way into news reporting.

It is worth nothing that the attempt to limit journalists' access to Libya ultimately evolved, and the LAJ began to allow journalists to enter LAJ-controlled areas, including Tripoli, provided that they stayed in the Rixos

Hotel in downtown Tripoli and left the hotel only with government minders on choreographed outings. While this successfully limited these journalists' view of the events in LAJ-controlled areas, it also drew unflattering attention to the regime's increasingly desperate attempts to control the discourse. Other journalists entered opposition-controlled areas in eastern Libya through Egypt, and the Libyan opposition, especially in its early days, was extremely open in providing them with access to the fighting. This reporting generated a steady stream of information that outweighed in volume of images, stories, and access to battles, the coverage from their colleges in Tripoli.

Discussion Questions

1. What kind of signal did Libya send the world when it shut down the Internet?
2. What kind of considerations are likely to have influenced the LAJ's decision to shut down the Internet?
3. How did blocking the Internet affect the credibility of news reports from the ground?

Notes

15. "Libyan Dictator Warns Against Using Facebook, Activists Arrested Following the Deposed Tunisian Dictator Footsteps in Suppressing Opponents," Arabic Network for Human Rights Information, February 13, 2011, http://www.anhri.net/en/?p=2101
16. Cajsa Wikstrom, "Calls for Weekend Protests in Syria," Al Jazeera, February 4, 2011, http://www.Al Jazeera.com/news/middleeast/2011/02/201122171649677912.html
17. T. A. Peter, "Libyans Turn Out in Hundreds to Protest Activist's Arrest," *Christian Science Monitor,* February 16, 2011, http://www.csmonitor.com/World/terrorism-security/2011/0216/Libyans-turn-out-in-hundreds-to-protest-activist-s-arrest
18. J. Cowie, "What Libya Learned from Egypt," Renesys, March 4, 2011, http://www.renesys.com/blog/2011/03/what-libya-learned-from-egypt.shtml
19. J. Cowie, "Libyan Disconnect," Renesys, Update March 4, 2011, http://www.renesys.com/blog/2011/02/libyan-disconnect-1.shtml
20. C. Labovitz, "Libya Firewall Begins to Crumble?," Default Free (blog), February 22, 2011, http://monkey.org/~labovit/blog//viewpage.php?page=libya_firewall_cracks
21. A. Dianotti, C. Squarcella, E. Alben, K.C. Claffy, M. Chiesa, M. Russo, and A. Pescapé, "Analysis of Country-wide Internet Outage Caused by Censorship," IMC'11, November 2–4, 2011, Berlin, Germany, http://www.caida.org/publications/papers/2011/outages_censorship/
22. Cowie, "What Libya Learned from Egypt."
23. Ibid.
24. Ibid.
25. J. Keating, "Someone in Libya Is Still Watching YouTube," Passport (blog), *Foreign Policy*, March 7, 2011, http://blog.foreignpolicy.com/posts/2011/03/07/someone_in_libya_is_still_watching_YouTube (registration required)
26. Interestingly, the first brief outages were based on router-level shutdowns similar to that applied by Egypt, although the presence of packet filtering was also observed. Some observers interpreted this to indicate that network administrators may have been testing filtering prior to implementing the March 3 Internet block.
27. A. Dianotti, "Analysis of Country-wide Internet Outages Caused by Censorship."
28. Specific evidence that these individuals were using the Libyan network for connectivity to conduct their attacks (and not, for example, two-way Internet) is circumstantial. However, in the case of one dissident whose online e-mail account was compromised, the account was later found to have been accessed by a computer operating from an IP address within Libya. Source: L9 to author, Personal communication, Fall 2011
29. Google Transparency Report, "All Products, Libya Traffic," divided by worldwide traffic and normalized, http://www.google.com/transparencyreport/traffic/?hl=en_US
30. "'Day of Rage' Kicks Off in Libya," Al Jazeera, February 17, 2011, http://www.aljazeera.com/news/africa/2011/02/201121755057219793.html
31. "Libya Source of Jamming of Lebanese News Channels: TRA," *Daily Star* (Lebanon), February 23, 2011, http://www.dailystar.com.lb/News/Politics/Feb/23/Libya-source-of-jamming-of-Lebanese-news-channels-TRA.ashx#axzz1Ev3JP000
32. "Jazeera Tracks Jamming Signal to Libya Spy Building," Reuters, February 21, 2011, http://af.reuters.com/article/libyaNews/idAFLDE71K2CV20110221
33. P.B. de Selding, "Thuraya Accuses Libya of Jamming Satellite Signals," SpaceNews, February 25, 2011, http://www.spacenews.com/satellite_telecom/110225-thuraya-accuses-libya-jamming.html
34. Ibid.
35. https://Twitter.com/#!/NicRobertsonCNN/status/43438546958303232
36. J. Williams, "The Difficulty of Reporting from Inside Libya," The Editors (blog), BBC News, http://www.bbc.co.uk/blogs/theeditors/2011/02/reporting_from_libya.html

CHAPTER
THREE

Tech That Turned the Net Back On

In the early days of the 2011 uprising, Libya's national telecommunications systems was heavily utilized by protesters, citizen journalists, and fighters alike. For example, on the front lines of the fighting in opposition-controlled parts of eastern Libya like Benghazi, most tactical and strategic communication made use of Libya's national cellular network and, in some cases, satellite telephones. Similarly, many of the most evocative videos of LAJ forces' and irregulars' actions against Libyan civilians in Benghazi were uploaded using the Libyan Internet. Cellphones as well as Voice Over Internet Protocol (VOIP) software like Skype also provided a means for news organizations and journalists to connect with Libyan sources for information "from the ground." All of this changed once the LAJ disabled Internet, landline, and mobile services beginning in early March.

Libyans responded quickly to the challenge, deploying a wide range of decentralized and ingenious solutions to re-establish connectivity, effectively undoing the denial of connectivity intended by the LAJ forces. As the Cyber Security Forum Initiative (CSFI) has pointed out, efforts to restore connectivity to Libyans both internally and by non-state actors were substantially faster than assistance via government channels.[37]

Interestingly, the communications shutdowns also rendered the Gaddafi regime's substantial monitoring apparatus for telephony and Internet communications deaf, instantly changing the information balance of the conflict. Libyan citizens who wished to maintain connectivity were driven to alternate, more decentralized forms of connectivity that didn't pass through regime-controlled networks. As will be discussed below, this may have triggered a substantial shift in LAJ efforts to intercept communications—which included deploying commercial cyber espionage tools.

Life Without the Internet

The loss of Internet and cellphone access had an immediate and dramatic effect on the communications ability of the Libyan opposition as well as

others throughout Libya. Libyans responded almost immediately with ad hoc efforts to maintain some form of communications. Initial solutions were highly labor-intensive and largely unable to replicate the connectivity or bandwidth that the opposition had enjoyed prior to the shutdown. The cellular phone shutdown, combined with jamming of Thuraya signals, for example, led opposition forces to temporarily resort to a very low-tech approach to communications:

> "We went to fight with flags: Yellow meant retreat, green meant advance," said Gen. Ahmed al-Ghatrani, a rebel commander in Benghazi. "Gadhafi forced us back to the stone age."[38]

On February 20, 2011, the BBC World News editor highlighted the effect of the Internet blackout on the material that they were able to draw from Internet and user-submitted sources:

> the flow of video—the so-called "user-generated-content"—has dwindled to a trickle as the authorities have periodically turned off the Internet. That means we have an additional responsibility—to be clear with our audiences not just what little we do know, but perhaps more significantly, what we don't.[39]

The trickle sometimes reflected a lot of labor-intensive processes, as video clips and news of the uprising had to be physically smuggled out of Libya and to the international media. One individual in Benghazi described transferring mobile phone video of the uprising to pocket flash drives and then transporting them into Egypt, where they could be uploaded.[40]

Two-Way Satellite Internet: Very Small Aperture Terminals

Without access to international and domestic Internet and telephone connectivity, many turned to two-way satellite Internet. Information is not available about the number of users of two-way satellite Internet in Libya prior to the 2011 revolution; however, the technology was frequently deployed in remote oil production installations and by others living far from urban areas. A typical two-way satellite Internet system, often referred to in Libya by its technical name of Very Small Aperture Terminal (VSAT), consists of three main parts: a dish, a modem, and a transmitter. VSAT systems transmit on a number of bands and receive data services from a number of international providers.

Libyan dissident Niz Mhani of the Free Generation Movement is seen within Tripoli in early July 2011, standing next to the VSAT system his group covertly used to keep up a steady flow of information critical of the Gaddafi regime. CNN pixelated his face to preserve his anonymity.

The system has a number of drawbacks that limit its wider use: data transfer is slower than typical Internet installations; it is often more expensive; and transmissions can be interfered with by bad weather or jamming. What became clear, however, is that the 2011 Revolution caught dealers of two-way satellite Internet in opposition-controlled towns like Benghazi and Misurata with stocks of satellite dishes and equipment, as well as the necessary relationships with service providers to register and maintain user accounts. In the first weeks of the conflict, the number of VSAT systems proliferated, either assembled from components already present in Libya as merchandise, "liberated" from government installations, or smuggled into opposition-controlled territory from abroad.

Less commonly used in most of Libya were broadband global area network (BGAN) devices. These are highly compact two-way satellite antennas with built-in data modems, mainly employed by journalists. BGAN devices also found their way to the opposition in specific areas, notably the Nafusa Mountains.[41]

Vignette: Misurata Reconnects with Two-Way Internet[42]

When the siege of Misurata began, Libyan opposition supporters in the city sought ways to show their plight to the world. As one Misurati active in supporting opposition military forces described it, they wanted to "cry for help . . . there was no great plan to ask . . . for a solution . . . [it was simply] a natural reaction" from a "human being who is being threatened."[43] When the Internet was cut, the mobile video they had captured of shelling and skirmishes with LAJ who had advanced on the city couldn't be broadcast, nor could they call Al Jazeera or the BBC to report on casualties. Encircled on three sides by LAJ forces, the Misuratis were isolated.

There was, however, a solution in the stocks of a two-way satellite distributor based in the city. As several Misuratis have described it, the distributor realized the value of what he had to the conflict and began to provide installations of two-way satellite connectivity to key strategic locations within the city. This individual also arranged for uninterrupted services to be provided to the VSAT systems he had installed, coordinating with his supplier in a Gulf country. As one Misurati who hosted several installations recalled, the dealer would say, "Once we are done, we will talk about the money." With the arrival of the first chartered ships bringing aid and other materials to Misurata from Malta, Tunisia, and Benghazi, the number of VSAT systems in the city swelled.

VSAT systems were soon installed in operations rooms throughout Misurata and used to provide communications support to military operations, the local councils, humanitarian and medical aid coordination groups, and media centers. As the fighting continued, fronts expanded, and key areas like the airport were retaken, they too were equipped with operations rooms and VSAT connectivity. Connections were actively monitored by shifts of people tasked 24/7 to answer incoming calls and maintain lines of communication.

VSAT systems remained in use in Misurata after the fight for the city ended and the battlefield moved outward, toward the east and west. They continued to provide communications between forward operating positions and operations rooms, as well as connections to journalists. Beginning in summer 2011, businessmen in Misurata established their own "operations room" with a VSAT connection that allowed them to contact their business partners to order materials and goods from outside, brought through the increasingly frequent boats from Malta, Tunisia, and Benghazi. By the end of the con-

flict, several Misuratis agree, there were at least 100 VSAT systems active in the city.[44] It is also worth noting that, as journalists began to enter the city, Misuratis offered them access to their VSAT connections at hotels and media centers.

Libyans Abroad Who Topped Up VSAT Accounts

Two-way satellite Internet, much like normal Internet services, requires a subscription with a service provider. Higher bandwidth connections, however, are often substantially more expensive than traditional Internet services, and charges frequently reflect data usage, creating a need for constant infusions of credit into highly active accounts. Libyans overseas would often contribute to the cause by purchasing credits for opposition figures whom they knew, sometimes unprompted.[45] A recent article documents the process, describing how a non-Libyan supporter of the opposition gained the trust of opposition figures in order to let her pay for their connections.[46]

Other Communications Technologies That Restored Connectivity

Although VSAT systems provided a wide range of communications functionality, Libyan opposition members worked to re-establish connectivity by making extensive use of tools like satellite phones and two-way radios. They also reconnected and reconfigured telecommunications infrastructure for landlines and mobile phones. While outside the scope of this case study, it should also be noted that "free" radio stations and newspapers emerged in opposition-controlled areas, providing pro-opposition news, information, and calls to arms. It is likely that captured radio stations served a dual morale and propaganda function, as their signals are likely to have been audible outside areas controlled by the opposition.[47]

Restoring the Cellphone and Landline Infrastructure

When LAJ forces disconnected mobile and landline telephony in Benghazi, these services were entirely unavailable for more than a month, forcing the Libyan opposition to adopt a wider range of innovative communications solutions. The convenience and ubiquity of existing landline and mobile infrastructure, combined with the LAJ jamming Thuraya signals, led opposition supporters to restore a localized telephone network that could operate using infrastructure and switches entirely located in opposition-controlled

territories.[48] After a month of effort, a Libyan-American telecommunications executive, with the support of the U.A.E. and Qatar, led a team of engineers that modified the Libyan network to provide domestic cellular services to Benghazi and other opposition-held areas. Equipment was provided by Gulf countries and others, not directly by the original manufacturer, Huawei Technologies, which refused to sell the compatible hardware to the opposition.[49] The engineers also made use of a captured database of existing numbers to help restore services. As the *Wall Street Journal* pointed out:

> Without Huawei, the backing from the Persian Gulf nations became essential—otherwise it is unlikely that international telecom vendors would have sold the sophisticated machinery to an unrecognized rebel government or individual businessmen, according to people familiar with the situation.[50]

The newly operational telephone system was attached to international telecommunications networks via satellite. Initially, although these phones were able to connect within the network, only a few connections to the global telephone network were made, reserved for the use of key opposition figures. In the early days of access to the restored system, all local calling was unbilled. As connectivity expanded, access to cellphones dramatically improved communications for a growing circle of opposition members, not just between the city and the front lines. It also improved their ability to connect to supporters and family abroad to negotiate for international support and weapons supplies, and to discuss strategy with envoys.

Although eastern Libya received much more media attention at the time, it wasn't the only area where connectivity was restored. In June 2011, some of the same people who worked to restore connectivity in Benghazi traveled covertly to the besieged city of Misurata to undertake a similar project, with training and material assistance from Dubai and other Gulf states as well as an international group of opposition supporters. Some groups traveled to the city to assist in restoring electricity and other utilities, and telecommunications engineers began restoring base stations and rebuilding the Misurati network.[51] According to a Misurati telecommunications expert familiar with the installation, the internal network was readied by July and became operational in early August. By the end of August, however, the temporary network was disassembled, and the communications infrastructure plugged back into Libya's larger network.[52] Because the connection was implemented much later in the year than Benghazi's network, Misuratis,

like opposition forces in western Libya, were left without telephone or cellular service for the majority of the conflict.

Radios

The use of tactical radios by the Libyan opposition grew after the conflict began; however, most of their communication took place on insecure, unencrypted, and unscrambled handheld radios. One Libyan who was involved with establishing a communications system during the battle of Bani Waleed in September and October 2011 described the network through which battlefield reports and command and control communications took place. Unencrypted radios were used on the battlefield to communicate from the front lines to forward operations rooms; VSATs were then used to communicate back to central operations rooms.[53]

Although a small number of encrypted radios were eventually introduced into the opposition forces, most radios were apparently used for communications in the clear. The risk associated with the use of unencrypted radio during the conflict was evident, and Misuratis invented a series of word codes and pseudonyms to conceal their true meaning from LAJ forces. "We knew that the Gaddafi regime was listening to the radios," said one Libyan familiar with the city's tactical communications infrastructure. Sometimes, he explained, the ability of both sides to hear each other led to a somewhat less tactical use: trading insults with opposing forces over open channels.[54] Similar stories are told by an opposition operative familiar with the situation in the Nafusa Mountains.[55]

Satellite Phones

Libyans made extensive use of satellite phones despite their limitations, which included difficulties with connectivity, cost, rapidly draining batteries, and the need for callers to stand in exposed locations to make calls. As an opposition supporter pointed out, satellite phones also needed topping up with credit like VSAT services. VSATs simplified the process, making it possible to use the Internet to make top-up purchases of credit, but in many cases relatives and others abroad purchased credit for in-country opposition supporters.[56]

The persistent attempts by the Gaddafi regime to thoroughly jam Thuraya phone services were not effective in denying full access to it or to other satellite phone networks, including Irridium and Inmarsat. In response to

the use of satellite telephones, the regime issued a threat of execution against "un-authorized" Thuraya users in early August 2011.[57] As the conflict grew, an increasing number of users migrated from Thuraya to other networks, both because of the interruptions associated with the intermittent jamming as well as a strong perception among many in the Libyan opposition that the Thuraya servers were especially vulnerable to LAJ signals intelligence or some other form of unspecified interception. The perception seemed to be partially due to the existence of commercial agreements between Thuraya and Libyan companies.[58] It would become clear after the conflict ended that this concern was at least in part well-founded: the LAJ was found to have training materials for the L3 Communications Tactical Thuraya Monitoring System, an interception and localization package developed for field-deployed signals intelligence applications.

A Note on Outside Support for Internet Reconnection

As Libyans scrambled to secure tools that would help them communicate without the Internet or cellphone networks, a number of online hacktivist groups including Telecomix and Anonymous, following a model deployed in Egypt, began posting instructions to Libyans about various strategies to circumvent the Internet shutdown, including dial-up numbers for modems and other strategies.[59] It remains unclear how extensively these materials and tools were used. Ultimately, it was Libyans themselves who deployed the technologies that restored their connections to the Internet.

Discussion Questions

1. What immediate effects did the Internet shutdown have on the Libyan opposition's communications ability?
2. What kind of trust was required to maintain satellite phone and VSAT connectivity?
3. In what ways did access to two-way satellite Internet (VSATs) transform Misurata's strategic position? How might their situation have been different without access to the Internet?
4. In what ways was the Libyan opposition able to create a communications structure that could serve both military and civilian needs? Can you think of key areas that the opposition did not address?

Notes

37. Project Cyber Dawn, Cyber Security Forum Initiative, April 17, 2011.
38. M. Coker and C. Levinson, "Rebels Hijack Gadhafi's Phone Network," *Wall Street Journal,* April 13 , 2011, http://online.wsj.com/article/SB10001424052748703841904576256512991215284.html
39. J. Williams, "The Difficulty of Reporting from Inside Libya," The Editors (blog), BBC News, http://www.bbc.co.uk/blogs/theeditors/2011/02/reporting_from_libya.html
40. D. Zucchino, "Telling Libya's Story over the Internet," *Los Angeles Times,* February 27, 2011, http://articles.latimes.com/2011/feb/27/world/la-fg-libya-information-20110227
41. Personal communication with L7, L8, Spring 2012.
42. This vignette is compiled from the narratives provided by three Misuratis who were active in the fighting.
43. Personal communication with L1, Spring 2012.
44. Personal communication with L8, L1, Spring 2012.
45. Personal communication with L8, L1, Spring 2012.
46. J. Pollock, "People Power 2.0: How Civilians Helped Win the Libyan Information War," *MIT Technology Review,* April 20, 2012, http://www.technologyreview.com/web/40214/
47. "New Media Emerge in 'Liberated' Libya," BBC News, February 25, 2011, http://www.bbc.co.uk/news/world-middle-east-12579451
48. M. Coker and C. Levinson, "Rebels Hijack Gadhafi's Phone Network." *Wall Street Journal,* April 13, 2011.
49. The U.S. House of Representatives Permanent Select Committee on Intelligence's October 2012 report highlighted the links between Huawei, ZTE, and the government of China: "Most importantly, that preliminary review highlighted the potential security threat posed by Chinese telecommunications companies with potential ties to the Chinese government or military. In particular, to the extent these companies are influenced by the state, or provide Chinese intelligence services access to telecommunications networks, the opportunity exists for further economic and foreign espionage by a foreign nation-state already known to be a major perpetrator of cyber espoionage." These connections are important aspects of the early 21st-century information environment and cyberspace operations, and it is important that readers understand that many nations around the world have Huawei and ZTE products installed in their communications networks. U.S House of Representatives Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE,* October 8, 2012, iv.
50. Ibid.
51. C. Huang, "Dubai Telecoms Engineers Supply Libyan Rebels with Mobile Phone Network," *National* (UAE), July 1, 2011, http://www.thenational.ae/news/world/africa/dubai-telecoms-engineers-supply-libyan-rebels-with-mobile-phone-network
52. Personal communication with L2, Spring 2012.
53. Personal communication with L1, Spring 2012.
54. Personal communication with L1, Spring 2012.
55. Personal communication with L3, Spring 2012.
56. Personal communication with L1, Spring 2012.
57. H. Bar, "Libyan Rebels on Offensive 6 Months into Uprising," AFP, August 11, 2011, https://ph.news.yahoo.com/news/libyan-rebels-offensive-6-months-uprising-090727205.html
58. See, for example, this press release from Thuraya: "Thuraya to Launch Post-Paid Mobile Satellite Services in Libya in Libya," November 8, 2010, http://www.thuraya.com/userfiles/files/Media%20Releases/2010/thuraya%20post%20paid%20mobile%20satellite%20service%20libya.pdf
59. Project Cyber Dawn, Cyber Security Forum Initiative.

CHAPTER
FOUR

The Public Face of a Networked Opposition

Getting Information Out (and Sometimes Back In)

As some commentators pointed out while the Libyan revolution was still underway,[60] the low penetration rates of Internet usage make it hard to argue that sources like Facebook or Twitter could have had a direct causal role in providing the population with information or views that would lead to a revolution. Certainly, information posted on a Facebook group in the first days of the revolution is unlikely to have reached even a small fraction of the Libyan population via web browsing.

Indeed, it seems likely that, like much of the rest of the Arab world, Al Jazeera was a much more widely watched source of information about the revolutions in neighboring countries. What, then, was the role of information put online during the first days of the Revolution? Free Internet services, including Facebook, Twitter, and YouTube, played a key role in getting information out of Libya, even after the Libyan government shut down the Internet. Propelling highly charged images, messages, and information into social media brought them to the attention of the international media and many other stakeholders. Once they reached widely watched channels like Al Jazeera, Al Arabaya, BBC, and CNN, many of these images were beamed back into Libya. Libyans who had posted them online were, albeit indirectly, broadcasting to the world, as well as back into Libya.

In a media environment where there was a strong, sometimes explicit, intuition that other countries would follow, evidence was eagerly sought for indicators that uprisings were beginning elsewhere. Access to social media allowed Libyans both inside the country and in the diaspora to post and read messages calling for protest. In the second week of February, 2011, these messages reached Libyans indirectly, as international media organizations like Al Jazeera reported on calls to protest and speculated about whether an uprising might be expected for Libya.

As videos and tweets and social media postings began circulating online, painting a picture of the extent of the protests and the violence of the LAJ response, they were picked up by international news organizations. This challenged the messaging of the Gaddafi regime, which went to great lengths to portray Libyans as firm supporters of Gaddafi and unsuccessfully tried to downplay the significance of these statements. It also created the appearance of widespread support for the revolution. One reporter observed:

> there has been another critical factor at work that has ensured that social media has maintained a high profile in these revolutions. That is the strong reliance that mainstream media such as the Doha-based television network Al Jazeera has had to place on material smuggled out via Facebook, YouTube and Twitter. This arrangement means that videos have often been broadcast back in to the country of origin – when Al Jazeera has managed to avoid having its signal blocked.[61]

Sultan Al Qassemi, an influential commentator on the Arab Spring who maintains a widely followed Twitter feed,[62] explained how he saw the role of social media in the Arab Spring:

> Where social media had a major impact was conveying the news to the outside world, bloggers and Twitter users were able to transmit news bites that would otherwise never make it to mainstream news media. . . . This information has been instrumental in garnering the attention of the citizens of the world who expressed solidarity with those suppressed individuals and may even put pressure on their own governments to react.[63]

As the revolution continued to grow and as Internet connectivity was restored, two-way Internet connections made possible a rapidly available stream of reports, video, and voices documenting LAJ forces' actions from inside the country. International media was able to call directly into fierce battles and otherwise inaccessible areas and receive a live update on the events. Libyan expatriates and exiles meanwhile maintained websites and Twitter feeds that aggregated and sometimes broke news about the conflict or solicited material support for aid and donations.

Before international correspondents were able to enter the besieged city of Misurata, for example, a number of increasingly organized groups began documenting the fighting using techniques that have come to be associated with citizen journalism. Sometimes these groups referred to themselves as

"media committees," "media centers," or "information committees." They took video cameras with them to the front lines, documented the fighting, and uploaded the material on Misurata-specific pages and channels on social media sites like YouTube and Facebook. All of this content flowed through two-way satellite Internet, maintained on VSAT terminals. These efforts were complemented by Misuratis' near-constant communications with international media via Skype voice and video calls, again over two-way satellites. Articulate and compelling voices, especially doctors, were reliably available to speak to media at all hours and to present evidence of the city's plight in the form of casualty numbers and descriptions of the wounded. As the fighting went on, this grew to include information about material captured from LAJ forces and updates on battles. Many Misuratis agree that the arrival of international correspondents was a turning point for increasing the international attention paid to Misurata. Still, as one remarked, "If it wasn't for the Internet and Skype, the world would have never heard of anything that went on in Misurata."[64]

The "Official" Revolution Facebook Page

In Libya, where public expression of dissent was rare prior to the revolution, some of the earliest public calls to protest could be found on Facebook. The "Day of Rage" Facebook page,[65] for example, which called for protests on February 17, 2011, received attention from Al Jazeera and other news media organizations shortly after it was created. Reports on the calls to protest were often accompanied by descriptions of the numbers of individuals who had "liked" or "joined" these calls. Al Jazeera actively reported on the page prior to February 17, noting that the site had had 4,400 followers on February 16 and that it had doubled to 9,600 followers the following day.[66]

Facebook was used extensively during the revolution, with both real-life and electronic groups and individuals creating a dramatic volume of pages in support of the uprising. The trend continued as the military element of the conflict wound down. In December 2011, the scale of this growth became clearer. Metrics of Facebook penetration rates indicate that Libya briefly became Facebook's fastest growing country in terms of national users, with a 588.86% increase in users from June to December 2011, to 316,000 users.[67]

Figure 4.1 Advertisements for a revolution. The advertisements provide advice about how to change DNS servers to make blocked sites available and encourage users to click to visit Libyan opposition websites. Metrics shown to the author indicate that the first advertisement was shown 33,365 times to Facebook users registered in Libya, the second to 41,037 users.[68]

Vignette: Advertising for Revolution

One young Libyan Internet user living in North America decided prior to the beginning of mass protests on February 17 to encourage other Libyan Internet users to access Libyan opposition websites.[69] His strategy? In what might be the first case of online advertising for a revolution, the 24-year-old purchased advertising space on Facebook targeting its 316,440 users who were registered as living in Libya. He designed his own small advertisements that encouraged Libyans to visit opposition websites and provided them with advice about how to circumvent regime IP filtering by changing their domain name servers (DNS).[70] When the opposition website he'd been directing viewers to was subjected to attack, he produced new advertising encouraging Libyans to visit the Day of Rage Facebook page. His reasoning was that the Facebook site could much better withstand any attempt at a distributed denial of service (DDoS) attack. His advertisements were displayed over 7 million times and resulted in over 60,000 clicks, 50,000 of them to the "official" site of the revolution, and they ran until the Libyan government decisively implemented the Internet blackout.

Opposition Websites

Prior to the revolution, many Libyans relied on opposition websites for news and opinion that challenged the Gaddafi regime's control of informa-

tion. Websites like Libya News and Views,[71] maintained by an expatriate, aggregated reporting about the country, and its politics didn't track the LAJ's official line. If some websites focused on gathering and providing news that were stifled, others, like Enough Gaddafi,[72] more directly lobbied for the departure of the Gaddafi regime. As calls for protest grew, these and other opposition websites began posting calls to protest, and in some cases hosting messages from Libyans urging others to join in the protest.[73]

A number of websites were established to serve as clearinghouses for information about the uprising. These sites aggregated and monitored Libyan social media feeds as well as international news or directly reported news and information from sources within the country. The largest of such sites, http://feb17.info, became a clearinghouse for information on the events in Libya. Media outlets used the site as an information source and a reliable ticker for events in Libya. It received millions of comments and even more traffic.[74] Another website, www.libyafeb17.com, played a similar role, albeit at a somewhat smaller scale. These sites' impact was impressive, especially given the sometimes small number of people staffing them. As the operator of feb17.info posted about the experience:

> As a matter of fact, we were only a team of 2 people! That's right, only two of us. Myself and my wife Sanne. My name is Haret Alfasi and I am a 24 year old Libyan raised in the UK. Tinkering with websites since the age of 12 led me down the path of web development which is what I do for a living. . . . At its peak, Libyafeb17.com was two laptops and a 19" Samsung monitor.[75]

Others brought a range of technical skill sets to documenting and reporting on the uprising. A website hosting a map of Libya that documented acts of violence against protesters and the shifting territories under the opposition and LAJ control was viewed over 314,000 times in the first 12 days of the revolution.[76]

Ad hoc groups and individual users were not alone in aggregating and "curating" social media information about the Libyan Revolution. Major news organizations including the *New York Times,* the *Guardian,* the BBC, Al Jazeera, and Reuters all maintained live-blog-style websites that compiled material in a streaming or continually updated format, often in a fusion of their own reporting, tweets, updates from the wire services, and so on.

Vignette: Mohammed Nabbous, Citizen Journalist

In the early days of the revolution, an articulate young Libyan man, Mohammed Nabbous, burst into prominence as a citizen journalist carrying updates from Libya to the world. Nabbous, who had operated a small Internet service provider in Benghazi, took advantage of his expertise and access to resources to set up a live broadcast of events taking place using the freely available functionality of the Livestream.com website. Livestream allows users to set up live-streamed video and audio feeds, while requiring only minimal technical expertise. Nabbous created a feed which he titled "Libya Alhurra,"[77] or "Free Libya." He began by installing a series of cameras at the Benghazi courthouse, which he streamed beginning on February 19, sometimes all at once and sometimes in tiled windows. The feeds made it possible to watch raw, real-time feeds of protesters as they marched in the main square, and they illustrated the scope of civilian support for the uprising and the varied demographics of the protesters.

On February 19, Nabbous began with a plea: Speaking into the camera, he requested international support for and attention to the violent response of LAJ forces to the Benghazi uprising. In one of his first videos, broadcast live, he can be seen talking via Skype with a journalist as he broadcasts the feed, sometimes repeating himself to answer her questions over the low-bandwidth connection. In the first video, reposted on YouTube, his message is clear, and compelling:

Screenshot of Mohammed Nabbous speaking during his first broadcast.

> How can you people just watch us being killed? . . . if we actually die there is . . . another group of my people . . . they're going to be online with you tomorrow so you can see how many funerals . . . how many people get buried. . . . I can't assure that I'm going to be alive in five minutes . . . I'm not afraid to die, I'm afraid to lose the battle . . . that's why I want the media to see what's going on.[78]

Nabbous quickly became a key point of contact for international media seeking to cover the uprising. He used his Skype connection to do live interviews with major international news organizations including CNN, Al Jazeera, and the BBC.[79]

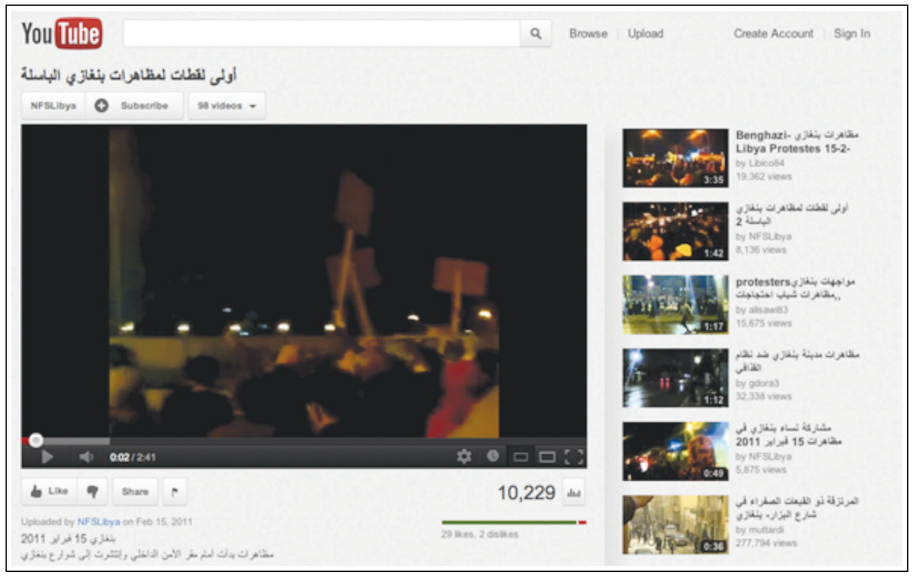
Nabbous's Livestream channel was watched by over 452,000 unique viewers in the first six weeks of the uprising, a volume that has been calculated at a total of 25 million "viewer minutes."[80] His feed didn't just attract viewers: a group of supporters and facilitators both in Libya and outside the country joined to help promote the feed and engage in various support activities. Assisted by a group of international supporters, he increasingly took on a role similar to a correspondent: taking his car and his camera to the front lines, investigating the aftermath of attacks, and even "broadcasting" information back to his Livestream via cellphone calls. Nabbous was shot dead on March 19 while reporting on apparent evidence that LAJ forces were not respecting the UN-demanded ceasefire of March 17, 2011 (UN Security Council Resolution 1973).

Compelling Video

The video-sharing website YouTube played a key role in disseminating video content from Libya. The first days of the conflict were marked by a series of videos, including some of the earliest evidence of protests in Benghazi from February 15 and disturbing footage of the LAJ forces' attempts to quash the rebellion. These videos were often shaky and amateurish, captured with cellular phones. In retrospect, it seems clear that the early video clips, sometimes accompanied by the filmers' commentary, helped an international audience see apparent eyewitness accounts of the Gaddafi regime's responses to Libyan protests.

In the early days of the conflict, for example, a YouTube channel maintained by the exiled opposition group the National Front for the Salvation of Libya hosted some of the earliest clips of protest in Libya, including a protest that took place on February 15.[81] These videos and similar ones were often multiply posted by individual accounts, and as the conflict went on, also posted to specific pro-opposition channels.

In the early days of the conflict, for example, a YouTube channel maintained by the exiled opposition group the National Front for the Salvation of



"First footage from the brave Benghazi demonstrations," YouTube video posted February 15, 2011 by the National Front for the Salvation of Libya

Libya hosted some of the earliest clips of protest in Libya, including a protest that took place on February 15.[81] These videos and similar ones were often multiply posted by individual accounts, and as the conflict went on, also posted to specific pro-opposition channels.

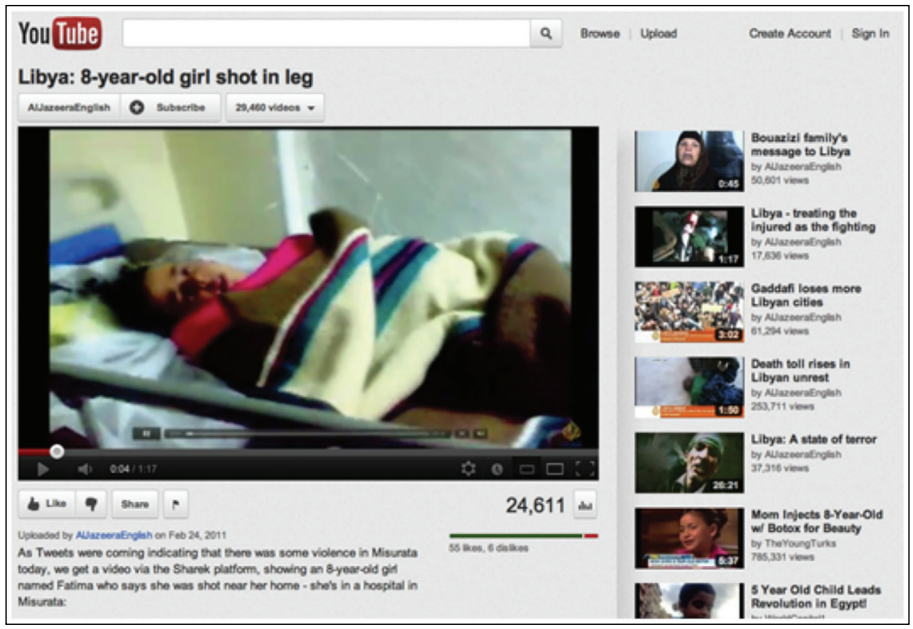
Videos posted on YouTube could quickly reach both domestic and international audiences. While many received substantial traffic on YouTube itself, the site also served as a mechanism to provide media content to news organizations that often rebroadcast them, sometimes with caveats about their inability to confirm the images' veracity. On February 22, for example, YouTube user "muttardi" posted a video titled "Yellow Hat Mercenaries – Bazaar St. Benghazi," showing men wearing yellow hard hats and raiding a Benghazi street.[82] Interestingly, YouTube's statistics indicate that the video received substantial viewership in Libya, suggesting a domestic audience in the early days of the revolution.

Yet the video wasn't limited to internal consumption. Like many others, it was quickly shared on multiple social media sites, including Facebook, where other users had reposted it. An embedded video on Facebook appears to have quickly driven over 9,000 viewers to the video almost as soon as it

was posted. Soon thereafter, the video was picked up by Al Jazeera's Live Blog,[83] which drove another 14,600 views. This, along with the rush of views to the original posting, appears to have propelled the video to YouTube's home page, which quickly generated more than 30,800 views. In less than 24 hours, the video was circulated globally, picked up in online postings by the Spanish El Pais,[84] the Belgian Het Nieuwsblad,[85] the French Liberation,[86] the German Der Spiegel,[87] and many other news organizations.

Recognizing the power of user-generated content, news organizations sometimes sought to directly solicit material. Al Jazeera, for example, had introduced a platform called Sharek that allowed its viewers to submit video and other content to the news network. According to Al Jazeera's head of social media, up to 1,600 videos a day were submitted to the site during the Arab Spring.[88] Videos from Libya were among the many from the Sharek platform that apparently made it onto the network's broadcasting. The content sometimes included highly troubling images of the civilian toll of war, or possible human rights violations. In the early days of the siege of Misurata, for example, a widely viewed video uploaded through

"Yellow Hat Mercenaries – Bazaar St. Benghazi." Note the hand holding what appears to be a cellphone or camera, also recording the scene.[89]



"Libya: 8-year-old girl shot in leg." The caption reads: "As Tweets were coming indicating that there was some violence in Misurata today, we get a video vie the Sharek platform, showing an 8-year-old girl named Fatima who says she was shot near her home – she's in a hospital in Misurata." [90]

the platform showed a young girl in a cast in a hospital bed, identified as an 8-year old, who describes being shot in the leg near her home.[91] Like many similar videos, it was subsequently mentioned and embedded in a number of outlets, including the *New York Times'* blog.[92]

As the conflict escalated, an increasingly sophisticated group of Libyans and Libyan opposition supporters supplemented the amateur and user-generated content by working to create more streamlined and informative content documenting the many features of the conflict, from humanitarian and logistical topics to video of battles, martyrs, captured material, prisoners, and evidence of potential human rights violations. Other videos showed behavior on the part of the LAJ forces that appeared to violate international norms of warfare. In many opposition-controlled areas, these documentary groups took over responsibility of covering the front lines, attempting to avoid compromising the operational security of the opposition, and adopting various practices for increased personal safety and security.

Some video was too graphic to make it onto Western news, although it spread widely online. Other compelling video made it into the news,[93] either provided directly or through journalists' vetting of material posted online, known as user-generated content. YouTube's role continued to be a key part of how international observers and consumers of media were exposed to the conflict: even Gaddafi's final moments were captured and posted to YouTube by dozens of Libyans, perhaps more.

The Libyan Opposition on Twitter

From the early days of the revolution, Twitter provided a constant stream of updates and information. Some accounts provided dispatches from the situation on the ground, with varying degrees of precision and objectivity. Others aggregated reporting and news on the Libyan conflict in mainstream media sources or aggregated information from other users. Yet the use of Twitter didn't end with journalistic transmission of information. Other Twitter accounts provided running commentary and dialogue about the conflict, as well as how it was covered. Key public personalities in the uprising like activist Guma al Gumaty[94] maintained feeds, as did many other actors in the conflict, some using pseudonyms like @changeinlibya.[95] They weighed in on issues or highlighted developments, and encouraged their followers to attend protests abroad. The influential commentator and Twitter user Sultan Al Qassemi named some of the other uses of social media during the early days of the uprising:

> Other uses for social media were to transmit information on medical requirements, essential telephone numbers, and the satellite frequencies of Al Jazeera—which is continuously being disrupted.[96]

In other cases, Twitter users used open-source information and personal contacts to gather information about LAJ figures abroad, posting personal phone numbers and other details of LAJ ambassadors and encouraging their followers to call them.[97] Notably, Twitter was also used in an attempt to directly influence the outcome of the conflict by providing information to NATO.[98]

In the earliest days, this included feeds that had existed prior to the uprising, including the Twitter feed of the National Front for the Salvation of Libya[99] and a Twitter feed associated with Enough Gaddafi,[100] both of which also maintained websites. As the conflict began, a second wave of Twitter

accounts emerged, some manned by individuals tweeting from inside Libya, others by members of the Libyan diaspora or other supporters who used phones and Skype to call into Libya to get updates.

The number of tweets grew rapidly, creating a volume and pace of material so great that it could not be monitored as a single feed without some form of filtering. As had been the case in Egypt, Twitter users engaged with Libya converged on a set of hashtags like "#feb17," "#Libya," and "#Tripoli" that they often appended to their messages to identify tweets as relevant to the revolution and make them easy to find.

The mainstream media paid a great deal of attention to Twitter as a source of information during the conflict. This usage wasn't limited to breaking news or pointing their followers to stories. Journalists and media organizations reported on events as "being reported on Twitter" as they developed, often before the same events were able to be reliably confirmed and reported through the major wire services. In other cases, specific journalists engaged directly with Twitter, using it to curate and refine citizen journalists' and Twitter users' coverage of the events, even enlisting their followers to engage in tasks like identifying ordnance used in the fighting. Journalists and other Twitter users sometimes used replies to tweets (public) or direct messages (private) to contact potential sources for interviews or to request clarification of a particular piece of news. This attention was tempered by the difficulties that news organizations faced in quickly confirming much of the tweeted information. In some cases, this reflected news organizations' limited on-the-ground access to correspondents and verifiable sources throughout all of Libya. Rumor and exaggeration were amplified, making it difficult for a casual observer to sort through the high volume of tweets.

The account of the Libyan Youth Movement (LYM) was one of the most widely followed Twitter feeds of the 2011 Libyan Revolution and provides a window into the many ways in which Twitter was used to cover the uprising. The group's Twitter feed, @ShababLibya, was initially run entirely by a small group of young Libyans based in the diaspora who operated the feed in contact with relatives and friends on the ground. It gained prominence early in the uprising for its near real-time information and commentary in support of the opposition, and quickly became a nexus for information

from inside the country as well as news updates. These grew to include details about NATO strikes, aid needs, reports of atrocities, and recorded telephone calls into Libya. At points the group also had members inside Tripoli who complemented the tweeting from the outside. The group, which also operates from a Facebook site, describes itself thusly:

> We are a group of Libyan Youth both in & out of Libya inspired by our brothers & sisters in Egypt & Tunisia. We'll do our best to bring Libya back Inshallah.[101]

The Twitter feed remains active today, with more than 65,000 followers and more than 22,000 tweets. It is largely managed and operated by Ayat Mneia, a young Libyan-Canadian. The LYM fielded an impressive range of media requests, and its members sometimes appeared directly on Al Jazeera. In other cases they worked to connect journalists with sources, a widely practiced but under-acknowledged element of the reporting on the Libyan revolution. The tweets from within Libya, often telegraphing information that hadn't yet been verified by news organizations or found on news wires like AP and Reuters, frequently provoked responses from journalists seeking further information. At times, the tweets themselves were reported as news. As the conflict continued, the LYM and others became more sophisticated in presenting information, adopting an increasingly journalistic style, including conventions like "Breaking:" to describe developing news, and more carefully highlighting the reliability of information. Along with many other Twitter feeds, it attempted to increase the accuracy of NATO strikes by tweeting targeting information.

Although groups like the LYM were primarily supported by Libyans, some supporters came from outside the Libyan community, such as Janice Clinch from Ontario, Canada:

> The 59-year-old has never met anybody from Libya. She has not visited the Arab world; chronic pain makes it hard for her to get around. But from her home near Seeley's Bay, 40 kilometres northeast of Kingston [Ontario, Canada], she joined a committed cadre of social media users who have become, in effect, volunteer intelligence analysts. On Twitter, Facebook and other services, they discuss satellite images, vessel tracking data and the latest gossip from their sources inside the country.[102]

Ms. Clinch's engagement extended beyond simply relaying news and information from Libyan social media sources:

> Months of online activism earned her a role as administrator of the Libyan Youth Movement page on Facebook—the only non-Libyan honoured with the job, she says—and on Monday she noticed that a regular member, somebody located in western Libya, had pinpointed a gas station converted into a temporary headquarters for Col. Gadhafi's forces. She tweeted the co-ordinates, along with the longitude and latitude of a few other targets passed along from the same source, asking NATO to "clean up" the government troops.
>
> Ms. Clinch was not sure whether NATO had bombed those locations, but she continued to scour the Internet for more leads.[103]

It is difficult to provide an easy set of categories that describe how many pro-opposition accounts covered the conflict. Clearly Ms. Clinch and LYM weren't just amplifying, curating, aggregating, or transmitting information from citizen journalists. Although the feeds clearly sought to influence people's perceptions of the conflict and enlist international support, they also were viewed by many as a mechanism to more directly support the military campaign in Libya.

Many Twitter reporters didn't just seek to provide targeting information to NATO; they also enthusiastically reported on NATO's actions, tracking airstrikes, explosions, and other evidence of NATO activity even as they encouraged NATO to attack certain coordinates. After an airstrike, for example, information obtained via communications with in-country contacts would emerge on Twitter within minutes, highlighting potential NATO successes or posting messages about how the targeting could be improved. This kind of information, NATO has acknowledged, was included in their post-strike damage assessments.[104]

The theme of reporting on NATO activity extended to radio transmissions that took place in the clear. For example, recordings of NATO airborne Psychological Operations (PSYOPS) broadcasts directed towards the LAJ forces and the warble of jamming on the same frequency made their way online. Information about the number of explosions, material destroyed, or amplification of PSYOPS messaging is likely to have improved NATO forces' situational awareness. In these cases, it is also unlikely to have posed

a threat to NATO's operational effectiveness, since it could be assumed that LAJ forces would have access to the same information.

Twitter reporting on NATO activities may have introduced new operational risks by, for example, reporting on the movement of NATO forces' aircraft in near-real time. In one case, an amateur radio enthusiast who monitored air traffic control frequencies picked up transmissions associated with NATO combat operations. When military airplanes would "go tactical" as they entered Libyan airspace, social media users would re-tweet scanner reports noting the transmission and wait to report on the expected strikes. It is unclear what, if any, operational value this might have had to the LAJ.

Vignette: Tripoli and the Free Generation Movement

On June 7, CNN correspondent David McKenzie described the extensive efforts undertaken by the LAJ government to script what Tripoli-based foreign correspondents saw of the city during their choreographed visits from the Rixos Hotel, where they had been sequestered:

> The view that journalists get while driving through Tripoli is typically witnessed through the windows of government buses driving along routes selected by government minders that show a pro-government landscape. It's a view the Libyan government wants the rest of the world to see: people united in support for Libyan leader Moammar Gadhafi.[105]

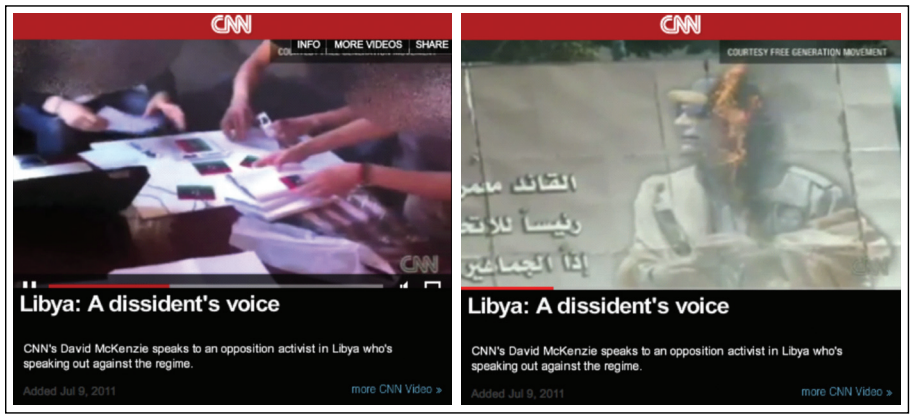
The image, of course, was an illusion. Tripoli had experienced intense protests in the early days of the uprising. After several days of protests followed by a heavy-handed crackdown and the heavy presence of security forces, the city appeared to have "calmed." The lack of reportable protests and incidents of violence was used by the regime in an attempt to script a story that, although the east might be against Gaddafi, Tripoli and much of western Libya firmly supported him.

Overt acts of protest in Tripoli were few after the early protests. However, one group of activists, the Free Generation Movement (FGM), worked steadily to ensure that the world media had access to videos and other material showing that Tripoli was not as calm as it seemed. These images were not simply for international consumption: featured in major news outlets, they were beamed back into Libya and viewed with interest in Tripoli.

FGM was led by 29-year-old maxillofacial surgeon Nizar Mhani under the nom de guerre "Niz," and relied on a network of in-country and expatriate opposition supporters, nearly all in their twenties. The movement's communications infrastructure was surprisingly simple. Niz had "liberated" a set of VSAT equipment from a government building earlier in the uprising and used it to post videos and take Skype calls from journalists, always happy to explain in perfect British English just how extensive support for the Libyan opposition in Tripoli really was. Later, as the conflict raged in the city, Niz was instrumental in making images and reports available that highlighted the tenuous control of LAJ forces over the city.

One video posted by the FGM shows a Molotov cocktail being prepared and then thrown against a large pro-Gaddafi billboard in Tripoli. The video shows Gaddafi's face engulfed in flames—and no rush of security services to extinguish the fire. Other videos show leaflet drops of anti-Gaddafi slogans, and anti-Gaddafi banners unfurled over roadways. Niz and his group also posted videos of battery-powered amplifiers connected to MP3 players that played a loop of Libya's pre-Gaddafi national anthem, which were placed in concealed or overt locations within the city. Again, tellingly, the videos indicated a lack of immediate response by security forces.

For such activities that broke the illusion of regime control and support, Niz and the other members of the FGM were targeted for arrest. The LAJ security forces discovered his identity and imprisoned several members of



CNN report on the Free Generation Movement showing some of its members preparing leaflets for dropping in the city (left) and burning a pro-Gaddafi billboard (right).

his family and friends; Niz and his cousin were forced into hiding. After some effort, FGM was again online, broadcasting from this safe house. Niz was also subjected to a sustained campaign of electronic attacks, described below. Ultimately, he tweeted the entire uprising, with interruptions, and was online and posting material when opposition forces entered the capital.

Regional Media Centers

As the uprising spread, what had initially been uncoordinated efforts to transmit information about the uprising to the outside world quickly grew. The initial videos and materials had been distributed by individuals or via groups like the National Front for the Salvation of Libya that had previously maintained an online presence. Over time, a number of groups emerged, often tied to specific places like Misurata, the Nafusa Mountains, or Tripoli. Sometimes named "media committees," these groups became key sources and clearinghouses for information and content, as well as points of contact for international media seeking interviews and updates.

For example, in the Nafusa Mountains, the town of Nalut established the Nalut Media Committee, which maintained a YouTube account as well as Facebook pages in Arabic, English, and French.[106] At the time of writing, their YouTube account had over 1.3 million views. Several towns over, the Zintan Media Committee also maintained an Arabic-language Facebook page[107] and a YouTube account. The media committees' content was sometimes widely viewed, while in other cases received only limited traffic.

Misurata similarly developed a series of media groups including Wefaq Libya or Freedom Group, which maintained both a YouTube site established on February 26, 2011 and a Twitter feed, as well as Facebook pages in Arabic and English.[108] By May 2012, videos from Freedom Group had been viewed over 4 million times. Similarly, the media group Misrata Patriots, formed in late April 2011, maintained a YouTube site, a Twitter feed, and a Facebook account (which was later hacked by pro-government electronic actors).[109]

The video postings of these media groups provides a window into the multiple roles that online video played in the conflict. Videos document skirmishes and pitched battles with LAJ forces, the effects of shelling and warfare during the siege to humans and property, motivational clips set to music, and a wide range of glimpses into the lives of Misuratis during the

conflict. They not only humanized the Misurati opposition fighters but also brought key elements of their plight, and their narrative of a struggle for freedom against a brutal dictator, to the attention of the world.

A Note on Pro-Regime Online Content

YouTube, Facebook, and Twitter also became spaces used by pro-LAJ individuals and groups to comment on opposition videos as well as to post their own content in an attempt to counter opposition messaging. On YouTube, for example, this meant filling the comments of pro-opposition videos with pro-Gaddafi comments, or mass-disliking pro-opposition content in an attempt to reduce its credibility or visibility. In other cases, this meant posting videos critical of the Libyan opposition or NATO intervention, and then mass-liking the video to increase its visibility. An unscientific survey of this pro-LAJ video content in summer 2011 revealed that it was often based on video originally produced by Libyan State Television, the Iranian Press TV, and Russia Today, all of which had adopted, to varying degrees, editorial policies that opposed the revolution, NATO intervention, and so on. On Facebook, LAJ supporters created a large volume of profiles with pseudonyms and profile photos containing pro-Gaddafi iconography and the use of the same green found in the LAJ flag. They used these profiles to post pro-Gaddafi slogans and material on their own pages and on the pages of those whom they had identified as opposition supporters. In some cases, these postings also contained disinformation (including false coordinates and other false reports), threats, and accusations, such as accusing pro-opposition accounts of being the tools of a foreign intelligence service. Some Libyan opposition supporters responded in kind, trading accusations and slogans with self-identified regime supporters. Many appeared to have avoided taking the bait, however, while others chose to report violent language and pro-regime propaganda as violations of the terms of service of social media websites, which sometimes resulted in content being pulled and profiles suspended.

The often aggressive, taunting, and threatening tone of pro-LAJ activities on social media may have undermined the LAJ's narrative that it was being attacked by gangs and thugs. By focusing on attempts to intimidate, silence, and berate pro-opposition social media users and content, pro-LAJ online

actors often echoed the language used by Gaddafi in his speeches, such as calling opposition supporters "rats." While their postings sometimes claimed human rights violations by NATO and the Libyan opposition, these claims were often discordant with the volume of aggressive and violent rhetoric they used. The overall impression may have instead supported the opposition's public narrative: that the Libyan opposition was faced with an irrational adversary, capable of inflicting grave human rights violations against his own people.

Discussion Questions

1. How did media coverage of social media expand and amplify the reach of actions in that realm?
2. In what ways does Mohammed Nabbous exemplify the ways in which individual Libyans were able to use the Internet to influence the international perception of the Uprising?
3. How did the Libyan opposition's use of YouTube evolve over the course of the conflict? What effect is this likely to have had on their credibility?
4. What does Ms. Clinch's story indicate about how the Internet can make global networks of support possible?
5. How did the pro-regime online activities and messaging on social media contrast with that of pro-opposition online activity?

Notes

60. J. Cole, "TV, Twitter, Facebook and the Libyan Revolution," Informed Comment (blog), August 24, 2011, http://www.juancole.com/2011/08/tv-Twitter-Facebook-and-the-libyan-revolution.html
61. P. Beaumont, "The Truth about Twitter, Facebook and the Uprisings in the Arab World," *Guardian*, February 25, 2011, http://www.guardian.co.uk/world/2011/feb/25/twitter-facebook-uprisings-arab-libya
62. https://Twitter.com/#!/sultanalqassemi
63. Beaumont, "The Truth about Twitter, Facebook and the Uprisings in the Arab World." ibid.
64. Personal communication with L1, Spring 2012.
65. https://www.Facebook.com/17022011libya
66. "'Day of Rage' Kicks Off in Libya," Al Jazeera, February 17, 2011, http://www.AlJazeera.com/news/africa/2011/02/201121755057219793.html
67. "International Social Media: A 2011 Round Up," Oban Multilingual SEO (blog), December 13, 2011, http://www.obanmultilingual.com/articles/december-2011/international-social-media-2011
68. Images and view count information provided by "Free Libya Cyber Command," Spring 2012.
69. Personal communication with the individual who prefers the nom de guerre "Free Libya Cyber Command," Spring 2012.
70. Domain Name Servers contain databases that link websites' Uniform Resource Locators (URLs) to IP addresses. Filtering at the DNS entails identifying requests from a user's computer to connect to a restricted or blocked website, then blocking or redirecting these requests to alternate websites, and refusing to connect to the correct websites' IP addresses.
71. http://www.libya-watanona.com/
72. http://enoughgaddafi.com; as of January 2013, the URL is no longer live.
73. "'Day of Rage' Kicks Off in Libya," Al Jazeera, February 17, 2011.
74. "Feb17.info Calls It a Day," *Libya Herald,* March 18, 2012, http://www.libyaherald.com/feb17-info-calls-it-a-day/
75. http://www.libyafeb17.com/
76. Project Cyber Dawn, Cyber Security Forum Initiative, April 17, 2011.
77. http://www.livestream.com/libya17feb/
78. "[Message From Libya]TELL THE WORLD WHAT IS HAPPENING TO US!!!!!.flv" YouTube video, uploaded Febuary 20, 2011, http://www.YouTube.com/watch?v=38EXALI60hg
79. J. Pollock, "People Power 2.0: How Civilians Helped Win the Libyan Information War," *MIT Technology Review,* http://www.technologyreview.com/web/40214/
80. Ibid.
81. NFSLLibya, YouTube channel, http://www.YouTube.com/user/NFSLibya; أولى لقطات لمظاهرات بنغازي الباسلة YouTube video, uploaded Febuary 15, 2011, http://www.YouTube.com/watch?v=T94EqeM4NGM&feature=player_embedded
82. "Qaddafi's Yellow Hat Mercenaries - Bazzar st. Benghazi Libya," YouTube video, uploaded Febuary 22, 2011, http://www.youtube.com/watch?v=xL8pQHsU2G0
83. "Live Blog – Libya Feb 23," Al Jazeera, February 23, 2011, http://blogs.aljazeera.com/blog/africa/live-blog-libya-feb-23
84. "Revueltas en el mundo islámico," *El Pais*, February 23, 2011, http://eskup.elpais.com/*revueltasenelmundoarabe2011
85. "Video: Schokkende beelden van protest in Libië," *Het Nieuwsblad*, February 23, 2011, http://www.nieuwsblad.be/article/detail.aspx?articleid=DMF20110223_078
86. "Une grande partie de la Libye serait tombée," *Libération*, February 23, 2011, http://www.liberation.fr/monde/01012321688-300-morts-en-libye-selon-les-autorites
87. "Regimetreue kämpfen um West-Libyen," *Der Spiegel*, February 23, 2011, http://www.spiegel.de/politik/ausland/0,1518,747173,00.html
88. R. McAthy, "Al Jazeera to Relaunch Citizen Media Platform Sharek," Journalism.co.uk, May 4, 2012, http://www.journalism.co.uk/news/al-jazeera-to-launch-new-multilingual-citizen-media-platform/s2/a549099/
89. المرتزقة ذو القبعات الصفراء في شارع البزار- بنغازي, YouTube video, uploaded Febuary 22, 2011, http://www.YouTube.com/watch?v=xL8pQHsU2G0
90. "Libya: 8-Year-Old Girl Shot in Leg," YouTube video, AlJazeera English, uploaded Febuary 24, 2011, http://www.YouTube.com/watch?v=nd1lnfsScnc

91. As it appeared in Spring 2012.
92. R. Mackey, "Feb. 24: Updates on Libyan Uprising," The Lede (blog), *New York Times*, February 24, 2011, http://thelede.blogs.nytimes.com/2011/02/24/latest-updates-on-libyan-uprising/
93. J. Pollock, "People Power 2.0: How Civilians Helped Win the Libyan Information War," *MIT Technology Review,* April 20, 2012, http://www.technologyreview.com/web/40214/
94. http://Twitter.com/Guma_el_gamaty
95. http://Twitter.com/ChangeInLibya
96. Beaumont, "The Truth about Twitter, Facebook, and the Uprisings in the Arab World."
97. T. Bradshaw and J. Blitz, "NATO Draws on Twitter for Libya Strikes," *Financial Times/Washington Post*, June 15, 2011, http://www.washingtonpost.com/world/nato-draws-on-Twitter-for-libya-strikes/2011/06/15/AGLJpTWH_story.html
98. G. Smith, "How Social Media Users Are Helping NATO Fight Gadhafi in Libya," *Globe and Mail* (Toronto), June 14, 2011, http://www.theglobeandmail.com/news/world/how-social-media-users-are-helping-nato-fight-gadhafi-in-libya/article583325/
99. http://Twitter.com/libyanfsl
100. http://Twitter.com/EnoughGaddafi
101. http://twitter.com/ShababLibya
102. Smith, "How Social Media Users are Helping NATO Fight Gadhafi in Libya."
103. Ibid.
104. Ibid.
105. D. McKenzie, "From Deep Inside Tripoli, Displays of Defiance," CNN, July 8, 2011, http://edition.cnn.com/2011/WORLD/africa/07/07/libya.tripoli.rebel/
106. https://www.YouTube.com/user/NALUT2011; http://www.Facebook.com/pages/ةروثلةيمالعاا-ةنجللا-17ريارب-ف-تولان-/221212461228498; http://www.Facebook.com/pages/Nalut-Feb17-Media-Committee/113462242072872; http://www.Facebook.com/pages/Le-comité-médiatique-de-la-révolution-de-17-Février-à-Nalute/221428421201443
107. http://www.Facebook.com/pages/قناة-الزنتان-على-الفيس-بوك/188788917808981
108. http://www.YouTube.com/user/miusrata17 miusrata/videos; https://Twitter.com/#!/freedomgroupTV; http://www.Facebook.com/wefaqly; http://www.Facebook.com/WefaqLibyaEn
109. http://www.YouTube.com/user/Patriots1Of7Misratah; https://Twitter.com/#!/fMisrataPatriots; https://www.Facebook.com/pages/Patriots-of-Misratah-/وطنيو-مصراته165630860162513?sk=info

CHAPTER
FIVE

Out of the Public Eye: Decentralized Communications of a Networked Opposition

Largely outside of the public eye, and intentionally concealed, the Libyan opposition made comprehensive use of a range of online tools to support their communications activities. Many of these networks were ad hoc. Yet the Internet played a substantial role in supporting the opposition's communications networks. Key coordination activities, from communications between frontline operations rooms and command centers to strategy discussions between opposition leadership and their international envoys to aid logistics, took place over restored Internet connections, as did private communications with journalists, aid and advocacy organizations, and representatives of foreign governments. The Internet even supported battlefield communications: collaborative targeting information was collected and sent to NATO contacts using free and accessible online tools like Google Earth, Skype, and Hotmail; and information was relayed between operations centers in the opposition command structure. Without attempting to be exhaustive, this section provides a brief introduction to some of these activities and tools during the 2011 Libyan revolution and concludes with a brief discussion of some of the associated vulnerabilities.

Networks of Support

Libya is not a large country, its population is relatively concentrated in urban areas, and, as commentators have noted, everyone seems to know each other. The Libyan diaspora is similarly linked to relatives and others back home, often by familial and geographic ties: a Misurati living in the Europe, for example, is likely to have strong and direct connections to other family members and cousins still in Misurata, as well as to other Misuratis in the diaspora. These kinds of network deserve brief discussion here, although they ultimately merit sociological study in their own right.

In a comprehensive article in the *MIT Technology Review,* John Pollock has described these family networks and personal connections as a "cousinate." [110]

Established long before the 2011 uprising, these networks allowed Libyans caught inside the country to quickly connect to networks of trust, relatives and friends outside. Not only did these networks make it possible to know who someone was, but they also made it possible to verify people as trustworthy, enabling networks from different places and families to expand, and ultimately, link together, coordinating material and political support for the uprising. A cousin might be a telecommunications engineer, work in an import/export firm, or have standing or prominence in a nation whose foreign policy supported the uprising. These people could be synergistically linked to other networks with bits and pieces of resources, ultimately resulting in a rich array of resources and logistical pathways to put them at the service of the Libyan opposition.

An opposition member might have access to multiple distinct categories of resources, making their network potentially useful for a wider range of activities than would normally fit in a traditional governmental or military organizational structure. They could draw on a resource base that was not fixed by the constraints of distance or professional hierarchy. Libyan opposition supporters on the ground and overseas frequently engaged in multiple types of activity, operating more as a distributed and networked group of resources than the rigidly hierarchic structures of the Gaddafi regime. These networks supplied much of the "on the ground" information fed into the social media sites, and they also served as trust networks for directing resources. While these networks are not the primary subject of this case study, it is important to highlight how powerfully they were enabled by access to restored connectivity and how their nature structured the kinds of communications that took place.

The same individual who might be regularly giving short interviews to international news organizations or who maintained a pro-opposition Twitter feed might also be directly involved in, say, coordinating material support to opposition forces, transmitting targeting intelligence to others, or lobbying the Libyan diaspora for funding. One such actor, Rida Benfayed, an expatriate who traveled to Libya's eastern port of Tobruk to support the opposition, is a good example of this plurality of roles. Benfayed seems to have functioned as a kind of information clearinghouse, receiving a steady flow of information and relaying it to the appropriate parties. Benfayed's

Skype account was organized by a series of categories: "English media, Arabic media, medical, ground information, politicians, and intelligence."[111] In another case, a Libyan who provided regular interviews to the media from Misurata also engaged in identifying targets for NATO, dialogue with a foreign country interested in providing material support, telecommunications support, and so on.

Not all of the nodes in these networks were Libyans, and it is interesting that many of the non-Libyan supporters of the opposition who engaged with the conflict electronically also adopted multiple roles. For example, Stephanie Lamy was an American living in Paris who was sympathetic to the opposition and supported Mohammed Nabbous's Livestream. Out of the public eye, Lamy also worked with contacts to transmit information to individuals whom she believed were in contact with NATO. When Lamy received information from an individual claiming to have intelligence about the movements of LAJ forces and to be retired from an European intelligence agency, for example, she transmitted this information to Rida Benfayed, who describes subsequently passing it on to Mustafa Abdu-Jalil, chair of the National Transitional Council.[112]

Many individual opposition actors adopted a node-like strategy, arguably allowing individuals to increase their usefulness by contributing where they could, across a wide range of domains. In order to do this effectively, of course, there needed to be a rich and fluid mechanism for exchanging information and knowing what resources were needed. While communications tools like Skype could support the person-to-person and group conversations that could be used once a specific task or set of resources was identified, private and secret groups on Facebook and other sites were used to exchange information across networks. They made it possible for individuals who had resources or connections to see where they might be able to assist, as well as to see who else was committing to support the same task.

Vignette: Internet on the Battlefield

It is mid-April 2011 and a Skype call is about to influence the outcome of a battle. Sifaw Twawa in Yefren commands a brigade of anti-Gaddafi fighters. They are considering an attack on a Grad launcher[113] that is part of the Gaddafi force's siege of the town in the Nafusa Mountains. He gets a call on his

cellphone patching him in to a group Skype chat. Two Libyan civilians in the diaspora are on the line, one a doctor in the UK, another a researcher in Finland. The doctor, Khalid Hatashe, had been trained in the use of Grad rocket systems during compulsory military service. He laid out to Twawa key information about the Grad system, including the critical fact that Tawawa's brigade was closer to the Grads than their minimum effective range, and that the troops operating the Grad launcher might be several hundred yards away, operating the system by wire. Their ensuing attack is a success, taking the pressure off Yefren.[114]

Getting Intelligence and Targeting Information to NATO

NATO forces openly used social media tools like Twitter for occasional media messaging. NATO also acknowledged that it engaged in monitoring social media for information about the Libyan conflict during Operation UNIFIED PROTECTOR. The overall sense among Twitter users during the revolution was that NATO and member countries were monitoring Twitter to gather information on potential targets, leading many users to explicitly tweet at NATO in an attempt to draw its attention to specific developments and coordinates. The media picked up on this and by early summer 2011 were extensively reporting on NATO's use of social media in its intelligence gathering, as in the following:

> NATO officials have acknowledged that social media reports contribute to their targeting process—but only after checking them against other, more reliable, sources of information.[115]

NATO Wing Commander Mike Bracken's acknowledgment that social media was being used to help nominate targets provided the public with a window into its official activities and how NATO incorporated social media into its analysis:

> We get information from open sources on the Internet; we get Twitter. . . . You name any source of media and our fusion center will deliver all of that into usable intelligence.[116]

Another NATO official explained that social media, including Twitter, helped focus NATO's attention to areas where LAJ forces were active:

> the organization monitors Twitter feeds from Tripoli and other places for "snippets of information." These could then be tested, corroborated or not,

> by NATO's own sources, including direct lines of communication with the rebels, and imagery and eavesdropping from Nimrod spy planes.[117]

The official explained that intelligence gathering using Twitter and other social media feeds was only one part of a broader fusion-based intelligence methodology, and apparently sought to reassure the public that NATO was not relying on information from Twitter as a single source and that it was aware that the LAJ might be using Twitter for disinformation:

> [NATO] is also aware that Gaddafi might be using Twitter to feed false information. "We have to be careful it is not used for propaganda [by LAJ forces]," the NATO official said.[118]

Tweeting and re-tweeting targeting information in a rapidly developing conflict could itself be subject to unintentional distortion and error:

> But even in the fast-moving environment of Twitter, intelligence analysts and armchair generals alike must beware that information can get old quickly. Replying to followers who "retweeted" tactical information, user Libyanandproud said: "NEGATIVE NEGATIVE, Coordinates changed!! FLUID!"[119]

Other uses by NATO member forces appear to have ranged from officially sanctioned to apocryphal. For example, despite explicit messaging that NATO intelligence was monitoring and analyzing social media, NATO member countries' actions in social media were sometimes contradictorily reported in the press. One newspaper, for example, reported that a Twitter account

> with apparent links to the British military . . . has even taken the unusual step of asking users to submit the precise co-ordinates of troops loyal to Colonel Moammar Gadhafi.[120]

Attempting to verify the claim the next day, a reporter writing for a different paper contacted the operator of the account, @HMS_Nonsuch,[121] and wrote the following:

> @HMS_Nonsuch told the Guardian he is a 50-year-old Birmingham man called Chris, and has "no connection" to any military or defence organisation.[122]

Meanwhile, further out of the public eye, NATO appears to have received a wide range of more or less formal targeting information and situational awareness from Libyans using social media, Skype, and other tools. A

French naval officer describes having created a large network of social media contacts in order to collect atmospheric information about the Libyan battle space. He soon found himself receiving what he described as much higher quality information, including specific information about targeting. While provided with no military intelligence, he describes being asked detailed questions by his superiors about his information. The officer estimated that he was faster than his vessel's traditional intelligence sources 80% of the time. He stated that he believed his network of Libyan sources provided him with better information than that received by traditional French intelligence channels.[123]

Many opposition members actively worked to provide information to NATO about LAJ forces' activities. Nagi Idris, for example, describes collecting humanitarian and medical information about fighters in Misurata, Benghazi, and the Nafusa Mountains. Idris and his wife, Gihan Badi, provided information, including precise coordinates when possible, to NATO's Civil-Military Co-operation group.[124] Another Libyan worked to establish operations rooms in Tunisia, Dubai, and Spain. He described his group as smuggling over 100 satellite phones into Libya and gathering detailed intelligence that was passed back to NATO. As an apparent mark of the role of networks of trust, he was able to get an approximate number of LAJ forces located in Brega based on information from a link in his "cousinate" to the company that supplied their meals—and he knew this information was reliable, because officers received better meals than their men did and the source knew how many of each type of meal was being prepared.[125]

Many other Libyans worked to provide similar information. As one Misurati explained, NATO received daily updates from his group and others containing targeting information.[126] The targeting process was straightforward and team-based. Team members would travel to the front lines or communicate with the fighting groups to ask if there was "anything they wanted hit." Subsequently, information would be physically brought back or transmitted to an operations room where other team members used Google Earth and Google Maps to locate the coordinates and create a targeting list, including Google Earth screen captures, latitude and longitude coordinates, and short briefs about each target. The targeting packages would then be transmitted to several locations, including Doha, where the

Libyan opposition maintained direct points of contact with NATO forces, and a NATO situation room. NATO would sometimes push questions back into this network, requesting clarification or further information. While the process allowed groups to transmit a substantial amount of timely and, in their view, accurate targeting information to NATO, several Misuratis have commented that it was not until foreign personnel in direct communication with NATO were physically on the ground in Misurata to assist in targeting that NATO responsiveness with air attacks operated at a speed that Misuratis felt was fast enough.

Brief Notes on Specific Tools

Skype: Communications Backbone of the Libyan Opposition

Of all the online communications tools used in the Libyan revolution, Skype distinguished itself as a near ubiquitous presence in operations rooms, media centers, and news desks. Skype is a powerful and free VOIP video call and chat client that is used by more than half a billion people around the globe.[127] It remained visible throughout the Arab Spring, notably as a frequently mentioned means by which interviews with opposition supporters were conducted. Skype similarly played a key public role in connecting journalists to sources throughout Libya and was a frequent presence in news reporting. Fighters and opposition supporters were interviewed live and with delays over Skype video. As stories developed or news broke, reporters regularly messaged contacts on the ground and in the opposition.

Out of the public eye, Skype played an essential role, permitting what many opposition supporters saw as a reasonably secure means for text, voice, and video communications. Its functionality permitted both person-to-person calls and textual conversations, as well as group chats, some of which lasted for weeks, and which opposition supporters sometimes used as clearinghouses for information and news.[128] It was believed that Skype-encrypted chat or voice communication could not be intercepted by LAJ security forces.[129]

Skype allowed opposition supporters from towns separated from each other by regime-controlled areas to communicate, coordinate strategy, and share information. It also proved to be a highly effective tool in connecting Libyans with opposition supporters throughout the diaspora. It was extensively used, for example, alongside satellite phones to coordinate aid needs

for Libyan-operated aid and material support to the city of Misurata. As one Misurati reflected, "If it wasn't for the Internet and Skype, the world would have never heard of anything that went on in Misurata. . . . thank God they couldn't cut it off."[130]

During the fighting in Misurata, the absence of a wireless network infrastructure, as well as the limited number of satellite phones and the difficulty using them, meant that Skype was used "even to call someone three km away." A Misurati explained that "even after" radios and other communications tools became more readily available, Skype's convenience as well as the perception of its security kept it as one of the dominant communications tools: "We knew that radios were not secure." They were sure the LAJ forces were listening to them. Misurati opposition fighters, according to several sources, used mostly unencrypted, unscrambled radios. If a boat was coming or leaving, "they wouldn't say it on the radio . . . they would do it on [Skype]."[131] The limited number of encrypted radios on both sides meant that fighters could listen in on the channels used by the other side. Misurati fighters and some fighters active in the Nafusa Mountains appear to have responded to this problem by adopting various code words and phrases and, in some cases among Amazigh populations, using distinctive and highly localized dialects that even nearby communities might have difficulty understanding.[132]

Skype conference calls also provided what many perceived as a secure mechanism to engage in coordinating strategy; one source recalls conference calls on strategy between Benghazi, Troubrouk, Misurata, and Tripoli.[133]

Vignette: Skype in Bani Waleed

As several Misuratis have described,[134] a key tipping point in the Bani Waleed conflict was the provision of VSAT systems and Skype installations to three forward operations rooms established in Zawiya and Tarhuna, as well as a main operations room in Tajoura. Prior to the installation of these operations rooms, fighters from Zawiya, Tarhuna, Tajoura, and Bani Waleed were fighting largely independently on different fronts. The establishment of communications rooms allowed the fighters to better coordinate their advances. It also provided them with a link to opposition members in Benghazi, who maintained direct contact with NATO. Between operations rooms, and between the main operations room and Benghazi, communications took place

mostly via Skype calls. Communications between fighters and operations rooms was via unencrypted radio, using verbal codes. While the outcome of the battle reflected many factors, LAJ forces' resistance was overcome just one week after these coordination mechanism were put in place, and the town became free.

Facebook Groups

While Facebook was extensively used to publicly post and share information and rich media about the revolution, the wide scope of Facebook use and the presence of many Libyan opposition actors on Facebook made it possible to benefit from another element of the site's functionality: groups. Facebook offers users the powerful ability to quickly create groups with several layers of privacy protection and secrecy, including open, closed, and secret groups. Closed (administrator consent required for entry) and secret (invitation only, not publicly listed) groups, for example, were frequently used for a wide range of Libyan opposition activities, from communicating with selected foreign correspondents and sharing breaking news to political discussions to coordinating information about logistical needs. It is difficult to survey the full range of these activities because of their private and invitation-only nature. Nevertheless, it can be generally observed that Facebook provided a convenient mechanism for what was clearly an ad hoc and highly spatially distributed network of opposition supporters in the diaspora and others on the ground to converge in nonpublic, moderated spaces and coordinate their activities. Groups on Facebook made it possible for a wide range of actors who had access to specific resources to monitor a constant flow of information about resource needs and resource availability, including humanitarian assistance, logistics, lobbying, opportunities for media contact, and so on. Supporters could be introduced to these groups if they had a specific set of resources or requests, and if they were considered trustworthy.

Online E-Mail

E-mail accounts could not replace the one-to-many functionality of a tool like Facebook. Similarly, e-mails couldn't reproduce the low-latency communications functionality offered by Skype during a time of uncertain communications. Not only was voice a more comfortable medium for many Libyan opposition actors, but as one opposition member explained,

it wasn't always possible to determine that a message had been read immediately. Still, e-mail could be used to transmit data and attachments in parallel with Skype calls, for example, and it was clearly useful for a number of activities where information was intended for a small set of recipients but attachments and other tools were necessary. A Skype call, for example, could provide information about a target set, and an e-mail follow-up could provide the coordinates and the details.

Prior to the revolution, a Hotmail or Gmail account might have been used for a mixture of business and personal activities. During the uprising, some Libyan opposition supporters continued to use personal accounts that had been established well before the 2011 uprising, but transformed them into tools of war fighting, coordination, media connections, and strategic communication. The same Hotmail or Yahoo! account might now also be used to communicate with international media, share documents and other materials within the opposition, coordinate humanitarian aid, and even interact with weapons suppliers or opposition members communicating with NATO. Many more accounts were created, often pseudonymously, and served similar functions.

Discussion Questions

1. How did networks of support and trust expand the Libyan opposition's access to resources? Were these networks complemented by social media?
2. How did NATO publicly explain how it was using social media? What are some of the ways that this might have shaped how the Libyan opposition used social media? What were some of the risks to this kind of disclosure?
3. What are two ways that particularly struck or surprised you about how the opposition used common tools to communicate? What kinds of functionality do these tools have that might not be found in their military equivalents? What do they lack?

Notes

110. J. Pollock, "People Power 2.0: How Civilians Helped Win the Libyan Information War," *MIT Technology Review,* April 20, 2012, http://www.technologyreview.com/web/40214/

111. Ibid.

112. Ibid.

113. The term used in Libya to refer to a 122 mm unguided multiple rocket artillery launcher that can be truck-mounted. The Grad was a commonly used rocket system in Libya, and it figured prominently in LAJ forces' actions against the opposition.

114. Pollock, "People Power 2.0."

115. G. Smith, "How Social Media Users Are Helping NATO Fight Gadhafi in Libya," *Globe and Mail* (Toronto), June 14, 2011, http://www.theglobeandmail.com/news/world/how-social-media-users-are-helping-nato-fight-gadhafi-in-libya/article583325/

116. A. Gabbatt, "NATO, Twitter and Air Strikes in Libya," Inside the Guardian (blog), June 15, 2011, http://www.guardian.co.uk/help/insideguardian/2011/jun/15/nato-twitter-libya

117. R. Norton-Taylor and N. Hopkins, "Libya Air Strikes: NATO Uses Twitter to Help Gather Targets," June 15, 2011, *Guardian*, http://www.guardian.co.uk/world/2011/jun/15/libya-nato-gathers-targets-twitter

118. Ibid.

119. T. Bradshaw and J. Blitz, "NATO Draws on Twitter for Libya Strikes," *Financial Times/Washington Post*, June 15, 2011, http://www.washingtonpost.com/world/nato-draws-on-Twitter-for-libya-strikes/2011/06/15/AGLJpTWH_story.html

120. Smith, "How Social Media Users Are Helping NATO Fight Gadhafi in Libya."

121. http://Twitter.com/HMS_nonsuch

122. Gabbatt, "NATO, Twitter and Air Strikes in Libya."

123. Pollock, "People Power 2.0."

124. Ibid.

125. Ibid.; Personal communication with J. Pollock, December 17, 2012.

126. Personal communication with L1, Spring 2012.

127. "Skype Grows FY Revenues 20%, Reaches 663 Mln Users," Telecompaper, March 8, 2011, http://www.telecompaper.com/news/skype-grows-fy-revenues-20-reaches-663-mln-users

128. In specific cases, journalists were also included in these chats, sometimes intervening to ask for updates or clarifications.

129. Personal communication with L1, Spring 2012.

130. Personal communication with L2, Spring 2012.

131. Ibid.

132. Personal communication with L8, Spring 2012; Personal communication with J. Pollock, December 14, 2012.

133. Personal communication with L2, Spring 2012.

134. Personal communication with L1 and L2, Spring 2012.

135. Personal communication with L1, Spring 2012.

136. Personal communication with L2, Spring 2012.

CHAPTER
SIX

Inherent Risks: Monitoring and Attacks

Pre-Revolution Monitoring at Home and Abroad

It was clear to Libyans before the 2011 revolution that political speech tied to one's name could be dangerous. Journalists and online commentators might be summoned for questioning or detained as "Internet prisoners" as a consequence of their writings published online.[137] One Libyan detained by the intelligence services, for example, was shown his correspondence with Libyan exile political organizations, along with pseudonyms he had used to publish abroad. In another case, a Libyan journalist was arrested as he prepared to meet a dissident contact he had known only by e-mail communication.[138] Even for dissidents abroad, criticism could be dangerous. Historically, Gaddafi's operatives had been known to strike dissidents overseas, in 1984 firing on a demonstration in front of the Libyan embassy in London in an incident that cost the life of a British police constable. In ensuing years, the Gaddafi regime used other tools to apply pressure on those who disagreed with them, making the regime an international pariah and encouraging legitimate fear of its ability to reach dissidents abroad or their families back home.

Although Libyans readily describe their perceptions that the regime engaged in some Internet filtering and monitoring, direct information about how the monitoring took place was largely unavailable prior to the 2011 revolution. Evidence for the most unsophisticated forms of monitoring was sometimes publicly visible: a 2009 Open Network Initiative (ONI) report on Libya[139] noted that visible surveillance was often present at Internet cafes. Beyond the direct presence of surveillance agents, the report noted, Internet cafes were encouraged to undertake their own self-monitoring. Some Internet filtering was also observed. The ONI identified evidence of somewhat limited and unsophisticated efforts of content filtering by the Gaddafi regime.[140] These seemed limited to a select group of targeted political websites, as well as websites linked to Libya's Amazigh (Berber) minority. The same

report also noted cases of political websites being hacked and their content replaced with pro-Gaddafi materials between 2008 and 2009.[141]

Regime Monitoring and Hacking Prior to the Revolution: What We Know

After the fall of Tripoli to opposition forces, Libyans made many startling discoveries about the secret parts of Gaddafi's regime. Concealed tunnel networks under Gaddafi's compound in Tripoli, opulent homes, and signs of decadence and eccentricities all emerged as fighters, reporters, and everyday Libyans passed through the doors of hastily abandoned buildings and compounds. Amidst emptied detention cells and piles of dossiers were discovered sophisticated Internet and telecommunications monitoring gear.

When reporters for the *Wall Street Journal* entered one of these locations after Tripoli's fall, they spotted and photographed a sign on the wall: "Help keep our classified business secret. Don't discuss classified information out of the HQ." The culture of secrecy in the intelligence services was highly effective. Beyond the sense that they were being monitored, the public appears to have not known a central core of the Gaddafi regime's Internet monitoring capabilities: Libya had purchased most of its network monitoring gear from large Western and Asian companies. The logo of one of them, Amesys, was visible in the upper left corner of the sign. The first public evidence for the presence of foreign companies may have emerged during a BBC report in which Amesys's name was visible.[142] A picture quickly grew of a surprising range of international companies that had provided tools to support telecommunications interceptions.

Two major monitoring systems have been publicly identified at the time of writing: the Amesys EAGLE system and the ZTE monitoring system. Reporters and others investigating these systems encountered a range of other equipment also supplied by international companies that provided further interception capabilities, including cellular, international, and satellite phone interception and tracking.

The Amesys EAGLE System

The EAGLE system cost the Libyan government approximately €10 million, and began to be installed in late July 2008, according to a person involved in its installation.[143] The installation of the product in Libya was a

Poster found on the wall of a Gaddafi regime monitoring facility HQ 2 with the Amesys logo in the corner.[144]

collaboration, as well as a test. Libya would be an "interesting laboratory" and a test bed for this system, allowing the company to test out its systems without limitations. The system was installed by French Amesys,[145] which describes itself as a multi-sector "Critical Systems Architect," which was at the time a subsidiary of the French company Bull.

The same source describes the interception as capturing 98% of Internet traffic in Libya from a small number of capture points:

> We did massive [interception]: we intercepted all the data passing through the [Libyan] Internet: e-mails, chats, Internet browsing, Voice Over IP.[146]

The surveillance apparatus had a three-tiered organizational structure. At the lowest levels were "basic operators" who were assigned to follow suspects and prepare reports. Basic operators would identify suspects based on key words and other behavior of interest in the massive traffic flow: "for example, how to put a university under interception and find suspects based on key words."[147]

Above the basic operators were officers, at least 20, who were charged with defining keywords and surveillance priorities. These individuals operated

out of three sites in Tripoli: one for the army, another for the police, and a third belonging to an unspecified part of the government. At the highest level, French military officers as well as Bull executives maintained contact with Abdullah Senussi, the head of Libya's intelligence services, who was involved in negotiating the interception product's functionality. The system made it possible to rapidly create and examine social network diagrams of targets' communications activities, examining the frequency of their communications with other actors.

According to the source, while the EAGLE system was turned on in August 2008, it suffered a number of crashes and setbacks before became fully operational in the beginning of 2010.

EAGLE promotional materials leaked into the public domain lay out what the system is capable of intercepting:

> [M]ore than 300 different network protocols including mail protocols (SMTP, POP3, IMAP . . .), Voice over IP conversations (SIP, H323, RTP, RTCP . . .), webmail transactions (Hotmail, Yahoo, Gmail . . .), or chat conversations (MSN, AIM, Yahoo! . . .). All of them are classified thanks to advanced techniques based on protocol syntax analysis (Deep Packet Inspection), whereas competitive products do it through network port identification that can easily be misled.[148]

In other words, the program can recognize and intercept the kind of traffic associated with each of the following activities:

- E-mail accessed by client software like Outlook, Thunderbird, or Eudora
- VOIP calls (although encrypted calls like Skype are not mentioned)
- Web browsing
- Online e-mails
- Chat programs like Microsoft Messenger, Yahoo! Chat, and AOL Instant Messenger

When installed on Libya's network, such a system could provide the Gaddafi regime's intelligence services with comprehensive access to a wide range of Libyan citizens' online activities.[149]

Interestingly, the leaked manual contained instructional material based on a real-world case: Libya, which Amesys had improperly redacted. OWNI

removed the redactions and found a list of dozens of e-mail addresses that were determined to be part of Mahmoud Al-Nakoua's contact list. Then 72, Al-Nakoua was a well-known Libyan exile and head of the opposition group the National Front for the Salvation of Libya. His contact list included Atia Lawgali, then 60, who played a founding role in establishing the opposition's National Transitional Council; Aly Ramadan Abuzaakouk, a well-known Libyan pro-democracy activist and operator of Transparency-Libya.com (now defunct); and Ashour Al Shamis, who operated the dissident Akhbar-Libya.com (also now defunct).[150] The OWNI investigation highlighted that Al Shamis and Abuzaakouk had both received funding from the National Endowment for Democracy, two of whose employees' e-mail addresses also appear on the list. Their funding included support for securing their communications from hacking and electronic attacks.

The ZTE ZXMT System

The second known monitoring center, installed in a building camouflaged under the bland name of the African Communication Center, was reported to exist by former LTT employees, but was only directly described by Matthiew Aikins in a May 2012 article.[151] This section highlights findings and materials from his reporting.

In photos of the equipment provided to Aikins by Human Rights Watch,[152] it is possible to identify equipment bearing the markings of the Zhongxing Telecommunication Equipment Corporation (ZTE), one of China's largest telecommunications companies. The large rack-mounted equipment in the monitoring center appears to have been built around the ZTE ZXMT interception product.[153] Information about the ZXMT system primarily comes from promotional materials and a presentation about the system apparently prepared for a potential Iranian client,[154] as well as photographs of the original monitoring center.

ZTE describes the system as their "turn-key," carrier-class lawful interception solution, a "vendor-independent" monitoring system with "powerful interoperability." ZTE highlights its ability to monitor communications across a class of products, including the PTSN network, mobile network (2G, 2.5G) the Internet network, and NGN networks.

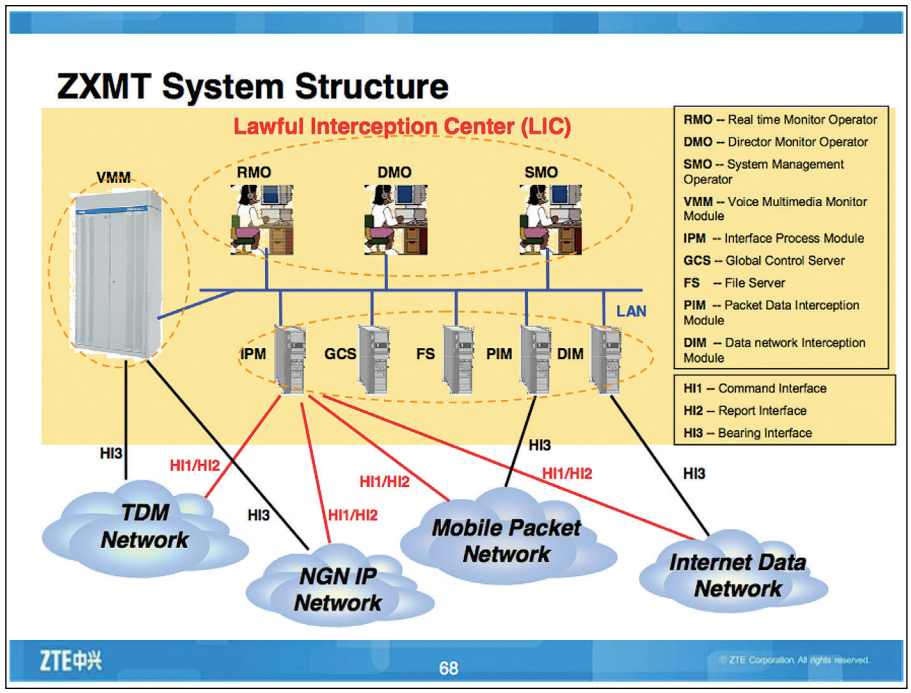


Figure 6.1 Page 68 of the ZTE marketing presentation shows the broad outlines of the system. It is likely that the images provided to Aikins include the data network interception module, labeled DIM here.

The photographs show that a technician appears to have helpfully labeled the servers with ZTE-branded stickers, listing a number of intercept features similar to those offered by Amesys: HTTP, POP3, FTP, IMAP, Telnet, Text FTP, Yahoo Messenger, and so on. Other photographs might have revealed more capabilities, but from these images we can draw a picture similar to that of Amesys. This system appears capable of intercepting:

- E-mail accessed by client software like Outlook, Thunderbird, or Eudora
- Web browsing
- File transfers
- Online e-mails
- Chat programs like Yahoo! Chat

In addition to the system's interception capabilities, photographic evidence shows that it is capable of storing intercepted material, making it possible to

subject the material to historical link analysis, and data mining. Unfortunately, little further information clarifying the command and control structure of the ZXMT monitoring system, target nominating, and monitoring is available in the public domain.

A Note on Other Forms of Monitoring

Evidence has emerged and been widely documented confirming Libyans' perceptions that the regime was monitoring telephone and cellular communications. Equipment capable of monitoring and tracking cellular telephones, landlines, and Thuraya-brand satellite telephones was found when monitoring centers were entered by opposition fighters.[155] Aikins describes mercenaries deployed in a kindergarten:

> Ukrainian mercenaries set up shop in a kindergarten, right around the corner from the intelligence headquarters; from there they snooped on sat-phone traffic using frequency scanners. Gadhafi had declared that anyone caught with a satellite phone could be sentenced to death.[156]

Practical evidence for the application of this equipment isn't hard to come by. In one report, two individuals were detained only four hours after calling a foreign correspondent from a Tripoli-based cellphone.[157] Monitoring equipment included multiple interception and call recording platforms for both domestic and international phone calls. The *Wall Street Journal* has reported that 30 million to 40 million minutes of mobile and landline phone calls were recorded and stored each month with interception equipment supplied by VASTech, a South African company that offers an intercept system that provides both massive interception and retention, and link analysis functionality.[158] Another company whose technology was reportedly in active use in Libya is Thales, which has developed a massive interception system called the National Platform for Legal Interception (Platforme Nationale des Interceptions Judiciares), or PNIJ. The PNIJ was developed for eventual nationwide deployment in France, but was first "commercialized" to Libya in 2008 without certain (presumably legal) protections for citizens planned in its French application.[159]

Satellite phone calls similarly were not immune. Photographs acquired by Human Rights Watch indicate that the LAJ likely possessed satellite telephony monitoring equipment developed by L3 Communications, an American company.[160]

Electronic Operations by the LAJ Against the Libyan Opposition

When the LAJ turned off the Internet and Libya's other telecommunications networks, it may have hoped to strike a mortal blow against the growth of an increasingly interconnected opposition. But it didn't. Turning off the Internet drove Libyans en masse to connect to the Internet in ways that totally bypassed Libyan networks and the powerful Amesys EAGLE and ZTE ZXMT monitoring systems that operated on them. By connecting via VSAT services whose earth stations were outside Libya, the opposition dramatically shifted the balance of information about their activities toward greater privacy and resistance to interception by Gaddafi's regime.[161] Cutting landline and cellular phone service further neutralized the regime's own listening apparatus, with the possible exception of Tripoli and other areas in the east where the phone networks remained active. There too, the Libyan opposition moved its communications toward more decentralized means of communications, substituting Skype for VSAT and satellite telephones or what had previously been phone calls, and later moving some communications onto restored, local communications networks in Benghazi and Misurata.

The Gaddafi regime's response? Try to hack the users and their websites. This section describes how the Gaddafi regime, supported by pro-government electronic actors, worked to exploit vulnerabilities in the ways that Libyans had reconnected themselves. Information about this phenomenon is documented in only a few places. As a result, much of this section relies on conversations with Libyans, as well as analysis of malware that they were sent.

Pro-Government Electronic Actors

Long before the fighting concluded, Libyans realized that their Internet use was under some kind of attack. Social media sites of opposition groups and individuals were sometimes hijacked and defaced with pro-Gaddafi imagery, online e-mail accounts were lost, and Skype accounts hijacked. At some point in spring 2011, Libyans more familiar with information technology began noticing that their friends' accounts were sending them small files they suspected might be malicious. Several key opposition websites also began behaving strangely, serving similarly suspicious files to the browsers that visited them. It is clear today that this reflected the efforts of pro-government electronic actors (PGEAs)[162] on behalf of the LAJ to regain

visibility on the communications and command and control activities of the Libyan opposition.

Who was doing the hacking? Patchy information has emerged about the Libyan side of this effort. Since the end of the fighting, employees of Libya's Internet provider LTT have described a room operated by the Interior Ministry where hacking took place. They have also described efforts to recruit hackers from overseas, including China and Eastern Europe, to engage in phishing campaigns and develop malware that could provide them with access to targeted computers.[163] The group that these former employees have offered a glimpse of may have been an organization known as the Libyan Electronic Army (LEA), which maintained a public presence by hijacking and defacing opposition social media sites, as well as other information operations activities.[164] In fact, the LEA maintained several locations

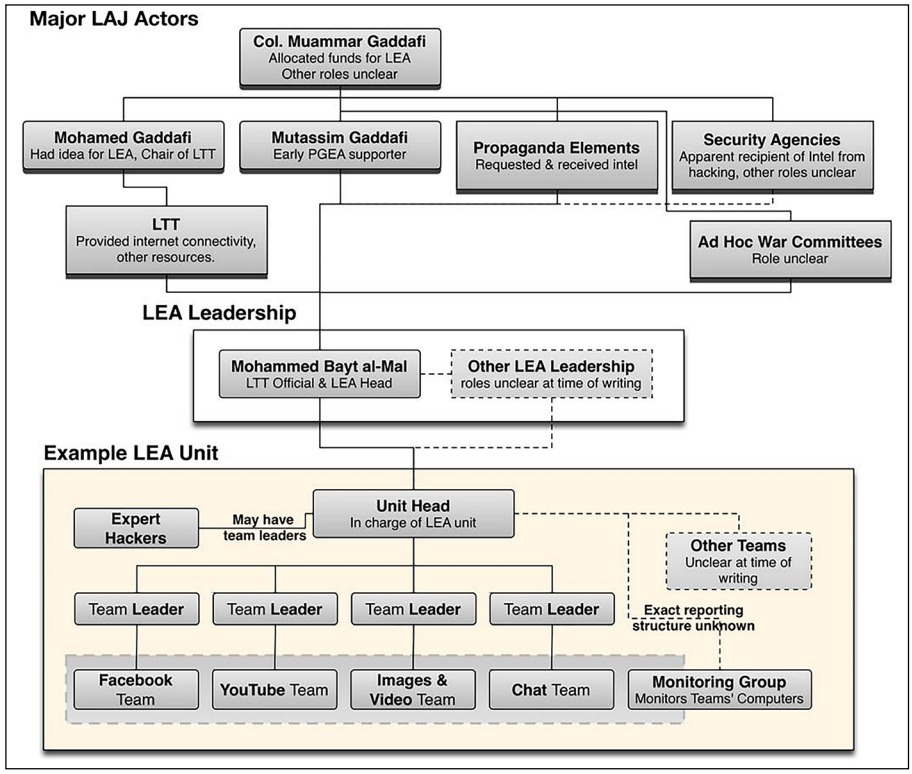


Figure 6.2 Potential, simplified command and control hierarchy of the Libyan Electronic Army for one LEA unit (of which there were reportedly at least three). Although the diagram indicates a fixed set of relationships, the LEA was not static.

throughout Tripoli, and appears to have operated with a sizeable base of volunteers and professional staff. Reportedly created at the urging of Mohamed Gaddafi, it grew increasingly formalized as the conflict progressed. (For information about the origins, background, and possible structure of the LEA, see Appendix C.)

The story of one, clearly junior, member of the LEA provides us with some insight into both the motivations that could lead someone to join the LEA and the way it worked:

> Nadia (not her real name) volunteered for the Electronic Army to protect herself after her uncle was arrested for helping protestors during the demonstrations . . . she submitted her ID papers and was accepted . . . she would go in whenever she felt like it to work at a three-story electronics factory in a suburb of Tripoli that housed one of the three wartime offices of the Electronic Army. She and the other volunteers would sit at the 40 or so PCs in the office, making pro-Gadhafi images, posting propaganda videos, and creating dozens of fake accounts to leave comments online.[165]

"Nadia" also illustrated the problems of morale and personnel that clearly beset the effort:

> [A]fter a while Nadia realized that the whole thing was a bit of a joke. Many members of the Electronic Army, she soon learned, were there largely because it was the only way to get Internet access in Tripoli during the war.[166]

While most of its members apparently were volunteers, the group also clearly employed the services of some professionals, including non-Libyans as well as Libyans overseas. Volunteers are reported to have been vetted with a background questionnaire, although not all of them were primarily motivated by patriotism.[167]

Seeming to confirm the limited skill and focus of the group of PGEAs, the Cyber Security Forum Initiative's April 2011 study of Libyan cyber security asserted that the primary focus of the relatively small number of regime supporters or "mercenary" hackers was defacing websites and concluded: "Gaddafi seems to lack internal state-supported hackers."[168] This appears to have been only partially correct: much of the hacking that took place during the revolution required little technical skill, and many of the activities of

PGEAs were limited to creating social media profiles that they used to post pro-Gaddafi material, deface websites, and flood the comments sections of opposition social media sites with pro-Gaddafi commentary. The Patriots of Misratah website is one of many examples: hijacked from a Misurata media group, it was hacked with pro-regime commentary and imagery.

Beyond public defacements, however, the LEA spent much of the revolution systematically attacking and compromising private communications networks and computers of the Libyan opposition.[169] According to a Libyan telecommunications engineer familiar with the matter, the more sophisticated members of the LEA have largely fled or gone into hiding, a claim that Aikins echoes. According to the same engineer, some are now among the post-revolution government's list of wanted individuals.[170]

Patriots of Misratah Facebook site as it appeared in spring 2012, still visibly defaced by pro-Gaddafi propaganda.

Non-Libyan PGEAs located outside the country may have taken part in actions against the Libyan opposition; however, evidence for this is very limited. Serbian Internet supporters of Gaddafi, for example, are believed by some to have been active in creating a wave of online social media–based pro-regime messaging, as well as claiming credit for defacing a number of opposition websites.[171]

Websites Hacked

A number of the highest-profile opposition websites, including EnoughGaddafi and feb17.info, were subjected to several kinds of attack. Although none was successful in permanently rendering the pages un-visitable, the attacks degraded the ability of the website operators to engage in effective messaging, and in at least one case may have exposed a site's visitors to malicious code. In the early days of the uprising, several pro-opposition pages were the targets of distributed denial of service attacks (DDoS), temporarily making it impossible to visit them.[172] Briefly, these attacks use a large number of computers (often machines compromised by malware and incorporated into a network of compromised machines, controlled by a remote attacker) to simultaneously generate an overwhelming amount of traffic to a specific page. If the attack is done correctly, the server(s) hosting the page will be unable to cope with the traffic, rendering the page un-visitable.

Later, the attacks took a more sophisticated direction: the websites of EnoughGaddafi.com and feb17.info were attacked based on an exploitation of vulnerabilities in their coding. The attack was used to compromise and modify material hosted on the sites, as well as to implant a piece of malware that vulnerable computers' browsers would automatically download. This malware was described as a remote access tool that would permit eavesdropping on keystrokes and audio, and presumably offer full access to file systems.[173]

Still other attacks involved using changing the domain registration of a prominent opposition website, again temporarily making it impossible for users to access the site.

Electronic Attacks Against Individual Libyans

A wide range of the attacks against Libyans can be categorized as account compromises. Without access to the servers and computers used to orches-

trate these attacks, their full scale and their success rate are likely to remain known only to PGEAs. Nevertheless, almost all of the Libyans engaged in the opposition and consulted for this case study could recall cases of friends and others who had various accounts hijacked during the course of the revolution. While it is likely that some accounts were compromised via insecure passwords or easily guessable account recovery questions, the most direct evidence comes from analysis of samples of malware sent by compromised accounts. Once an individual's computer was infected, any of the accounts that they connected to was likely to be compromised, including chat programs, Skype, e-mail, and Facebook.

LTT employees have described a desire on the part of the Libyan regime to compromise and monitor Skype communications.[174] This desire was similar, no doubt, to that of the Egyptian government, which at the time of its own revolution was considering the purchase of a half-million-dollar package that would provide it with access to the contents of Skype calls, among other things.[175]

Skype was an understandable target for the Gaddafi regime: it had become a central tool of opposition communications networks and was widely believed to be secure from LAJ interception. Indeed, Skype's encryption, even when traveling across regime-controlled networks, would have probably frustrated attempts at interception, as there is no evidence that the Gaddafi regime was able to decrypt Skype communications. Additionally, Skype communications over VSAT systems meant that the opposition's traffic exited the VSAT network at ground stations outside Libya, further limiting what could be observed. Yet, as the conflict demonstrates, it was quite possible to use social engineering to accomplish some of the same ends.

Although it is unclear how the wave of hacking began, its outlines can be described. Skype users whose computers had been compromised would find their accounts hijacked. The hijacked account, operated by PGEAs, would begin sending contextually relevant messages to accounts on the compromised users' contact lists. These messages would be followed by a file transfer, with files sometimes titled in ways that appeared relevant to previous chat transcripts. The files were malicious, however, designed to provide access to compromised machines. This access included the ability

to monitor activity on the machines, as well as enabling their microphones. In this way a target's Skype communications could be intercepted before they left the computer, and then covertly exfiltrated to those conducting the monitoring from the target computer.

The wave of hacking through Skype, and the use of compromised accounts, fueled another kind of paranoia. As one opposition member wrote while the conflict was still underway:

> I panicked. What if the person on the screen wasn't really who I thought he was? What if some security apparatus had hacked his account? Should I really be chatting to him?[176]

To encourage paranoia, the LAJ leadership chose to exploit its access to certain Skype calls, including playing the audio of Skype calls on state television and claiming the ability to intercept them.

Electronic Attacks Against Journalists

The targeting of the Libyan opposition by PGEAs was just one way in which the LAJ attempted to access communications pertinent to the conflict. Former Gaddafi regime officials with access to materials from the Libyan intelligence services have described efforts to compromise reporters' accounts. One example, a video sent to journalists purporting to depict human rights abuses in Tripoli, actually contained a remote-access Trojan. A former regime official noted that the attacks against journalists were largely unsophisticated, yet effective inasmuch as targeted individuals were willing to execute the content: "The problem wasn't the sophistication of the tools, but rather the lack of knowledge of the reporters."[177]

Friendly contacts within the Gaddafi regime sometimes tipped off pro-opposition figures about material exfiltrated from reporters' computers. One of these documents included an in-country source list for CNN. That document was clearly confidential and directly stated the concern of those using it that the contacts were both sensitive and closely held. A CNN official acknowledged that there had been a "possible breach" and noted his belief that "many sources who were speaking to these correspondents have been captured or killed."[178]

Malware Samples from PGEA Attacks: An Analysis

Samples of the malicious software deployed against several Libyan opposition targets have been collected and analyzed. This section briefly describes the analysis of these files by a security researcher, highlighting the capabilities of the underlying remote-access Trojan/remote administration tool.[179] Importantly, antivirus detection on the samples when initially deployed was quite low, meaning that most antivirus programs would not have recognized them as malicious.

Two files sent by the compromised accounts of the individual described below in Case 1 were saved by two contacts who received them. They are remote-access Trojans, programs that provide a remote individual access to key functions of the targeted computer. These programs, frequently used as part of cyber-criminal activity, can be acquired online from a shadowy community of developers and programmers.

Analysis reveals that the files were first compiled in early May 2011, shortly before they were sent to the target computer. Once executed by the user, either file places a file named Windowsdef.exe onto the target system. This file functions as a keylogger, capturing the user's typing. The program modifies the Windows registry to ensure that it is executed each time the user logs in, modifies Windows Explorer to give the program the ability to access files and run programs, and monitors the user by activating the web-cam and microphone. It also modifies the Windows firewall to allow itself to connect out of the computer, masquerading as Windows Messenger. The program also checks the IP address of the compromised machine, providing the attackers with information about the machine's location.

Example Cases of Account Compromise

To illustrate the types of compromise that took place during the conflict, this section briefly provides anonymized descriptions of Libyan opposition members who were successfully targeted by electronic attack.[180]

Case 1
Location: Western Libya
Connection: VSAT
Route of Compromise: Likely Trojan
Known Compromised Accounts : Skype, Facebook, online e-mail

Consequences: Degraded communications ability, loss of secrecy, infection of other accounts
Compromised Accounts Used?: Malware sent, targeted to contact list

The individual in this case played a central role in both aid and arms procurement in his city, and also acted as an information clearinghouse for aid and material requirements. Additionally, he played a role in hosting NATO liaison personnel. The first evidence of compromise showed in his inability to access his online e-mail account. Shortly thereafter, several of his contacts observed that his Skype account was sending out a series of suspicious files to his contacts. These file names included gaddafigooglemaps.exe, gadaffimaps.exe, misrataaid.exe, misratadeaths.exe, and natocontacts.exe.

Each of these names alluded to a feature of this person's activities that the attackers had presumably discovered. Sent to an unsuspecting contact, the files might easily have been executed. The compromise of some of his friends' accounts shortly thereafter indicated that this may have happened. It was later determined that his computer had been infected by several remote-access Trojans. Given the nature of this individual's activities, as well as the physical location of his computer in a highly protected area in which sensitive operational discussions were held, the machine may have provided a substantial window into the military and aid activities of the opposition in his city.

Gaddafigooglemaps.exe has been identified as the remote-access Trojan Blackshades NET, a sophisticated commercial Trojan easily available for purchase online with a rich set of functionality that permits a wide range of potentially illegal activities, including remote surveillance.[181] Interestingly, Blackshades NET has re-emerged approximately one year later, deployed against members of the Syrian opposition by Syrian PGEAs.[182]

Case 2
Location: Western Libya
Connection: VSAT
Route of Compromise: Unknown
Known Compromised Accounts: Facebook, online e-mail, MSN
Consequences: Degraded communications ability, loss of secrecy
Compromised Accounts Used?: Facebook account defaced with pro-Gaddafi material; pro-Gaddafi messages sent to contacts via e-mail

This individual played a number of roles in the opposition. A professional with good English and a flair for speaking with the press, he was a frequent source for international reporting. He also served as an emissary for the military council of his city and was directly involved in overseeing the assembling and transmission of targeting information to NATO contacts. His e-mail was a key component of this work: the same account not only served as a way to arrange interviews and communicate while overseas, it also served as his tool for transmitting coordinates and target descriptions. The first evidence that he was a target came when his MSN Messenger contacts "vanished" one day early in the uprising. After deciding that MSN was unsafe, he continued to use his e-mail account until he found himself unable to gain access. Shortly thereafter, his e-mail account appears to have been used to gain access to his Facebook page, which was subsequently defaced with pro-Gaddafi images, slogans, and disinformation. Although he received no information that his accounts were sending malware, he learned that his Hotmail account was used to send pro-Gaddafi messages to his contact list. He described the loss of his online e-mail account, along with the connectivity that it provided, as devastating.

Given the nature of his activities, it is likely that his account would have provided a detailed window into key aspects and individuals involved in the targeting process, as well as communications with various parties providing support to the opposition.

Case 3
Location: Western Libya
Connection: VSAT
Route of Compromise: Unknown, possibly via malicious use of account recovery
Known Compromised Accounts: YouTube, online e-mail
Consequences: Degraded communications ability, inability to communicate with journalists, loss of secrecy, possible disclosure of identity
Compromised Accounts: Made inaccessible
Compromised Accounts Used?: None observed

This very high-profile activist experienced the loss of his Gmail account, which was tied to his widely viewed YouTube account. Loss of access to these accounts made it impossible for the activist to post high-impact videos. It

also led to the possibility that his full identity, which had been camouflaged, might be revealed by the e-mail traffic contained in the account. He later discovered that information likely exfiltrated from his account, including identifying information about individuals he had been in contact with, were present in his file in Libyan state security. When access to the account was later recovered, it became apparent that it had been accessed by a computer with a Libyan IP address, strongly indicating that the compromise may have originated within Libya.

Discussion Questions

1. How did the Libyan opposition's forced switch to two-way satellite Internet and other connectivity impact the level of visibility that the LAJ had on Libyan network communications?
2. What strategies did the LAJ undertake to regain access to Libyan opposition communications?
3. The LAJ deployed PGEAs to hack the opposition's communications. What factors do you suspect contributed to their success in penetrating in some cases? What factors might have protected other opposition members?
4. PGEAs used inexpensive commercial malware designed for cybercrime and simple hacking techniques. Should these be considered "poor man's cyber weapons"? Why or why not?

Notes

137. N. Messieh, "How Far Gadhafi Went to Monitor Libya's Internet Activity," *Next Web*, August 30, 2011, http://thenextweb.com/me/2011/08/30/how-far-gadhafi-went-to-monitor-libyas-Internet-activity/

138. "Exclusive: How Gaddafi Spied on the Fathers of the New Libya," OWNI, December 1, 2011, http://owni.eu/2011/12/01/exclusive-how-gaddafi-spied-on-the-fathers-of-the-new-libya/

139. "Internet Filtering in Libya," OpenNet Initiative, August 6, 2009, http://opennet.net/research/profiles/libya

140. Blocking of previously designated IP addresses at the level of the LTT; ibid.

141. Ibid.

142. T. Dennis, "French Provide Geolocation Capability to Gaddafi Spies," GoMoNews, August 30, 2011, http://www.gomonews.com/french-provide-geolocation-capability-to-gadafi-spies/

143. F. Amedo, " 'Comment j'ai mis 5 millions de Libyens sur écoute,' " *Le Figaro*, September 6, 2011, http://www.lefigaro.fr/international/2011/09/01/01003-20110901ARTFIG00412-comment-j-ai-mis-8-millions-de-libyens-sur-ecoute.php

144. J.M. Manach, "Al Jazeera espionné par Amesys," OWNI, December 14, 2011, http://owni.fr/2011/12/14/al-jazeera-amesys-espionnage-spyfiles-libye/

145. http://www.amesys.fr/

146. Original text: "On faisait du massif: on interceptait toutes les données passant sur Internet: mails, chats, navigations Internet et conversation sur IP." Quoted in Amedo, " 'Comment j'ai mis 5 millions de Libyens sur écoute.' "

147. Original text: "...par exemple, comment placer une université sous interception et trouver des individus suspects en fonction de mots clefs." Quoted in Ibid.

148. "Glint: Strategic Nationwide Interception Based on EAGLE Core Technology," Amesys, September 2011, http://reflets.info/wp-content/uploads/2011/09/Glint_EN.pdf

149. See also: J.M. Manach, "Mode d'emploi du big brother Libyen," OWNI, September 7, 2011, http://owni.fr/2011/09/07/le-mode-demploi-du-big-brother-libyen/

150. "Exclusive: How Gaddafi Spied on the Fathers of the New Libya."

151. P. Sonne and M. Coker, "Firms Aided Libyan Spies," *Wall Street Journal*, August 30, 2011, https://www.wsj.com/articles/SB10001424053111904199404576538721260166388; M. Aikins, "Jamming Tripoli: Inside Moammar Gadhafi's Secret Surveillance Network," *Wired*, May 18, 2012, http://www.wired.com/threatlevel/2012/05/ff_libya/

152. M. Aikins, Personal communication.

153. One photo shows a ZTE-branded nameplate, identifying the system as the Phase 1-IGW-LIC, which may indicate the system Intercept Gateway Legal Intercept Controller or similar.

154. "PTSN Transformation via ZTE NGN Solution: ZTE F3G Migration Solution," PDF of a presentation provided to Iran Telecommunication Research Center, May 4-5, 2008. Author's collection.

155. Sonne and Coker, "Firms Aided Libyan Spies"; Aikins, "Jamming Tripoli." "

156. Aikins, "Jamming Tripoli."

157. Sonne and Coker, "Firms Aided Libyan Spies."

158. Ibid.

159. F. Amedo, "La France mal armée pour enquêter sur le Net," *Le Figaro*, April 26, 2011, http://www. lefigaro.fr/actualite-france/2011/04/25/01016-20110425ARTFIG00443-la-france-mal-armee-pour-enqueter-sur-le-net.php

160. Aikins, "Jamming Tripoli."

161. At the time of writing, publicly available evidence cannot confirm the existence or the scope and scale of VSAT interception or monitoring capacities.

162. Author's Note: I have settled on this term to describe hackers and other electronic actors whose actions identify them as acting in support of a government, but whose direct affiliation with the government are unknown, imperfectly understood, informal, not subject to standard government hierarchies of command and control, or controversial.

163. I. Sigal, "Libya: Foreign Hackers and Surveillance," Global Voices Advocacy (blog), October 26, 2011, http://advocacy.globalvoicesonline.org/2011/10/27/libya-foreign-hackers-and-surveillance/

164. Aikins, "Jamming Tripoli."

165. Ibid.

166. Ibid.

167. Ibid.

168. Project Cyber Dawn, Cyber Security Forum Initiative, April 17, 2011.

169. Ibid.

170. Personal communication with L2, Spring 2012.

171. Personal communication with L3, Spring 2012.

172. Personal communication with L4, Spring 2012.

173. S. Stecklow, P. Sonne, and M. Bradley, "Mideast Uses Western Tools to Battle the Skype Rebellion," *Wall Street Journal*, June 1, 2011, http://online.wsj.com/article/SB10001424052702304520804576345970862420038.html

174. Sigal, "Libya: Foreign Hackers and Surveillance."

175. Stecklow et al., "Mideast Uses Western Tools to Battle the Skype Rebellion."

176. N. Daoud, "Fear and Revolution in Libya," n.d., http://www.lb.boell.org/downloads/Perspectives_02-33_Nahla_Daoud.pdf

177. M. Aikins, "The Spy Who Came in From the Code," *Columbia Journalism Review*, May 4, 2012, http://www.cjr.org/feature/the_spy_who_came_in_from_the_c.php

178. Ibid.

179. Analysis of malware described in this section has been conducted by security researcher Morgan Marquis-Biore.

180. The cases are drawn from personal communication with victims.

181. A. Kujawa, "You Dirty RAT! Part 2 – BlackShades NET," MalwareBytes Unpacked (blog), June 15, 2012, http://blog.malwarebytes.org/intelligence/2012/06/you-dirty-rat-part-2-blackshades-net/

182. E. Galperin and M. Marqis-Boire "New Malware Targeting Syrian Activists Uses Blackshades Commercial Trojan," Electronic Frontier Foundation (blog), July 12, 2012, https://www.eff.org/deeplinks/2012/07/new-blackshades-malware

CHAPTER
SEVEN

Conclusions

Asymmetries of Risk

The Libyan opposition's ability to rebound from a complete Internet and communications blackout illustrates its immense value to an opposition movement in an asymmetric conflict. The remarkably diverse ways they used their regained Internet connectivity helped them overcome substantial asymmetries in access to resources and communications networks. Yet many of the opposition's ad hoc communications networks and the ways in which it reconnected guided both individuals and groups into a series of practices that did little to mitigate the asymmetries of risk between it and the LAJ.

While these risks were not fatal to the opposition's success, NATO support likely buffered the opposition from some of the greatest vulnerabilities introduced by weak operational security. This discussion will briefly highlight these themes before concluding with a discussion of the implications of this case for future conflicts.

By being forced to move into Internet connectivity and communications that the LAJ could not observe, the opposition ended up achieving greater security for their communications. They may have enhanced this in specific instances by their preference for tools like Skype, which the LAJ was probably unable to un-encrypt. Yet, as the previous section illustrates, host-level security remained almost completely unaddressed.

The ways that the Libyan opposition used social media and the Internet made it possible for a geographically distributed group of Libyans, both in-country and in the diaspora, to contribute to many aspects of the fight, and to do so while benefitting from the often-rich situational awareness offered by groups that served as information clearinghouses. This kind of fusion of information, needs, tactics, and strategizing made it easier for information to reach the right people. It also meant that decisions could be made with surprising responsiveness and with the benefit of a great deal of

situational awareness. Information, however, was also much less compartmentalized and hence more vulnerable to access by the "wrong" people. The price of operational security was clearly not fully appreciated.

Comprehensive Vulnerability

Throughout the conflict, many Libyan opposition actors sought to protect their identities or conceal key features of their activities from LAJ security services. In areas that were under LAJ control, opposition actors faced imprisonment, physical violence, torture, and possible death for their activities. Even in areas militarily under their own control or otherwise denied to the LAJ, opposition actors still risked reprisals to family members, as well as the operational security risk that their actions could provide the LAJ with sensitive information.

It is important to note how serious the operational security risks were with the use of social media accounts to engage in opposition activities, and how imperfectly these risks were mitigated. When the revolution began, many opposition members turned to pre-existing networks of friends, neighbors, and associates. This often meant using familiar tools that could be quickly accessed, including existing social media and e-mail accounts.

Keeping old accounts and online identities associated with real names or consistent aliases from before the revolution was, of course, convenient and efficient: e-mail accounts and social media profiles are a repository of contacts and other personal information. Changing or discarding accounts could mean becoming unreachable by old contacts. Many in the opposition also engaged in a wide range of posting and other public or semi-public communications in support of the opposition on social media, using the same accounts that they used for more sensitive activities. These practices made them vulnerable to discovery and unmasking. Even when members adopted pseudonyms for more sensitive activities, they often communicated with Libyans who did not disguise their online identities.

All of these activities made the Libyan opposition networks, groups, and individuals highly vulnerable to a range of straightforward network analyses, targeting, and attack. Even if specific individuals practiced consistently strong personal operational security, being an informed and contributing opposition supporter often required some degree of participation in social networks.

This kind of activity could in turn make the individual vulnerable to the weaker links of their network.

The LAJ appears to have lost its access to sophisticated network analysis analytics through Amesys and ZTE monitoring equipment when it disabled the Internet, and it is unlikely that it was able to reproduce this level of automated analysis of the opposition based on the skills and resources of PGEA and the LAJ intelligence services. Nevertheless, the LAJ's apparent ability to target specific high-value but not public targets, such as the Libyan described in Case 1, suggests that it successfully exploited some features of the opposition's networks.

The accounts and computer of a single electronically compromised well-connected opposition supporter could be, and likely were, exploited to gather information about that person's entire network of contacts, associations, and communications on social media and to collect extensive information from groups to which they belonged. The participants and the entire transcript of an invitation-only or closed Facebook group could, for example, be viewed from the beginning using a single compromised account. The same would have been true for Skype, e-mail, and other accounts.

Risks Never Addressed

When the Gaddafi regime cut the Internet, it inflicted a widely criticized blow against Libyans' ability to communicate with each other and with the outside world. The regime was not able to keep Libyans offline for long, however. This case study tells the story, both within the public eye and far out of it, of how communications activities by the Libyan opposition were underpinned by a range of low-cost and decentralized technologies that often relied on Internet connectivity. The Internet didn't just connect Libyans as individuals and groups to the Internet; it also connected them to diaspora Libyans, friendly countries, the world media, and many other key resources.

By shutting down the Internet, the regime clearly hoped to stop the spread of rebellion, or perhaps to prevent information and documentation of its crackdown from reaching a global audience. In the process, the LAJ also completely disabled their pre-revolution Internet-monitoring infrastructure. But their efforts to regain a view of opposition communications didn't cease.

Throughout the conflict, PGEAs, apparently operating under the direction of the LAJ or possibly the personalized supervision of Gaddafi's son Mohamed, embarked on a multi-pronged electronic campaign against the Libyan opposition. They publicly harassed and attempted to counter-message the opposition. These attempts were often very crude, and did little to change the public image of the Gaddafi regime as a violent and unreasonable actor intent on silencing its citizens. Further from the public eye, PGEAs worked to hack and exploit opposition members' accounts and planted tools that allowed them to exfiltrate sometimes highly sensitive information about their adversaries.

An ex-regime official noted that the wave of attacks was unsophisticated. Some targets recognized that they were being asked to execute malicious files and refrained from opening them, yet many others did not. Why would such an elementary security precaution be ignored? It appears that the emphasis after the Gaddafi regime shut down the regime was on *connecting,* not *securing*—on restoring connectivity through different tools outside the regime's control and on fighting battles. When they did reconnect, it was with the urgency of a group in mortal danger, intensely preoccupied with the ongoing fighting. As one Libyan put it, "If we were vulnerable we couldn't care less . . . we were desperate to get our voices out . . . it was a matter of life or death . . . it was just vital to get this information out."[183] Although Libyans made highly effective use of the Internet in many spheres of the conflict, they did so with comparatively little understanding of how they themselves might be targeted online.

Many Libyans entered the conflict with considerable know-how and resources to invest in restoring Internet connectivity but little experience in circumvention and security tools. Few had pre-revolution experience with trying to evade the regime's censorship or monitoring. Although Internet monitoring was widely perceived to exist prior to the revolution, Libyans' Internet usage had not been honed by the need to bypass extensive filtering or censorship.[184] The substantial breaches of operational security, personal safety, and source confidentiality described here should illustrate the extreme risks faced by opposition groups that use standard Internet tools and common operating systems. While they may be able to connect by a combination of strong motivation, resources, and ingenuity, security is another matter.

Although some in the Libyan opposition recognized the risk, this author has been unable to find any evidence of comprehensive threat modeling, auditing, or mitigation strategies at any influential level beyond specific responses to individual attacks (e.g., on a website).

The impact of these electronic exploitations are hard to quantify. It is unclear how direct the intelligence-gathering linkages were between PGEAs and, say, officers engaged in battlefield strategy. Had the linkages been good, and had NATO airpower not been present to interdict certain troop movements, these exploitations might have influenced the outcomes of battles. It is not hard to imagine that had many of the compromised individuals not been physically located in areas denied to LAJ forces, they would have been likely targets for elimination.

Moving Forward

Lessons from the 2011 Libyan revolution are still being digested. The author hopes the reader will come away with a sense that LAJ attempts to hack and disrupt the opposition's use of Internet technology were, although failures, something to be taken very seriously. At the time of writing, the Syrian opposition is using many of the same communications tools and practices as the Libyan opposition did. It is now abundantly clear that many of the same tactics that the Gaddafi regime used against Libyans, such as targeted malware and extensive attacks against social media activities, are being aggressively deployed by PGEAs in Syria. While the presence of NATO support for the Libyan opposition may have decisively tipped the battle in its favor, this support may also have masked just how risky some of the opposition's communications practices really were. Figures in arms procurement, military planning, and aid in Misurata were hacked, and their computers were used to spy on them. If NATO hadn't been able to interdict LAJ attempts to enter Misurata, this kind of knowledge might have substantially changed the course of the fighting and the outcome of the revolution.

In conflicts without an overwhelming superiority of force on the side of the opposition, we must understand the risks associated with opposition groups and fighters' use of mass-audience "civilian" Internet technology. This is doubly true when communications remain on networks that remain under regime control. More generally, there are inherent dangers associated

with using common online tools in high-risk situations, especially given the tremendous disparity in security resources and expertise between opposition groups and states. Additionally, the emergence of pro-government electronic actors, whose behavior and collaboration with governments can be analogized to militias in some cases, represents a serious and under documented category of online threat. The risk is particularly great for decentralized groups and individuals with limited resources and expertise in security, and for whom the Internet has become a central tool in their efforts for reform and democracy. Failure to understand and prepare for these threats is a substantial risk that opposition movements and their international partners and supporters cannot afford to take.

Discussion Questions

1. After reading this case study, what is your perspective on whether commonly used online services are safe enough to provide the communications backbone to an opposition movement in a conflict?
2. What are the inherent operational security risks to using social networking? How were these risks amplified for the Libyan opposition?
3. Can you think of two measures that could have been taken by the Libyan opposition to increase their operational security, given their choice of communications tools?
4. Name several ways that an international actor, such as a NATO member state, could have assisted the Libyan opposition in increasing their operational security and mitigating the threat from PGEAs.

Notes

183. Interview with L2, Spring 2012.

184. I. Sigal, ""Libya: Foreign Hackers and Surveillance," Global Voices Advocacy (blog), October 26, 2011, http://advocacy.globalvoicesonline.org/2011/10/27/libya-foreign-hackers-and-surveillance/

Appendix A
Libya Country Profile

Libya Before the Uprising: A Brief Note[185]

After a military coup in 1969, Libya was ruled by Colonel Muammar Abu Minyar al-Gaddafi until 2011. During the first decades of his rule, Gaddafi developed unique political philosophy from a combination of socialist theory and Islam. He applied this philosophy to the governmental structure of Libya while simultaneously using oil revenues to promote this ideology abroad.

An unsuccessful military attempt to establish control of areas of Northern Chad in 1987 led to a retreat, Libya was strongly sanctioned by the United Nations over its responsibility for the Lockerbie bombing in 1992. These sanctions were suspended and later removed in 2003 after Libya admitted its role in the bombing and simultaneously announced it would cease support for terrorism and end its efforts to develop weapons of mass destruction (WMDs). These measures were followed by financial compensation to the victims of terrorist acts sponsored by Libya. The U.S. completed its removal of unilateral sanctions against Libya in 2006. Libya's willingness to undertake these measures led to a reopening of diplomatic relations, including with Western powers.

This trend of apparent reform continued right up to the uprising, with the Libyan government implementing a wide range of measures intended to normalize its diplomatic and economic position. This relatively recent opening and the lifting of multilateral and unilateral sanctions explains how a state widely perceived as an international pariah could have acquired sophisticated export-controlled monitoring and surveillance equipment from Western companies like Amesys.

Libya Today

At the time of writing, Libya has passed from the 2011 revolution into a challenging period of reconstruction. It is governed under an interim constitution by the National Transitional Council, an entity first created during the 2011 uprising. After a relatively peaceful election, Libyans have elected a General National Congress that will draft Libya's new, permanent constitution, before it is put to a referendum by the Libyan people.

Appendix B
Timeline of the 2011 Libyan Revolution

The 2011 Libyan revolution lasted just over eight months. The conflict began as a series of small protests in the eastern city of Benghazi, the direct result of the detention of a well-known lawyer. It ended with the total defeat of forces loyal to Colonel Muammar Gaddafi and the end of his regime. This brief and selective timeline provides an overview of key events in the conflict and highlights events relevant to this case study.

The Arab Spring

A series of protests that began in Tunisia on December 18, 2010, have since given way to a series of political transformations throughout the Middle East and North Africa (MENA). After the first protests in Tunisia, which forced out its president, leaders in Egypt, Libya, and Yemen have all been forced from power. Meanwhile, other countries like Bahrain experienced substantial civil unrest, and Syria is undergoing a civil war. Since 2010, substantial protests have also taken place in Algeria, Iraq, Jordan, Kuwait, Morocco, and Sudan, with sporadic protests in Lebanon, Mauritania, Oman, Saudi Arabia, and the Western Sahara.[186]

In many cases, attempts by MENA governments to control protests seem to have had the opposite of the intended effect, fueling protesters' grievances and fulfilling many protestors' perception that their states are governed by regimes incapable of accepting democratic rule or the political preferences of large segments of their populations. At the time of writing, not only does political unrest continue in several countries, but the political implications for the region and beyond continue to unfold. Secondary effects continue to unfold as well, such as the ongoing crisis in Mali, which appears to have been partially fueled by groups that supported Gaddafi during the Libyan revolution, traveling with new weapons and experience to Northern Mali.

The Early Days

February 4

News organizations report that calls for protest in Libya on February 17 have emerged in social media.

February 13

Media reports that the Gaddafi regime has arrested some activists using social media and warned Libyans not to use Facebook.

February 15

The first signs that a large popular uprising might be underway. Hundreds of protesters take to the streets to protest the arrest of lawyer Fethi Tarbel, who had been campaigning for the release of political prisoners.

February 16

- Protests in Tripoli, Benghazi's central square, Derna, and Zintan result in clashes, sometimes violent, with police.
- "Day of Anger" Facebook page count of followers doubles.

February 17

- "Day of Rage"/"Day of Anger"/"Day of Revolt" protests throughout Libya. Protests in Benghazi and Tripoli are met with violent, lethal force.
- Al Jazeera announces that their programming is being removed from state-owned cable networks.

February 18–19

- Large protests in Benghazi's central square. Protests also take place in Bayda, Derna, Toubrouk, Misurata, and Tripoli. The protests are met with violent, sometimes lethal, force. Some in the international community express concern over violence against civilians.
- The regime undertakes a 6.8- hour Internet blackout in the evening of the 18th, and an 8.3-hour Internet blackout on the evening of the 19th.
- Nilesat and Arabsat satellites subjected to jamming from inside Libya.
- Mohammed Nabbous establishes Libya Alhurra TV, broadcasting from Benghazi.

February 20

- Intensity of protests increase in Benghazi, Tripoli, and throughout Libya. Reported casualties also increase.
- Protesters attempt to seize Green Square in Tripoli.
- Reports that elements of the local military have joined in protests.
- Gaddafi's son, Saif al-Islam, blames Israel and foreign actors for protests.
- International community urges Gaddafi regime to refrain from violence.
- News organizations' attempts to enter Libya are rebuffed.

February 21–24

- Protests in Benghazi take control of large parts of the city, and protesters in Tripoli take control of key buildings as casualty numbers continue to grow.
- Later protests in Zawiya and Tripoli are put down with substantial lethal force.
- Two pilots from Libyan Air Force defect to Malta with their Mirage F-1 fighter jets.
- Military commander and interior minister Abdul Fatah Younis resigns, defects.
- Battle of Misurata begins with attacks on Libyan Air Force planes and personnel.
- Gaddafi makes appearance on Libyan television to confirm he has not fled Tripoli, urges Libyans not to believe television broadcasts from "stray dogs." Within 24 hours makes a second appearance, stating he is prepared to die as a "martyr." Threatens to use even more force.
- Al Jazeera accuses the Libyan government of jamming its signal, affecting broadcasting in the region. Pinpoints jamming to Libyan government-operated facility south of Tripoli.
- Reporting increasingly highlights the possibility that the regime will fall.

February 25

- More protests in Tripoli after several days of calm, met with intense violence.
- Thuraya announces that jamming has been underway for approximately a week on their satellites serving Libya, accuses Libyan government, says it is working to restore services.
- Conflict intensifies, increasingly organized opposition.

February 26–March 2

- UN Security Council votes to impose sanctions, embargo, and asset freeze on Gaddafi's family and regime. Refers Libya's leaders to the International Criminal Court.
- Other international sanctions against Gaddafi and his family.
- Major battles in Zawiya.
- Formation of the National Transitional Council (NTC) on February 26.

- In various interviews and statements, Gaddafi confirms he will not step away from power.
- Increasingly organized opposition fighting in Benghazi, partly under direction of Younis.

March 3

Total Internet blackout. Phone system disruptions throughout Libya, phone services cut to eastern Libya.

March 4

The NTC announces that it is the only legitimate representative of Libya as Gaddafi loyalists.

March 5–16

- LAJ forces mount sustained attacks against opposition forces in eastern Libya, fighting over contested areas of Ras Lanuf, Brega, and Adjdbia.
- Countries including France begin to recognize NTC as legitimate representative of Libya.

The United Nations Security Council Passes Key Resolutions, NATO Begins Air Campaign

March 17

The UN Security Council votes to impose no-fly zone and other military action to protect Libyan civilians.

March 19

- UK and French forces launch air attack, halt advance of LAJ forces towards Brega.
- Mohammed Nabbous killed hours before the air attack.

March 31

NATO Operation UNIFIED PROTECTOR officially begins in Libya to enforce UN Security Council Resolutions 1970 and 1973, which include no-fly zone, civilian protection, and arms embargo.

The Libyan Conflict Extends on Multiple Fronts

April 1– August 19

- Libyan opposition forces from Benghazi secure control of Benghazi and eastern Libya with the exception of Sirte and neighboring towns.

- After months of siege, fighters from Misurata free the town from LAJ forces in mid-May, pushing opposition control south and eastwards.
- Opposition fighters in the Jebel Jafusa (Nafusa Mountains) fight town-by-town to assert control over the region.
- Southern Libya, Sirte, Sabha, Bani Waleed, Tripoli, and its outskirts all remain under LAJ forces' control.
- Hacking of computers first reported in early May. Original locations and targets unknown.

August 20–23

- Operation ODYSSEY DAWN: Libyan opposition forces enter Tripoli from multiple fronts, supported by NATO airstrikes and resistance sleeper cells in the capital. They meet only light resistance.
- Gaddafi's compound and broadcasting facilities overrun.

September 8–13

- NTC leader Abdu Jalil arrives in Tripoli, makes first speech from the capital.
- Fighting shifts towards goal of overtaking remaining bastions of Gaddafi Loyalist control.

Multiple Opposition Fighting Forces Gain Control of Remaining Pockets of Gaddafi Loyalists

September 21

Sabha, bastion of Gaddafi loyalists, falls to NTC control.

October 17

Bani Waleed captured, one of the remaining strongholds of Gaddafi loyalists.

October 20–22

- NTC fighters establish complete control of Sirte, with support from NATO airstrikes, eliminating the last pocket of Gaddafi loyalists.
- October 20: Gaddafi is captured and dies in custody.
- October 22: End of hostilities announced.

October 31st

All NATO military operations cease in Libya.

Appendix C
The Libyan Electronic Army – History and Structure

The self-styled "Electronic Army" tracks its origins, according to a number of reports, to a small group of PGEAs who were assembled prior to the 2011 revolution, although the exact timeline of its creation is uncertain. According to an account provided to someone conducting research in Libya shortly after the fall of Gaddafi's regime,[187] some of these individuals were reportedly active at the encouragement of Gaddafi's son Mutassim in the context of efforts to respond to exile groups' information operations in the late 2000s, although they may have begun working together before this. Mutassim had been infuriated by content posted showing him at decadent and lavish parties, and the group was reportedly constituted to pull down the content and retaliate against the people responsible. Beyond attempting to compromise accounts, the group is reported to have systematically abused the copyright infringement reporting functionality of sites like YouTube to attempt to get users and channels banned.

While the composition of this early group remains somewhat unclear, membership reportedly included requirements of a rudimentary background check.[188] The term "Electronic Army"[189] seems to have been introduced at some point during this period. One of the individuals apparently involved in this pre-revolution hacking was Ahmed Gwaider, one of the few Libyan hackers who was sympathetic to Gaddafi's regime. Aikins' reporting has Gwaider involved in pro-government hacking prior to 2010, when he was provided with a villa and a small team working under him. Gwaider's skills are described as especially keen in tricking or manipulating targets into executing malicious software, divulging credentials, or providing access to target machines. One dissident described how during the revolution Gwaider used social engineering to convince her to open a Microsoft Word document containing a malicious file. Gwaider used the software to capture photos of the dissident without her headscarf, which he later posted online, and to secretly record and exfiltrate a Skype conversation with a foreign journalist, which was later broadcast on state television.[190] While Gwaider's exact position in the formal LEA structure is unclear, his preference for social-engineered malware fits the LEA's known attack style.

After the 2011 revolution began, this group of PGEAs evolved into a more formalized Libyan Electronic Army (LEA), reportedly at the urging of Mohamed Gaddafi. Reports from multiple sources indicate that the LEA membership and resources expanded as the conflict began. Equipment was purchased, buildings were allocated, and the LEA gained an increasingly formalized structure, although the exact organizational hierarchy remains unclear.

Aikins has reported that the group may have had over 600 members in Tripoli alone.[191] What were the responsibilities of these members? One source[192] intimately familiar with the LEA described the group as operating from at least three locations within Tripoli.[193] This individual's description of one location can provide an outline of some of the LEA's activities. The building's equipment was reportedly purchased as part of a payment of one million Libyan dinars (approximately $800,000), allocated by Muammar Gaddafi.[194] The building, which we will refer to as an organizational unit, housed several teams, each with its own leader. There was a Facebook team, a YouTube team, a team dedicated to compromising chat accounts (e.g. Yahoo! Chat), a team dedicated to producing video and imagery content, and so on. The unit included internal network surveillance of the teams' activities. Details are scarce about these internal monitors, but they appear to have included a more experienced group in the LEA and were comprised of some individuals linked to LTT. LEA volunteers who transgressed while on premises were sometimes threatened by their superiors.[195]

We can infer from this that the LEA likely had a structure that included multiple units, each with a leader, which are likely to have had teams with team leaders.[196] These units reportedly received direction from Mohammed Bayt al-Mal, who held a senior position at LTT, according to Aikins' reporting. However, other names have emerged as working closely with Bayt al-Mal from sources familiar with the LEA,[197] complicating the idea of a unified structure. The same sources also note that the LEA sometimes provided information to elements of the LAJ directly involved in propaganda. At least one source has named several Libyan television personalities as direct recipients of information exfiltrated from compromised opposition computers, a narrative that matches the occasional use of clearly hacked material (e.g., the audio of Skype calls) on LAJ-controlled channels during the conflict. Other parts of the LAJ government may have been recipients of this information, but there is limited evidence available at the time of writing to confirm a fixed command or reporting relationship.

Appendix D
Terms and Abbreviations

Common Terms

Amesys – French technology company, creator of the EAGLE interception package purchased by Libya

Amesys EAGLE – Massive intercept solution permitting the capture, storage, and automated network analysis of a wide range of electronic communications

Blackshades NET – A remote-access Trojan be used against the Libyan opposition

Domain name server (DNS) – Domain name servers contain databases that link websites' URLs to Internet Protocol (IP) addresses. Filtering at the DNS entails identifying requests from a user's computer to connect to a restricted or blocked website, then blocking or redirecting these requests to alternate websites, and refusing to connect to the correct website's IP address.

GRAD rocket 122 mm – Unguided multiple rocket artillery launcher that can be truck-mounted. The Grad was a commonly used rocket system in Libya, and it figured prominently in LAJ forces' actions against the Libyan opposition.

Huawei – Huawei Technologies Company, a Chinese multinational and the world's largest telecommunications equipment company

Keylogger – Software that records a user's keystrokes. Commonly incorporated into remote-access Trojans.

Libyan Arab Jamahiriya (LAJ) – Government of Libya, 1977–2011

Libyan Arab Jamahiriya forces – Term used in this case study to refer to all Libyan armed forces (army, air force, navy), pro-Gaddafi tribal units, paramilitary forces, and mercenaries

Libyan opposition forces – Term used in this case study to refer to all fighting forces loyal to the National Transitional Council, including the Free Libyan Air Force, the National Liberation Army, and other anti-Gaddafi fighting units not under the NTC's centralized command

Libyan Telecom and Technology – Libya's Internet provider, chaired by Mohamed Gaddafi, son of Muammar Gaddafi

National Front for the Salvation of Libya – Exiled opposition group, active online from the first days of the revolution

Pro-Government Electronic Actor (PGEA) – Author's term. Hackers and other electronic actors whose actions identify them as acting in support of a government, but whose direct affiliation with the government are unknown, imperfectly understood, informal, not subject to standard government hierarchies of command and control, or controversial

Remote-access Trojan – Malicious software that allows a remote attacker to execute arbitrary code and exfiltrate information from a target computer

Remote administration tool – See: Remote-access Trojan

Thuraya – A satellite phone and services provider widely used in the Middle East and North Africa

Two-way satellite Internet – Equipment for the upload and download of data using satellite connectivity, typically including a ground station communicating with a satellite network

Very Small Aperture Terminal – Ground station for a two-way satellite Internet connection

Voice Over Internet Protocol – Technologies permitting voice communication over the Internet

ZTE – Zhongxing Telecommunication Equipment Corporation, China's second largest telecommunications equipment and services company

ZTE ZXMT – Massive intercept solution by ZTE that permits the capture, storage, and automated network analysis of a wide range of electronic communications

Common Abbreviations

DDoS	Distributed Denial of Service Attack
DNS	Domain Name Server
GPTC	General Post and Telecommunications Company
IP	Internet Protocol
LAJ	Libyan Arab Jamahiriya
LEA	Libyan Electronic Army
LTT	Libyan Telecom and Technology Company
NFSL	National Front for the Salvation of Libya
NTC	National Transitional Council
PGEA	Pro-Government Electronic Actor
RAT	Remote Administration Tool/Remote-Access Trojan
VOIP	Voice Over Internet Protocol
VSAT	Very Small Aperture Terminal

Notes

185. Paraphrased from "Libya," *CIA World Factbook*, 2012, https://www.cia.gov/library/publications/the-world-factbook/geos/ly.html

186. For an in-depth review of the events of the Arab Spring up to the end of 2011, see "Arabian Spring 2010-2011," Uppsala University, Department of Peace and Conflict Research, http://www.pcr.uu.se/digitalAssets/87/87711_chronologic_timeline_arabian_spring.pdf

187. The individual conducting research requested to remain anonymous, citing security concerns, and is referred to here as L5. Personal communication with the author, Winter 2012-2013.

188. Ibid.

189. الجيش الالكترونية

190. "M. Aikins, "Jamming Tripoli: Inside Moammar Gadhafi's Secret Surveillance Network," *Wired*, May 18, 2012, http://www.wired.com/threatlevel/2012/05/ff_libya/

191. Aikins, "Jamming Tripoli."

192. Personal communication with L5.

193. Locations: One in the Dahra neighborhood of Tripoli, another in the vicinity of Abu Slim, and the third near the Tareeg al Shat (the Coastal Road). Other locations have been suggested by other sources but remain unclear at time of writing.

194. Ibid. Reportedly intended to be followed by a second payment. It is unclear whether this payment was ever made.

195. Ibid.

196. It is unclear whether any of these teams operated across LEA locations or whether each team operated only under the authority of the unit they were located in; however, those that the source was familiar with appear to have operated somewhat independently of each other.

197. Ibid.

Further Reading

M. Aikins, "Jamming Tripoli: Inside Moammar Gadhafi's Secret Surveillance Network," *Wired*, May 18, 2012, http://www.wired.com/threatlevel/2012/05/ff_libya/

M. Aikins, "The Spy Who Came in from the Code," *Columbia Journalism Review*, May 4, 2012, http://www.cjr.org/feature/the_spy_who_came_in_from_the_c.php

T. Bradshaw and J. Blitz, "NATO Draws on Twitter for Libya Strikes," *Financial Times/Washington Post*, June 15, 2011, http://www.washingtonpost.com/world/nato-draws-on-Twitter-for-libya-strikes/2011/06/15/AGLJpTWH_story.html

M. Coker and C. Levinson, "Rebels Hijack Gadhafi's Phone Network," *Wall Street Journal*, April 13, 2011, http://online.wsj.com/article/SB10001424052748703841904576256512991215284.html

M. Coker and P. Sonne, "Life Under the Gaze of Gadhafi's Spies," *Wall Street Journal*, December 14, 2011, http://online.wsj.com/article/SB10001424052970203764804577056230832805896.html

J. Pollock, "People Power 2.0: How Civilians Helped Win the Libyan Information War," *MIT Technology Review*, April 20, 2012, http://www.technologyreview.com/web/40214/

I. Sigal, "Libya: Foreign Hackers and Surveillance," Global Voices Advocacy (blog), October 26, 2011, http://advocacy.globalvoicesonline.org/2011/10/27/libya-foreign-hackers-and-surveillance/

P. Sonne and M. Coker, "Firms Aided Libyan Spies," *Wall Street Journal*, August 30, 2011, http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html

S. Stecklow, P. Sonne, and M. Bradley, "Mideast Uses Western Tools to Battle the Skype Rebellion," *Wall Street Journal*, June 1, 2011, http://online.wsj.com/article/SB10001424052702304520804576345970862420038.html

Study Guide

Discussion Questions — *from the text*

CHAPTER ONE

1. How did Libya's level of Internet penetration compare to its neighbors? Does this challenge the idea that the Internet could have facilitated an Internet shutdown?
2. How might Libya's centralized Internet infrastructure and governance have facilitated an Internet shutdown?

CHAPTER TWO

1. What kind of signal did Libya send the world when it shut down the Internet?
2. What kind of considerations are likely to have influenced the LAJ's decision to shut down the Internet?
3. How did blocking the Internet affect the credibility of news reports from the ground?

CHAPTER THREE

1. What immediate effects did the Internet shutdown have on the Libyan opposition's communications ability?
2. What kind of trust was required to maintain satellite phone and VSAT connectivity?
3. In what ways did access to two-way satellite Internet (VSATs) transform Misurata's strategic position? How might their situation have been different without access to the Internet?
4. In what ways was the Libyan opposition able to create a communications structure that could serve both military and civilian needs? Can you think of key areas that the opposition did not address?

CHAPTER FOUR

1. How did media coverage of social media expand and amplify the reach of actions in that realm?
2. In what ways does Mohammed Nabbous exemplify the ways in which individual Libyans were able to use the Internet to influence the international perception of the Uprising?
3. How did the Libyan opposition's use of YouTube evolve over the course of the conflict? What effect is this likely to have had on their credibility?
4. What does Ms. Clinch's story indicate about how the Internet can make global networks of support possible?
5. How did the pro-regime online activities and messaging on social media contrast with that of pro-opposition online activity?

CHAPTER FIVE

1. How did networks of support and trust expand the Libyan opposition's access to resources? Were these networks complemented by social media?
2. How did NATO publicly explain how it was using social media? What are some of the ways that this might have shaped how the Libyan opposition used social media? What were some of the risks to this kind of disclosure?
3. What are two ways that particularly struck or surprised you about how the opposition used common tools to communicate? What kinds of functionality do these tools have that might not be found in their military equivalents? What do they lack?

CHAPTER SIX

1. How did the Libyan opposition's forced switch to two-way satellite Internet and other connectivity impact the level of visibility that the LAJ had on Libyan network communications?
2. What strategies did the LAJ undertake to regain access to Libyan opposition communications?

3. The LAJ deployed PGEAs to hack the opposition's communications. What factors do you suspect contributed to their success in penetrating in some cases? What factors might have protected other opposition members?
4. PGEAs used inexpensive commercial malware designed for cybercrime and simple hacking techniques. Should these be considered "poor man's cyber weapons"? Why or why not?

CHAPTER SEVEN

1. After reading this case study, what is your perspective on whether commonly used online services are safe enough to provide the communications backbone to an opposition movement in a conflict?
2. What are the inherent operational security risks to using social networking? How were these risks amplified for the Libyan opposition?
3. Can you think of two measures that could have been taken by the Libyan opposition to increase their operational security, given their choice of communications tools?
4. Name several ways that an international actor, such as a NATO member state, could have assisted the Libyan opposition in increasing their operational security and mitigating the threat from PGEAs.

About the Author

John Scott-Railton is a senior researcher at the Citizen Lab, University of Toronto, focusing on technological threats to civil society. He co-founded the Voices Projects in 2012, which supported the free and open flow of information during Internet shutdowns in Egypt and Libya. Previously a fellow at Google Ideas and Alphabet, at the time of this writing Scott-Railton was a doctoral student at UCLA, and a Research Fellow at the Citizen Lab, University of Toronto.

www.usnwc.edu
www.usnwc.edu/ciwag

ISBN 978-1-935352-54-9