FOI

Social media and ICT during the Arab Spring

MIKAEL ERIKSSON, ULRIK FRANKE,
MAGDALENA GRANÅSEN, DAVID LINDAHL

FOI-R--3702--SE
ISSN 1650-1942 July 2013

Mikael Eriksson, Ulrik Franke, Magdalena Granåsen, David Lindahl

Social media and ICT during the Arab Spring

Bild/Cover: Wikimedia Commons, Sherif9282

Titel	Sociala medier och ICT under den arabiska våren
Title	Social media and ICT during the Arab Spring
Rapportnr/Report no	FOI-R--3702--SE
Månad/Month	Juli/July
Utgivningsår/Year	2013
Antal sidor/Pages	43 p
ISSN	1650-1942
Kund/Customer	
FoT område	
Forskningsområde	Informationssäkerhet och kommunikation
Projektnr/Project no	I35404
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Informations- och aerosystem

Sammanfattning

Under den så kallade arabiska våren använde aktivister i hög grad öppet tillgängliga tekniska hjälpmedel som Facebook för att organisera sig och bekämpa regimerna. Regimerna i sin tur försökte med olika metoder att begränsa aktivisternas möjlighet att kommunicera med varandra och med utländsk media. Rapporten tar upp exempel på olika incidenter och diskuterar hur tekniken användes i de olika fallen. Slutsats är att ICT (*Information and Communication Technologies*) i vissa fall fungerade som en kraftig kapacitetshöjande faktor men att den inte i sig orsakade händelseförloppet.

Nyckelord: Arabiska våren, internet, sociala medier, cyberkrig, distribuerade kommunikationssystem, övervakning, privatliv

Summary

During the so called Arab spring, activists made extensive use of openly available technical tools such as Facebook to organize and fight the regimes. The regimes in their turn took various actions to keep the activists from communicating with each other and with foreign media. This report gives examples of incidents and discusses how technology was used in various cases. The conclusion is that the use of ICT (Information and Communication Technologies) in some cases was a force multiplier for the opposition, but that it was not the cause of the uprisings.

Keywords: Arab Spring, Internet, Social media, cyber war, distributed Command and Control, Surveillance, Privacy

Preface

This report has been produced within the National Security in the Information Society (SPIS) project at FOI. This project studies the complex interplay between our modern information society and national security, an evolving field that has attracted considerable attention in the wake of the Arab spring.

The report has benefitted from the comments of Teodor Sommestad, who made valuable remarks as a reviewer.

Stockholm, June 2013
Ulrik Franke, SPIS project manager

Table of contents

1 Introduction

1.1 Aim and purpose

This study was conducted as part of the FOI project "National Security in the Information Society" (SPIS). SPIS is an internal competence-building project, intended to develop methods for studying the interplay between ICT and social and political events, as well as to explore the role and functions of modern ICTs in international relations. As such, this report is intended to document a part of a work in progress.

The aim of this report is to describe how different actors used Information and Communication Technologies (ICT) during the Arab Spring and to discuss the effects of ICT on the outcomes of the Arab spring. The rationale for this is the widely diverging opinions found on the importance of ICT during these events in the literature and in the public debate. Some claim that ICT was essential to the revolutions (hence the term "Twitter revolution"), others maintain that ICT played a much less prominent role. This report aims to shed some light on this issue by a literature review, by examining a number of ICT-related episodes during the revolutions, and by expert interviews, thus putting the differing opinions into perspective.

1.2 Scope and delimitations

The "Arab Spring" is a conceptual delineation of a series of social and political events across the Arab world starting in 2011. Scholars and participants of the Arab spring have different connotations of what these events actually entail as well as different opinions on when they started. While some experts suggest that the revolts were the culmination of prolonged underground opposition against incumbent regimes, others view the shift from covert social force to overt rebellion as virtually instantaneous.

Despite differences, most observers agree that each Arab state in the Middle East and North Africa exhibited a political dynamic of its own. Hence, it is more precise to refer to the events in Tunisia as the *Jasmine Revolution*, to the events in Egypt as *the 25 January revolt*, etc. [30]. Still, in this report, the main focus is on common traits such as the large popular participation and in particular the use of social media and ICT to mobilize support. In this respect, the term "Arab spring" is used as convenient and well-known shorthand for the common traits studied, not as a concept uncritically endorsed.

Furthermore, in this study we are primarily interested in the events at the outset of revolts, in particular the events during 2011.Wheras the Arab revolts affected

many states in the area, the focus of this study is Egypt, Libya, Tunisia and Syria. Apart from Yemen, these were the states perhaps most directly affected by the events [33].

It should be noted that the scope of this report is the role of ICT in the revolutions only. The time frame investigated excludes the use of ICT in the post-revolutionary setting, e.g. for e-government, polling, or democratic reforms in general. In these respects, each state had its own particular set of challenges, well out of scope for this report. See Jones [52] and Berman [13] for two competing views on how to understand the challenges facing the Arab revolts.

1.3 Method

First, a literature review was carried out. The aim was to get an understanding of the role and importance of ICT for opposition, protest and revolution, with a focus on the Arab spring. Research databases such as Thomson Reuters Web of Knowledge, Scopus, International Security & Counter Terrorism Reference Center, ProQuest, and Google Scholar where searched using queries such as "ICT Arab spring", "ICT social change" and "ICT democratization". The results were screened for relevance, and additional results were obtained by looking at articles citing or cited by the ones already found. The resulting body of literature is certainly not exhaustive, but it served as an important foundation for the rest of the study.

Second, two semi-structured interviews were conducted via Skype. The interview questions were spawned by the literature review, as well as by discussions within the National Security in the Information Society (SPIS) project team. The following areas were discussed with each of the informants:

- Social media and ICT-related events during the Arab Spring
- Attempts to monitor or regulate use of social media and ICT during these events
- Who used social media and ICT and for what purpose
    - Incumbent regimes
    - Opposition
    - International community
- The technical skills of different actors and their awareness about the opportunities and risks of using social media and ICT.
- The actual effects of social media and ICT on the outcomes of the Arab Spring

Informant 1 was Doctor Susan Alnaqshbandi of Tilburg University in the Netherlands. Her speciality is within security in computer networks and she has recently investigated the role of social media in the Egyptian revolution.

Informant 2 was Peter Fein, an Internet activist and "namefag" (i.e. media liaison) in *Anonymous*, who has worked with *Telecomix*, *Anonymous* and other networks to stop censorship and keep Internet access available in Iran, Syria, Egypt and other countries.

Third, the report was written as a synthesis between the literature review and the interviews. For clarity and accessibility, the exposition also includes background information on the events of the Arab spring, mainly re-used from previous work by one of the authors (cf. Eriksson [30] [31] [32] and Eriksson & Zetterlund [33]). As for the ICT incidents described, they have been chosen both from the literature and from examples given by the informants. Broadly, the following categories are represented:

- Well-known or famous blog posts, tweets etc., and actors with large bases of followers addressing discontent and protests.
- Bloggers and others being targeted by the incumbent regimes.
- Regime attacks, censorship, and disconnects on ICT services and infrastructure.
- Protective measures taken by activists or insurgents to counter regime attempts to diminish their use of ICT.
- Insurgent activities enabled by ICT and probably impossible without it

Collectively, these indicators are reasonable measures of the effects of ICT on the revolutions.[1]

1.4 Reading instructions

The report is organized in a straightforward manner. Chapter 2 gives an exposition of the existing literature, highlighting the controversies over the role of ICT in revolutions. Chapter 3 outlines events, social media use and ICT incidents by country, looking at Tunisia, Egypt, Libya and Syria respectively.

[1] For ease of exposition, the indicators have not been structured according to any taxonomy but have rather interwoven with the rest of the text. One possible taxonomy would be the generations of internet control, proposed by Deibert & Rohozinski [25], but being concerned exclusively with the internet, some important dimensions are missing. Another alternative would be the information operations taxonomy used by Franke [37], but its military NATO origins make it less suitable in the present setting.

Chapter 4 offers a synthesis of the literature review and the interviews, describing the actual effects of ICT.

The report serves several purposes. To an audience not familiar with the literature on ICT and social change, it contains a useful summary and further references to different scholarly perspectives. To those familiar with the Arab spring, but not with its ICT aspects, the report offers an accessible summary of important ICT incidents throughout the revolutions. To other scholars, the interviews and our conclusions offer a small additional contribution to the understanding of the field.

2 Related work

Since the events in late 2010 and early 2011, a lot has been written on the Arab spring in general and the role played by ICT in particular. The aim of this short literature review is not to exhaustively describe this field of scholarship, but to sketch some of the important arguments that have been brought forward for and against the importance of ICT, broadly construed, for protests, social change, and revolutions. This body of literature also includes work that predates the Arab spring, or relates to other parts of the world.

2.1 The importance of ICT for opposition, protests and revolutions

A key argument for the importance of ICT is that the Internet can offer a new media environment, free from censorship. This allows alternative messages to surface, demonstrations to be co-ordinated and online petitions to gain support. Ahmad et al. [5] for example advance this argument in the context of the (non-revolutionary) development in Malaysia. Abbott [2] agrees, based on studies of the elections in Malaysia 2008 and Singapore 2011. This line of argument is not new. In 1999, Dartnell [24] based on a case-study of the Peruvian MRTA, argued that the internet creates a new landscape that is hard to censor, that is not connected to a single physical location, and that can reach a receptive and anonymous public. This creates what he calls a *Verbindungnetzschaft*, a networked identity and organisation. Kilo [56] makes the more philosophical point, with reference to Syria, that the experience of freedom in the public space of the internet can foster a desire to experience freedom in the physical world as well. Alqudsi-Ghabra [7] argues that the speed and density of information created the preconditions for the revolutions in Tunisia, Egypt, and Libya. He also highlights the importance of redundancy to avoid censorship: if Facebook was censored, Twitter was used instead.

Chebib & Sohail [19] expand on this argument in the Egyptian context, claiming that the events in Egypt were affected in three ways:

1. Acceleration: information is disseminated faster
2. Social media became source material for news agencies
3. Coordination: Mubarak's eventually unsuccessful attempt to stop the revolution by shutting down the Internet signalled that he perceived the people as the enemy, making it counterproductive.

Abdelhay [3] makes a similar case, claiming that ICT had an "enormous impact" on societal and political changes in North Africa by challenging government media restrictions, enabling organization of protests, and encouraging media

coverage. The importance of media coverage is highlighted by Hamdy & Gomaa [43] who investigate the different framing of the Egyptian uprising in traditional media and social media. Whereas government newspapers promoted the image of a conspiracy against the state, social media largely framed the events as "a revolution for freedom and justice". Nanabhay & Farmanfarmaian [66] stress how social media triggered mainstream media, creating what they call an *amplified public sphere*. Hounshell [46] describes how journalists used Twitter as a source of real-time information, which was redistributed to the world audience. Gonzalez-Quijano [41] agrees that social and traditional media are best analyzed not one by one, but as a single "eco system". A 2011 article in the *Strategic Survey* journal entitled Strategic Policy Issues [79] agrees that the principal role of ICT in Tunisia and Egypt was to draw international attention, not to mobilize people to the streets.

Hussain & Howard [50] argue that ICT can build a networked community long before any revolutionary events. Such preparation allows small groups to coordinate much larger crowds whenever the active protests start, using ICT as one tool among many. ICT can also be used to spread news to the rest of the world. However, Hussain & Howard stress that ICT development cannot be assessed in a vacuum. It must be seen in relation to the systems of early warning, surveillance and countermeasures that are employed by the regime. With reference to the Arab spring, the authors note that Saudi Arabia, Bahrain and the United Arab Emirates – countries that were seemingly unaffected by upheavals – all had sophisticated such systems in place. Bryant [18] examines both regimes that survived and regimes that collapsed in the Arab spring, and argues that technology itself should be seen as neutral, capable of supporting revolutionaries and dictators alike.

Diamond [26] also explores the importance of the sophistication of countermeasures, contrasting Malaysia (no sophisticated internet control) with China (very sophisticated internet control). He concludes that though ICT help expose abuse of power or allow "smart mobs" to be coordinated by text messaging, there is an on-going race between democracies and autocrats, the outcome of which is still unknown. This could be contrasted with the more optimistic Alqudsi-Ghabra [7], who stresses that the creativity of the protesters largely allowed them to escape censorship.

Dunn [28] also highlights the importance of the cell phone in her study of the events in Egypt. She describes the interplay between activists and the regime, noting that the regime escalated from targeting contents to platforms (e.g. Twitter) to infrastructure (e.g. the national internet segment). Along with this escalation of measures, the risks to the regime (political, economic, and reputational) were also increased.

Diani [27] argues that ICT might have helped overcome some traditional problems for democracy movements in the Middle East and North Africa

(MENA) region, namely by bridging existing conflicts within the urban middle class. Furthermore, ICT can help in circumventing surveillance and repression, as long as it is not overly sophisticated. Diani concludes that it is reasonable to believe that ICT can facilitate the necessary coordination in an *ad hoc* coalition in a revolt, but less reasonable to believe that ICT can foster the kind of long-term civic virtues needed for democracy. Bellin [12] agrees that ICT played some role in bridging conflicts so that the "empirical novelty" of a huge, cross-class protest movement could emerge. Szajkowski [81] more enthusiastically argues that social media played a pivotal role not only in coordinating action, but also in synchronising beliefs.

Farrell [34] agrees with Diamond about the race between democracies and autocrats, but points out the possibility that ICT might have given a larger boost to activists than to state security forces, thus shifting the balance. He also describes the mechanism of "preference falsification", where citizens keep their actual opinions of the powers that be close to themselves, for fear of repercussions. However, ICT has the potential to rapidly change this state of affairs, if it offers an anonymous arena free from such repercussions. This goes some way towards explaining why it can be so important for repressive regimes to maintain the impression that foreign interests are behind protests and unrest: if preference falsification dwindles, everyone can very suddenly discover that everyone else indeed dislikes the regime. Farrell also points to lower transaction costs as an important mechanism by which ICT can impact politics. Spier [77] further elaborates on how ICT could be fitted within existing sociological theories on collective action.

Expanding the issue of mechanisms, Howard et al. [48] identify three possibilities opened to activists by ICT: (i) building networks with each other, (ii) create social capital and (iii) organise political activism in several ways:

1. The Tunisian blogosphere made dialog on political change possible
2. Twitter distributed information to foreign journalists, facilitating cross-border news dissemination
3. Facebook was a central node of discontent in Egypt
4. YouTube made possible news distribution and citizen journalism, spreading news that otherwise would have remained unknown

Kyriakopoulou [57] delineates three steps of how ICT becomes important for the opposition in authoritarian states:

1. Censorship, surveillance and general discontent makes ICT an important tool to access information.
2. People come together in online social forums for deliberation, creating social capital.

3. What happens online becomes even more important as it contributes to an extended, global, public sphere, where information about the conditions in a particular authoritarian state can be spread to the rest of the world. This also allows discussion between democracy activists on location and in the diaspora.

The use of social networks to spread information, both internally and externally is highlighted by Mansour [62].

2.2 Scepticism about the importance of ICT

A simple argument against the importance of ICT is that it is communication and information that matters, not means of propagation. Anderson [9] makes this point, noting that in 2011 Facebook delivered the instigating messages, in 1919 print newspapers did. Alterman [8] argues that online social networks were not a major factor in causing the protests of the Arab spring. Dartnell [24] points out the historical parallels, citing post-revolutionary France in 1789 as an example of a utopian belief in the ability of the printed word and the newspaper to foster a well working (direct) democracy. Then came Napoleon, who renewed censorship and established a government monopoly on the printing press. Diamond [26] agrees, observing that while the printing press did play an important role for the reformation, the renaissance, and the scientific revolution, it also helped create the modern state and its censorship. Kazamias [54] observes that it is far too easy to attribute events to the latest technology: the fall of the Soviet empire to the T-shirt, the anti-globalization movement to text messaging, or the Arab spring to Facebook. Ironically, Kazamias observes, those who took this line of reasoning the most serious were the leaders of the Egyptian police state, who decided to shut down the internet. However, Hassanpour [45] claims that the actual causes of revolutions are disinformation and rumours, not technology. Therefore, he argues, the decision to shut down the internet might have actually *triggered* the revolution. Less connectivity, maintains Hassanpour, fosters the rumours of person-to-person communication necessary for revolt.

Olorunnisola & Martin [68] argue that the media reports on the Arab spring are coloured by oversimplifications and technological determinism. Claims about Facebook and Twitter having caused or hosted protests are made without proper sources. Olorunnisola & Martin call for a more nuanced discussion: there is no scientific consensus, but scholars do agree that activities on and offline can interact with and reinforce each other. Cottle [22] argues along similar lines, claiming that while labels such as “Twitter revolution” do less than justice to the complexities, new media and ICT certainly did play a role. Hassan [44] also adheres to this position, noting that though Twitter and Facebook did play a role in mobilizing people during the Arab spring, this role has been exaggerated in western media. Gonzalez-Quijano [41] points to the different political, economic,

and social circumstances of the different countries, stressing the interplay of social and traditional media.

Saleh [74] points out that too simple conceptual models of the interaction between ICT and society can be misleading. The popular dictator's dilemma model; "allow internet and risk being overthrown, or forbid it and risk economic stagnation", is an oversimplification, claims Saleh, which makes it harder for researchers to see what actually happens on the ground.

Morozov [64] has famously coined the term "slacktivism" meaning that online activism does not necessarily translate into offline activism, and might indeed serve as a substitute for it, thus decreasing rather than increasing actual effects. Allowing citizens to "let off steam" online but not allowing any spill-over into the physical world has been described as a strategy of the Kremlin in Russia [60]. However, recent research finds a close relation between pro-social behavior online and offline [17], suggesting that the slacktivism effect might be exaggerated.

Comunello & Anzera [21], similar to us, perceive two opposing groups of scholars: the *digital evangelists* who emphasize the revolutionary role of social media, and the *techno-realists* who minimize that same role. Their own assessment is more nuanced, claiming that empirical research so far has not provided results that unequivocally support either side. Indeed, when the complexities of the interplay of society, technology and political systems are taken into account, neither side is likely to be right.

3 The Arab Revolts

In a sense, the popular revolts in the Arab world are still on-going in mid- 2013. However, unlike the initial – and often spontaneous – popular protests, the revolts have now taken different political turns. A number of Arab states have now entered into a post-authoritarian process (e.g. Tunisia, Egypt, and Libya); others have initiated a reform track (Morocco, Algeria, Yemen, Jordan, etc.). In some cases the calls for civil liberties have met only brute force responses (e.g. Saudi Arabia, Bahrain, etc.). Syria is painfully engaged in a civil war, reminding us on the complexity of social upheaval. Each state is now engulfed in its own particular set of challenges. The following outlines the events and ICT-related incidents of the initial revolutionary upheavals.

3.1 Tunisia

This introductory section is based on the corresponding section in Eriksson & Zetterlund [33], slightly updated.

The events in Tunisia in late 2010 triggered the Arab revolts that subsequently spread across North Africa and the Middle East [51] [50] [35]. Today, Tunisia may be considered the country that has undertaken the most profound democratic reforms [73]. The process of social and political change is still on-going but has suffered a number of complex political challenges considered democratic set-backs by experts [30]. The government has been criticized for both lack of democratic aspiration and lack of governing experience.

Shortly after the ousting of President Ben Ali (January 14th, 2011), the opposition began a process of rooting out representatives of the former political, economic, military and police elites. The central idea was to rid the state of former Ben Ali loyalists to ensure that democratic practices and governance were given a fighting chance in the new government. In retrospect, however, the political purge of former Ben Ali loyalists had unwanted repercussions on the political reform process. One such an important implication was that several Ben Ali party affiliates did not participate in the elections to the Constituent Assembly on October 23rd, 2011. This paved the way for the *Enahda*, an Islamist political party, to become the largest party in the new assembly [31]. Furthermore, the purge of former regime loyalists might have left the new government without crucial political skill and experience required to rule the country. The incumbent government has been criticised by the opposition for lacking the required skills to govern. Indeed, by mid-2013 opposition to Tunisia's first democratically elected government is growing. Demonstrations are repeatedly held, some organised using social media in the same fashion as during the anti- Ben Ali revolt. However, the political context is different. Whereas the opposition in the final hours of Ben Ali's rule was much about beating the state (i.e. the government,

the police, the intelligence system, etc.); the wall of fear has now been overcome and government reactions to protests are now within democratic control. This is not to say, however, that there are not instances of grave human rights abuses, see e.g. Amnesty International [1].

In defence of the incumbent government, one might also note that the social and political challenges of reconstituting the state following years of authoritarian rule are immense. Power-struggles have been endemic for the past three years. There are also considerable social and political challenges to the democratic project posed by religious factions and political parties such as Salafi groups and moderate groups such al-Nahda [55].

3.1.1 Examples of ICT use

During the reign of president Zine El Abidine Ben Ali opposition was suppressed and censorship was widespread in both traditional and digital media. Periodically access to user-content sites such as YouTube, Flickr, and some blog-services was blocked. Garbia described how accounts belonging to bloggers critical of the government were hacked, and content deleted [39].

In addition, bloggers and activists using ICT were contacted through telephone or in person and threatened in various ways in order to silence them. Openly criticising the government could lead to prison sentences of several years as well as torture.

3.1.2 Wikileaks and social media

In November 2010 Wikileaks published a large number of telegrams from the United States diplomatic service sent from various embassies around the world. Among them were several from Tunisia. These telegrams revealed a number of facts about the regime that angered the Tunisian public [42].

This leak, coming as it did shortly before the immolation of Mohamed Bouazizi on December 17 have been pointed to by some as a contributing factor to the size and fervour of the protests that followed [10]. An indication that this might be correct is that the online activity increased dramatically in just a few weeks following the leak, with several hundreds of thousands of Tunisians creating accounts on Facebook alone [61]. These new accounts, as well as older ones, was used to share information in near real time about events as they unfolded combined with pictures and video that was censored in the government media.

It should be noted, however, that these are activities that had been used for years before the Arab Spring. Even during the oppression bloggers and vloggers (i.e. video bloggers, e.g. on YouTube) had shared information about oppression, and communicated with foreign human rights activists over the Internet. What happened at this time was that as widespread rioting and protests took place these

bloggers and vloggers published accounts of the events. This meant that new content was produced in real time, covering the events as they unfolded, bypassing the governments´ censorship. The producers in turn encouraged others to join in, both in creating media and in protesting, so as the number of demonstrators grew, the number of media producers and bloggers spreading the word grew too.

3.1.3 User defence

In order to defend themselves from harassment and arrest, some users had taken technical precautions when using the Internet. One of these technical precautions is TOR. TOR, short for *the onion router*, is a tool that can be used to keep from being tracked when on the Internet. A bit simplified, it shuffles the users' traffic in an obscure and encrypted manner between volunteer computers before it sends it to the destination. Ideally this means that although the government can trace the communication between the user and the first node in the TOR-net, it cannot find out to what other computer the user's computer is communicating with.

The usage of Tor rose dramatically from November 2010 with 20-50 users to nearly 700 users in middle January [83]. This may seem to be a great step forward for the anonymity online. However, compared to the total number of Internet users in Tunisia, 3.6 million in 2010, it is obvious that only a small minority used TOR to obscure their communication.

This is an example of something that the authors of this report see repeating itself time and time again. The vast majority of users could, with relative ease protect themselves from at least several types of surveillance, but are ignorant of the need, the solutions, and unskilled in implementing them.

When interviewed for this report, Fein lamented this fact [36]. He mentioned this as one of the greatest obstacles to assisting freedom activists.

3.1.4 Government attack

In early 2011 Facebook pages and blogs of prominent critics was hijacked by government agents who logged in and changed the passwords [73].

There does not appear to have been any attempts at using the hijacked accounts to broadcast propaganda, and some bloggers even managed to convince Facebook and Google to reset their passwords, and could then get access to their content and resume their activities. Others found their content deleted. What differed from earlier hijackings of this sort was the numbers of account affected and the speed of which the accounts were hijacked.

According to Ryan [73] the operation started on the eighth of January[2] when the Tunisian Internet Agency, TIA, blocked the HTTP protocol[3]. This protocol is used to keep user name and passwords secret when using sites such as Google and Facebook.

As a result of this blockage, everyone trying to use these sites got a warning that https could not be used. But the consequence of this was not clear to the vast majority of users. Those who accepted the HTTP-connection were exposed to a password-sniffing attack. The Tunisian government, more specifically the ATI, controlled the national infrastructure, and with it all access points between Tunisia and the international Internet. This meant that they could monitor all traffic on the networks, including that going to and from international sites.

The attack itself was done through intercepting the traffic sent from the website, and changing the return address so that login information the user sent went to a non-existent Internet address. Traffic to this fake address was captured by the TIA and the data harvested. The user meanwhile having entered his password got a response back from the site saying that the page was not found.

The TIA then used the login information to access the Facebook accounts of users deemed to be important from an influence point of view, and deleted their data, silencing them. Also, the TIA could access all the information the users had uploaded, and could see who was talking with whom, and in that way gain valuable intelligence about the activists' networks and social circles.

This type of attack is commonly known as a man-in-the-middle-attack, for obvious reasons.

If the users had been suspicious and informed they would not have used an Internet connection without HTTPS, but that would only have helped them from getting their accounts hacked. They would still not have been able to access the services they wanted. In a situation when an oppressive government has total control of the infrastructure, it is very difficult for a user to defend against abuse.

---

[2] According to Madrigal [61][61][61] the attack started as early as December 25th 2010. It is the authors' experience that this kind of discrepancies between versions of events is typical of IT-incidents during the Arab Spring. Different actors come to different conclusions depending on their own experiences, and hard facts are hard to come by.

[3] A protocol in this context is an agreed upon message format that computers use to communicate. More specifically, HTTPS is a protocol extension of the common web-surfing protocol, HTTP. The added S means *secure*, and indicates that the communication is encrypted.

3.1.5 Countermeasures by the international community

Within a short time after the attack started a security update was manufactured and distributed over the Internet. It consisted of a small program which, when added to the browser, simply deleted the TIA attack code from the incoming web page before the browser could be fooled. It was also written in such a way that it would automatically update itself to counter any new attack code the TIA might later insert.

The problem with this solution was that most users are not capable to download and run an update script. This tends to be a recurring problem when users try to defend themselves against surveillance. The main body of users are interacting with ICT in a black-box-manner. That is, they have no intrinsic understanding of how the technology actually works. This in turn means that they really have no sound way in which to determine what is safe to do, or how to use security measures in a proper way.

And even if they are told what to do, the details of, for example, how to modify the behaviour of a web browser is something they have no skills for. The reason of course is that under normal circumstances the ICT is used in the manner it is designed for, and the users have no need to alter it.

3.2 Egypt

This introductory section is based on the corresponding section in Eriksson & Zetterlund [33], slightly updated.

Similar to the initial protest movements in Tunisia, the anti-Mubarak opposition initially consisted of a broad base of citizens from different classes and interests, united by the demand for regime change and the urge for democracy. Following 18 days of demonstrations, President Hosni Mubarak left office on February 11th, 2011.

The initial democratisation process proceeded smoothly, not least with the election for the National Assembly (held on November 28th, 211). However, as feared by secular and liberal parties at the time, the well-organised Islamist parties (i.e. the Freedom and Justice Party and the more conservative Islamist party *al-Nour*) did well and ended up as the foremost winners, mainly due to the underground local presence across Egypt they had built throughout the reign of Mubarak. This presence, in place and ready, gave Islamists a head start following the downfall of the regime. Unsurprisingly, political Islamists also won the presidential elections held on 16–17th June 2012, when the Muslim Brotherhood's (MB) informal candidate, Mohammed Morsi, was elected President of Egypt.

3.2.1 Examples of ICT use

An increasing number of studies have recently been published describing the Revolt in Egypt from the point of view of social media (cf. e.g. Bashir [11]). Before and during the Egyptian revolution, social media and ICT played a crucial role in encouraging people to protest, spreading hope, organising the protests and informing the world outside Egypt know about what was happening [15]. A frequently quoted tweet by an Egyptian activist during the protests says that "we use Facebook to schedule the protests, Twitter to coordinate and YouTube to tell the world" [49]. Bhuiyan [15] claims that the government initially underestimated the power of social media, however in order to prevent interaction with other nations and perhaps in an attempt to stop the protests, the government blocked ICT.

3.2.2 Whael Ghonim

Whael Ghonim, the Middle East marketing director for Google, believed in Facebook as a revolutionary tool. Combining his technical and marketing skills, he became Egypt´s most important cyber activist [40]. Besides his ordinary work at Google, he ran the Facebook fan page of Mohamed ElBaradei, who was the main opposition leader before the revolution.

In June 2010, the young blogger Khaled Said was beaten and killed by the police as a consequence of posting a video of police officers engaged in illegal activities [78]. Shortly thereafter, Whael Ghonim started the Facebook page "We are all Khaled Said" in reaction to the murder and to police brutality, justified by the Emergency Law which allows the police to arrest people without charge [82]. On the Facebook page, Whael posted pictures of the corpse of Khaled Said, as evidence that the death was caused by the beating and not drug abuse, as was claimed by the authorities. The Facebook page became immensely popular, attracting 500 000 members [78].

Inspired by the Tunisian protests during the 14th of January, Ghonim set up a Facebook event, inviting the Facebook page members to participate in a protest on January 25th. Over three days, more than 50 000 members responded that they would attend the event [40].

3.2.3 Asmaa Mahfouz

Another blogger is Asmaa Mahfouz, activist and one of the founders of the April 6 Youth Movement, an Egyptian activist group established in Spring 2008 to support striking workers in El-Mahalla El-Kubra, an industrial town. This movement used social media and ICT to rally support for the strikers. It later grew to tens of thousands of active members using Facebook and other online

tools to champion human rights causes and criticizing nepotism, corruption and censorship in Egypt.

She later used her influence to rally people to the "Day of Rage" proposed by Ghonim.

3.2.4 Twitter down, Facebook follows

Twitter is a social messaging service where anyone with an account can make short comments which are tagged with subject headers preceded by a hash tag (#). For example, a comment can be "Rally at Tahir Square tomorrow noon! Protest! #Tahirsquare #Arabspring "

Users can subscribe to subject headers, but also to specific accounts. This enables users to follow everything written about an interesting subject, and everything written by an interesting person. The most influential Twitters have followings in the tens of millions all over the world.

On January 25th of, the SSI[4] ordered Twitter to be blocked which meant that not traffic to or from the Twitter servers were sent over the Egyptian Internet. The next day, Facebook was blocked. Apparently this did not have the desired effect, so on January 27th almost the entire Internet of Egypt was shut down.

According to BGPMon [14] the shutdown was gradual; one Internet Service Provider (ISP) after another was shut down with intervals of about ten minutes. This indicates that although the SSI has control over the Internet exchange points where the oceanic cables connect with Egyptian ISPs, they called the ISP: s and ordered them to shut down rather than to shut down the exchange point. Freedom House [75] on the other hand claims that the Internet Exchange in Ramses street Cairo was indeed shut down.

The result was that as of evening the 27th of January, only a very small minority of Egyptians had access to Internet or SMS text messaging.

3.2.5 International response

Activists abroad were already organized since the events in Tunisia, and acted quickly. Knowing that a large part of Egyptian Internet users had dial-up Internet, activists convinced ISPs in France, Sweden, the Netherlands and others countries to power up old modem banks no longer in use. These enabled Egyptians to dial abroad and connect to Internet, in some cases for free.

[4] Egypt's State Security Investigations Service (SSI), the national internal security agency.

Other services set up to facilitate the flow of information included activists manning phones, taking messages and sending them on to addressees in email- or twitter-format. Some even manned HAM-radio sets to transcribe messages from those in Egypt out of cell phone range.

Several companies supported the revolution. Some Telecom operators donated free calls to the modem banks, and on the 30th of January, Google activated the Speak2Tweet-service. This enabled Egyptians to place an ordinary phone call to a certain number, leave a message on an answering machine. The machine then tweeted the message with the tag #Egypt. It was also possible for a user to call the number and listen to the voicetweets.

The combination of the blackout not being very effective, and the scathing criticism from the international community led to the Internet being restored on February 2nd.

3.3 Libya

This introductory section is based on the corresponding section in Eriksson & Zetterlund [33], slightly updated.

Just like in Tunisia and Egypt, anti-Gaddafi street protests soon grew into formation of National Transitional Council (NTC) bidding to overthrow the incumbent regime in Libya. The initial demonstrations started on February 15th 2011 [29].

A turning point for opposition forces was the decision on March 17th 2011 by the United Nations Security Council to adopt resolution 1973 (2011), which called on UN member states to take all necessary measures to protect Libyan civilians, including the establishment of a no-fly zone and an arms embargo[84].

During the course of the spring, the rebels tried to establish themselves as a democratic alternative to the government in Tripoli. The military campaign eventually resulted in the conquest of Tripoli in late August and the killing of Libyan leader Muammar Gaddafi on 20th of October 2011[58] [59].

3.3.1 Examples of ICT use

Before the revolution, the government of Libya had relatively little censorship of the Internet, relying instead on surveillance and threats of arrest to induce self-censorship to keep its political opposition in line.

However, the degree of surveillance was far greater than most of its inhabitants realized. Most of the users of Internet cafés had noticed overt surveillance in the form of security service personnel, and laws that required users to show identity credentials and reveal their cell phone number in order to get service. But Libya

had also a number of secret surveillance systems, supplied by private companies. Thales, Amesys, ZTE, among others.

These systems gave the regime information about almost everything done online, such as emails, web browsing, voice over Internet, and so on [76].

3.3.2 Day of Anger

In a Facebook post on January 28th, Libyans are encouraged to protest in a "Day of Anger" on February 17th. Over the following weeks the number of supporters grew to the point where the regime felt compelled to act. On February 13th the Libyan Dictator Muammar Gaddafi made a public statement where he warned against the use of Facebook. On the same day, several Internet activists were arrested. The result was not what the regime had hoped. On February 15th and 16th large protests take place in Libya and on the 17 had spread throughout Libya.

3.3.3 Information disruption

On February 17 Al Jazeera announced that its programs have been removed from the state television networks in Libya. On February 18 the Libyan Internet was taken down for nearly seven hours. On the following day it was taken down again, for a little over eight hours. During these two days the regime also used electronic warfare technology to disrupt communication with the Nilesat and Arabsat communications satellites.

Al Jazeera accused the regime of using electronic warfare to jam its transmissions during February 21st-25th, claiming that the source of the jamming was a government facility outside Tripoli. Thuraya Communications claimed that they too had their satellites jammed intermittently for a week.

3.3.4 Armed uprising

When the uprising began, and in the early stages of what was to become a civil war, the rebels used the available communications technology. They used cell phones for tactical battlefield communication, Facebook and Skype for planning and logistics, Twitter for propaganda and information and so on. Although most of this communication was unencrypted and insecure, the immediate need overrode any security concerns [76].

3.3.5 Blackout

On March 3rd almost all Internet service throughout Libya went down. Many phone systems suffered disruptions, and communication from Tripoli to East Libya was cut off entirely.

Internet observers noticed that Libya had chosen a different tactic than Egypt did. There was traffic to and from Libya. It would seem that instead of shutting down the infrastructure, the Libyans had closed firewalls leaving only a few government facilities with access to the outside world.

3.3.6 Ad Astra

A peculiar feature of the Libyan communications grid is the prevalence of satellite communication. Since large areas of Libya are unpopulated desert, oil fields, and remote towns satellite communication is widely used alongside local cell phone networks. This meant that when the blackout happened, large numbers of satellite terminals were available in store facilities, at vendors, etc. Very quickly, these were put to use to contact the outside world as well as to communicate between the rebel groups of what was now an armed rebellion.

Even though the Gaddafi Regime tried to jam satellites, they were largely unsuccessful. The final result of the Internet blackout was that the rebels, forced to ad hoc solutions could maintain an adequate amount of communication. The government surveillance organisations on the other hand that relied on Internet surveillance lost all capability to monitor the rebel activity.

3.3.7 Opposition nominating targets to NATO

During the Libyan Revolution, rebels in the city of Misrata wanted to encourage NATO to intensify airstrikes on certain targets. Using Google Earth, rebels marked the positions of potential targets. A screenshot of the map and target location was e-mailed to groups outside Libya that were in contact with NATO. The Gaddafi regime reacted to the initiative by hijacking opponents' e-mail accounts through sending e-mails with attached files containing remote-access Trojans [76].

3.4 Syria

This introductory section is based on the corresponding section in Eriksson & Zetterlund [33], slightly updated.

Syria is one of the states in the Arab world where the transformation from authoritarianism to democracy faced the toughest resistance. Syria also poses a special case in the sense that it is geographically located in a strategically

sensitive place, with neighbouring states such as Israel, Iran, Turkey and Jordan. The mere combination of size of the country, the interests of external actors (e.g. US, UK, France and Russia), the ethnic mix, and the strong position of al-Assad and his Baath party made the conditions for a successful revolution in Syria very difficult.

The protesters' initial demands from activists were mostly about human rights, social justice, government accountability and an end to the martial law in effect since 1963. There were also specific demands for the government to step down from power and for the ousting of key political and economic figures. The government responded to these demands with promises of reform, trying to convince activists as well as foreign diplomats that it was prepared to listen. However, as the gravity of the opposition increased in early 2011, the government in Damascus was increasingly challenged by the domestic street protests.

Turning increasingly violent, the opposition gained increasing control of the countryside of Syria. Still, the military initially remained intact and in firm control over the country though the number of political defections increased by the month.

A problem for the opposition has been its inability to unite in a single chain of command. Instead, it splintered into a number of opposition parties and self-defence councils. For example, some of Syria's opposition forces united in August 2011 under the auspices of the Syrian National Council (SNC). The Council was set up inter alia after several meetings in Turkey. While the SNC represents a vast number of opposition forces, it is a far cry from representing all opposition groups inside and outside Syria. Nevertheless, the EU on October 10th 2011 welcomed the formation of the SNC as a prominent actor.

As the situation on ground deteriorated, a number of diplomatic actions were taken to tackle the increasingly violent situation in Syria. For example in March 2012, former UN Secretary-General Kofi Annan, appointed as the joint UN and Arab League envoy to Syria, met with President al-Assad to propose a cease-fire which included the withdrawal of government troops from Syrian towns and villages. By this time nearly 10,000 citizens had been killed since the start of the uprising. The first international observers landed in Syria on April 15th as part of a team of international observers tasked with overseeing Syria's fragile ceasefire that took effect on the April 12th. However, neither side complied with the Annan proposal nor did the incumbent government make it possible for the observers to do their job.

Having initially been a mass rally against the regime, the character of anti-Assad opposition turned increasingly ethnic and sectarian. Anecdotal evidence suggested early on in the conflict that there was an influx of foreign fighters into

Syria (some backed by foreign governments like Iran, e.g. al-Quds soldiers), some carrying a radical Islamist agenda (e.g. Jihadists coming from Iraq).

With al-Assad showing no signs of backing down from power, the uprising finally made it to Damascus in mid-2012. Until this time the armed revolt had mainly been carried out in the periphery (country side), but had over the months steadily moved towards Damascus. Despite the severity of the conflict, al-Assad did not officially declare that Syria was "at war" until June 26th, 2012. Meanwhile, the Arab League urged al-Assad to step down.

Following a political and military deadlock between the government and the various opposition forces, Kofi Annan resigned as the UN-Arab League's special envoy, and was succeeded by Lakhdar Brahimi. Following a Security Council meeting in late September, Brahimi summarized the situation in Syria as posing a clear threat to international peace and security.

Regarding the dynamics on ground in Syria, foreign governments have sought different means to support opposition. For example, the US has actively been engaged in supporting rebels by providing them with equipment for "non-lethal" purposes (e.g. communications gear).

Reports of a deteriorating humanitarian situation in Syria kept the international community's attention on Syria. Not only did the situation deteriorate inside Syria (Human Rights Watch reports that opposition forces are committing war crimes, including extrajudicial executions, torture, and ill-treatment of detainees) but also in the whole region. UNHCR predicted that nearly 700,000 Syrian refugees would have fled to neighbouring countries by the end of 2012, with two or three-thousand more crossing each day. The worsening situation in the early fall of 2012 prompted a number of Western and Gulf countries to consider increasing their backing of the Syrian opposition. For example, in late September 2012 a senior US State Department official says the US will send more aid to the Syrian opposition to help them "protect and defend themselves," while promising that the support will not include weapons or ammunition. Looming in the background was the issue of how to properly interpret the UN backed idea of protecting civilians, a question further fuelled by the controversies over the interpretation of the UN Security Council resolutions 1970 and 1973 on Libya. At the EU level, the issue of imposing telecom sanctions on Syria was placed on the agenda but was met resistance by Sweden, arguing that such sanction would mainly weaken the opposing forces.

In 2012, the violence in Syria also increasingly lead to spill-over effects, thereby dragging countries such as Turkey, Israel, Jordan, Iran and Lebanon into direct action (whether military or political). For example, in the early autumn of 2012, the border between Turkey and Syria was increasingly affected by the instability inside Syria. Following cross-border shelling from Syria, Turkey's parliament authorized military operations against Syria if its army shelled targets inside

Turkey. Moreover, news sources claimed that Israeli jets had attacked a military research centre near Damascus. Unverified reports also speak of Iranian efforts to smuggle weapons of mass destruction into Lebanon being targeted by Israel. Furthermore, the Israeli Defence Forces redeployed the Iron Dome system to the border with Syria.

The conflict in Syria also took a new turn in the later of half of 2012 when several major opposition forces including the Syrian National Council united as the *National Coalition for Syrian Revolutionary and Opposition Forces* at a meeting in Qatar. The new opposition body was immediate recognized by the Arab League. In December 2012, the US joined countries such as Britain, France, Turkey, Spain and a number of Gulf States in formally recognizing Syria's opposition National Coalition as "the legitimate representative" of the Syrian people.

In June 2013, the US reported that it now has evidence that the Assad regime has used chemical weapons, and that as a consequence, US support to the rebels will be increased and probably include weapons and ammunition [71].

3.4.1 Examples of ICT use

The Syrian Internet had been heavily censored since long before the uprisings. Syria has been on Reporters without borders' "List of Internet enemies" continuously since 2006 when it was first established [70].

In addition to censoring a large range of websites, the regime has promoted self-censorship through vaguely worded laws such as Decree number six, "publishing news aimed at shaking the people's confidence in the revolution" [69].

According to Fein the perception in Syria was that the government did not really care about apolitical downloaders [36]. That is, as long as the users only downloaded material from the Internet there was little risk of getting harassed or arrested.

The combination of online surveillance, censorship and physical threat to dissidents and activists led to Syria being named the third worst country to be a blogger in by the Committee to Protect Journalists in their Special report 2009 [20].

3.4.2 Increasing freedom

Interestingly, during the first months of the Arab spring Syria relaxed its restrictions and allowed access to YouTube and Facebook on the 8th of February 2011. This was interpreted by some as a statement of confidence that Syria would not be affected by the disturbances in neighbouring countries. Others pointed out that because of the relatively lax enforcement of the laws when the

users restricted themselves to downloading, many people already accessed these sites through proxies and anonymizers. What the government did was to let them continue, but in a way that let the regime monitor their activities.

3.4.3 Internet Shutdown

On June 3rd, STE (Syrian Telecom) shut down the Syrian Internet in response to the protests. This shutdown was not total. According to Cowie [23] roughly one third of Syrian networks remained online, among them all the government networks. Among the networks shut down was the entire Syrian 3G mobile data network.

Later on STE has shut down all communication, in November 2012 and in May 2013.

3.4.4 *Telecomix* and *Anonymous*

According to Fein the opposition in Syria did not want to use modems to call outside the country in the manner the Egyptians had done [36]. This was because the government controlled all telecommunications exit points of from Syria, both landlines and cell networks.

Instead the activist collective *Telecomix* scanned the hosts in Syria and found a number of government sites that had been improperly set up. Specifically, they had a file sharing service turned on without password. By connecting to these servers activists could upload data to them, which the *Telecomix* activists could then access from outside Syria and relay to the regular media, or publish on social media.

4 Effects of social media and ICT on the Arab Spring

"Social media played a great role in the outcome of the Arab spring, but not only social media: All digital technology. Internet for information gathering, the social media for connecting people [and] instant global reporting. It is also a fact that [ICT] played a significant role in Egypt and in Tunisia, but not a great role in Syria and Libya." Susan Alnaqshbandi [6]

4.1 How does ICT differ from other media?

ICT has changed the world in many ways. What is now commonly known as Web 1.0 made it easier for everyone to become a producer of information. Individuals, organizations and companies could create websites and reach a mass audience, previously only available using expensive printing presses or broadcasting equipment for radio and television. However, communication was still mainly one-way: from producer to consumer.

With the advent of *user-generated contents*, this changed [53]. Blogs, RSS-feeds, wikis, tags, and mashups making it all come together seamlessly changed the internet into a medium of two-way communication, Web 2.0 [65]. Today, users can record events as they unfold, and upload them to a video stream in real time. From that moment, other end users can save, copy, and redistribute the message. A user who hears about the message can search for it and find it archived later. In this way, users collectively produce, consume and disseminate content in a truly distributed manner. These are the building blocks of Dartnell's *Verbindungnetzschaft* [24] and the *amplified public sphere* of Nanabhay & Farmanfarmaian [66].

However, the internet is built to accommodate reliability, billing, low cost, speed of delivery, and ease of use, not anonymity or confidentiality. Internet service providers keep track of addresses and traffic, wireless devices can be tracked by their radio communications, and anyone using a cell phone is carrying a potential positioning and eavesdropping device. These circumstances are cornerstones in the surveillance and censorship systems used by oppressive regimes [18] [26].

4.2 Common factors

Although there are many differences between the countries affected by the Arab spring, certain aspects of the ICT use are common for all the countries. These common factors are discussed below.

Activist individuals and activist organisations were early adopters of ICT [36]. This is reminiscent of Farrell's argument that ICT might have given a larger boost to activists than to state security forces [36]. The dissidents had used ICT for years, some for decades, to inform, expose and organise against the regimes [36]. The importance of this preparatory phase has also been stressed by Hussain & Howard [50].

The ICT communities are not leaderless. Some bloggers and activists have significantly more clout than others. However, the ICT communities are not *dependent* on single leaders. When the regimes arrested one or more bloggers, their followers did not stop seeking out information, they simply shifted to other sources [36]. Alqudsi-Ghabra has also emphasized this redundancy [7]. Sometimes followers, outraged by what had happened to the blogger they followed, became activists themselves. Hassanpour [45] takes this argument to the largest possible scale, claiming that Mubarak's decision to shut down the internet might have *triggered* the revolution.

Most of the regimes were clearly hampered in their attempts to stifle ICT by the fact that they themselves were dependent on the same infrastructure [36]. There was also a significant economic cost – Howard et al. estimate that Mubarak's interruption of digital services cost Egypt's economy at least $90 million [47]. Even at the peak of censorship, as when Egypt shut down Internet, the phone networks remained up and running [36]. Furthermore, Roberts et al. have argued that the ease of shutting down the internet depends on the complexity of the supporting infrastructures [72], though Egypt is not very complex by their measure.

The online communities react with tremendous speed. Unhampered by bureaucracy or traditional hierarchies, individuals start to act as soon as they perceive something being wrong [36]. Others join in, and very soon different solutions are tested, rejected, modified and adopted. This dynamic has some similarities to information quality work in a community-based encyclopaedia such as Wikipedia [80] or bug-fixing in open source software projects [16] [4].

The same speed of adaptation applies to technology. If one type of technology becomes unavailable, migration to other means of communication takes place within hours or days [36]. Alqudsi-Ghabra has also emphasized this redundancy [7]. Often older, less powerful technology is used to bridge gaps between modern technologies, for example voicemail transcribed into text and published on the Internet.

4.3 Activist use of ICT

As mentioned before, various groups and individuals had been using ICT before the protests began, mainly for information dissemination, but also simply to build

social capital [48] [57]. This continued in much the same way during the uprising.

Based on the literature and interviews, two force multipliers available to the revolutionaries seem particularly important: *broadcasting* and *speed of communication* [36] [6].

The broadcasting made it possible for everyone to participate as soon as certain information had been spread, for example the twitter tag #Jan25. This reduces transaction costs: instead of having to meet and communicate with hundreds of people, a single person could potentially communicate with the entire population [36]. Furthermore, the use of broadcasting to reach traditional media, particularly abroad, was important [43] [46] [41] [79]. Individuals within the network contacted foreign media, who broadcasted their information and content over TV and radio, reaching not only foreigners, but parts of the domestic population not connected to the network [6].

As for speed, this communication is practically immediate [7] [19]. A single person seeing security forces approaching can alert thousands of people within seconds [36].

To avoid government surveillance and countermeasures, *information security* is a key concern. There are many methods that could in principle be employed by the users, but they are mostly unknown to activists, and difficult to use properly without training and assistance. This holds true despite well-meaning "How-to"-documents published on the internet. A key observation is that activists do not have any training in basic operational security, the way for instance military personnel does. This includes holistic reasoning about security, such as understanding that encrypted communication does little good if the material is stored unencrypted on hard drives likely to be seized when someone is arrested [36].

Fein, in the interview, reported that *Anonymous*, working with activists in various countries have found it necessary to work in a tight mentor role, with individual interaction over long time in order to overcome these problems [36]. It is not merely a skill set that must be acquired, but in some cases a whole culture that must be overcome. If, in your culture, conversation and communication takes place in groups, how can you implement a "need to know"-policy without alienating your comrades?

4.4 Regime use of ICT

Of course, the regime security services tried to counter the use of ICT by the rebels. In Tunisia, Egypt and Libya, they were ultimately unsuccessful [36]. Still, countries such as Saudi Arabia, Bahrain and the United Arab Emirates – where no revolutions took place – all had sophisticated systems for surveillance and

censorship in place [50]. In Tunisia, Egypt and Libya, surveillance might have been very good, but the enforcement of the laws was still restricted to physically arresting people, and when hundreds of thousands of people break the law at the same time, this is almost impossible. Nevertheless, it is clear that technology is capable of supporting both revolutionaries and dictators [18].

Shutting down the infrastructure is a double-edged sword, in that it may be essential to both sides in a conflict. However, many have argued that rebels and activists are more agile in rerouting to other technology [7] [34] [36]. Nevertheless, it should be noted that when the infrastructure was initially shut down, the rebels experienced great difficulties. If this had been coordinated with physical activities, the regimes of Tunisia, Egypt and Libya might have had greater success. As it turned out, the agencies using the ICT did not properly coordinate activity with the ones acting in the physical world. This is reminiscent of the difficulty of planning and coordinating military information operations [37] [67] [63].

Nonetheless, it is reasonable to believe that oppressive states will analyse and adapt their systems to better counter the use of ICT by dissidents, for example by preparing their infrastructure for selective shutdown or preparing in advance for the arrest of people who are known focal points of social media. As noted above, Saudi Arabia, Bahrain and the United Arab Emirates have already begun [50]. Some point to post-Soviet countries as a main source of inspiration for more sophisticated methods of internet control in authoritarian regimes [25]. Regardless, it is clear that Russia is taking the “threat” from ICT seriously, and is acting to counter it [38]. It remains to be seen whether future activists can use ICT as successfully against regimes that are skilled, ICT-competent and prepared.

5 References

[1] Amnesty International Annual Report on Tunisia. http://www.amnesty.org/en/region/tunisia/report-2013, 2013. Amnesty International, retrieved 2 July 2013.

[2] Jason P Abbott. Cacophony or Empowerment? Analysing the Impact of New Information Communication Technologies and New Social Media in Southeast Asia. *Journal of Current Southeast Asian Affairs*, 30(4):3–31, 2012.

[3] Nawaf Abdelhay. The Arab uprising 2011: new media in the hands of a new generation in North Africa. In *Aslib Proceedings*, volume 64, pages 529–539. Emerald Group Publishing Limited, 2012.

[4] Mark Aberdour. Achieving quality in open-source software. *Software, IEEE*, 24(1):58–64, 2007.

[5] Fauziah Ahmad, Chang Peng Kee, Normah Mustaffa, Faridah Ibrahim, Wan Amizah Wan Mahmud, and Dafrizal Dafrizal. Information propagation and the forces of social media in Malaysia. *Asian Social Science*, 8(5):71–76, 2012.

[6] Interview with Susan Alnaqshbandi, Tilburg University, 13 December 2012. Interviewed by David Lindahl.

[7] Taghreed Alqudsi-ghabra. Creative use of social media in the revolutions of Tunisia, Egypt & Libya. *International Journal of Interdisciplinary Social Sciences*, 6(6):147–158, 2012.

[8] Jon B Alterman. The revolution will not be tweeted. *The Washington Quarterly*, 34(4):103–116, 2011.

[9] Lisa Anderson. Demystifying the Arab spring: parsing the differences between Tunisia, Egypt, and Libya. *Foreign Aff.*, 90:2–7, 2011.

[10] Judy Bachrach. Wikihistory: Did the leaks inspire the Arab Spring? *World Affairs*, 174:35, 2011.

[11] Manaf Bashir. Framing an Online Social Movement: How Do the Leadership and Partici-pants of the Egyptian 6th of April Youth Movement Frame their Facebook Activism? *International Review of Information Ethics*, 18:71–83, 2012.

[12] Eva Bellin. Reconsidering the Robustness of Authoritarianism in the Middle East: Lessons from the Arab Spring. *Comparative Politics*, 44(2):127–149, 2012.

[13] Sheri Berman. The Promise of the Arab Spring. *Foreign Affairs*, 92(1):64–74, 2013.

[14] Internet in Egypt offline. https://bgpmon.net/?p=450, 28 January 2011. Retrieved 2 July 2013.

[15] Serajul I Bhuiyan. Social media and its effectiveness in the political reform movement in Egypt. *Middle East Media Educator*, 1(1):14–20, 2011.

[16] Jürgen Bitzer and Philipp JH Schröder. Bug-fixing and code-writing: The private provision of open source software. *Information Economics and Policy*, 17(3):389–406, 2005.

[17] Constantin M Bosancianu, Steve Powell, and Esad Bratovic. Social Capital and Pro-Social Behavior Online and Offline. *International Journal of Internet Science*, 8:49–68, 2013.

[18] Elizabeth I Bryant. The Iron Fist vs. the Microchip. *Journal of Strategic Security*, 5(2):1–26, 2012.

[19] Nadine Kassem Chebib and Rabia Minatullah Sohail. The reasons social media contributed to the 2011 Egyptian revolution. *International Journal of Business Research and Management (IJBRM)*, 2:139–62, 2011.

[20] 10 worst countries to be a blogger. http://www.cpj.org/reports/2009/04/10-worst-countries-to-be-a-blogger.php, 30 April 2009. CPJ Committee to protect Journalists, retrieved 2 July 2013.

[21] Francesca Comunello and Giuseppe Anzera. Will the revolution be tweeted? A conceptual framework for understanding the social media and the Arab Spring. *Islam and Christian–Muslim Relations*, 23(4):453–470, 2012.

[22] Simon Cottle. Media and the Arab uprisings of 2011: Research notes. *Journalism*, 12(5):647–659, 2011.

[23] Jim Cowie. Syrian Internet Shutdown. http://www.renesys.com/2011/06/syrian-internet-shutdown/. Retrieved 2 July 2013.

[24] Michael Dartnell. Insurgency online: Elements for a theory of anti-government internet communications. *Small Wars & Insurgencies*, 10(3):116–135, 1999.

[25] R. Deibert and R. Rohozinski. Control and subversion in Russian cyberspace. In Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, editors, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, pages 15–34. MIT Press Cambridge, MA, 2010.

[26] Larry Diamond. Liberation technology. *Journal of Democracy*, 21(3):69–83, 2010.

[27] Mario Diani. Networks and internet into perspective. *Swiss Political Science Review*, 17(4):469–474, 2011.

[28] Alexandra Dunn. Unplugging a nation: State media strategy during Egypt's January 25 uprising. *Fletcher F. World Aff.*, 35:15, 2011.

[29] Andrew England. Gaddafi turns screw on his people. http://www.ft.com/intl/cms/s/0/bbb1b688-3d20-11e0-bbff-00144feabdc0.html#axzz2ahluAMkz, February 2013. Financial Times, retrieved 11 July 2013.

[30] Mikael Eriksson. Perils Accompanying the Moment of Promise. Technical report, FOI, the Swedish Defence Research Agency, 2011. FOI-R--3273--SE.

[31] Mikael Eriksson. Re-Orient? – An overview of the Arab revolutions and the balance of power in the Middle East. Technical report, FOI, the Swedish Defence Research Agency, 2012. FOI-R--3278--SE.

[32] Mikael Eriksson. When Still Waters Fizz: the Fall of the 'Republican Monarchy' in Egypt. Technical report, FOI, the Swedish Defence Research Agency, 2012. FOI-R--3526--SE.

[33] Mikael Eriksson and Kristina Zetterlund. Dealing with change: EU and AU responses to the uprising in Tunisia, Egypt and Libya. Technical report, FOI, the Swedish Defence Research Agency, 2013. FOI-R--3589--SE.

[34] Henry Farrell. The consequences of the internet for politics. *Annual Review of Political Science*, 15:35–52, 2012.

[35] Mohammad Fazlhashemi. *Den arabiska våren: Folkets uppror i Mellanöstern och Nordafrika*. Historiska Media, Lund, 2013.

[36] Interview with Peter Fein, *Anonymous*, 22 February 2013. Interviewed by David Lindahl.

[37] Ulrik Franke. Information operations on the Internet: A catalog of modi operandi. Technical report, FOI, the Swedish Defence Research Agency, 2013. FOI-R--3658--SE.

[38] Ulrik Franke and Carolina Vendil Pallin. Russian Politics and the Internet in 2012. Technical report, FOI, the Swedish Defence Research Agency, 2012. FOI-R--3590--SE.

[39] Shami Ben Garbia. Tunisia: Flickr, Video-sharing Websites, Blog Aggregators and Critical Blogs Are Not Welcome. http://advocacy.globalvoicesonline.org/2010/04/28/tunisia-flickr-video-sharing-

websites-blogs-aggregators-and-critial-blogs-are-not-welcome/. GlobalVoices Advocacy, retrieved 2 July 2013.

[40] Mike Giglio. The Facebook freedom fighter. http://www.thedailybeast.com/newsweek/2011/02/13/the-facebook-freedom-fighter.html, 13 February 2011. Newsweek, retrieved 2 July 2013.

[41] Yves Gonzalez-Quijano. The Arab riots in digital transition times. Myths and Realities. *Nueva Sociedad: democracia y politica en America Latina*, pages 110–121, 2011.

[42] The Guardian. US embassy cables documents. http://www.guardian.co.uk/world/us-embassy-cables-documents/217138, 7 December 2010. Retrieved 2 July 2013.

[43] Naila Hamdy and Ehab H Gomaa. Framing the Egyptian uprising in Arabic language newspapers and social media. *Journal of Communication*, 62(2):195–211, 2012.

[44] Kawa Hassan. Making Sense of the Arab Spring: Listening to the voices of Middle Eastern activists. *Development*, 55(2):232–238, 2012.

[45] N. Hassanpour. Media disruption exacerbates revolutionary unrest: Evidence from Mubarak's natural experiment. In *APSA 2011 Annual Meeting Paper*, 2011. Available at SSRN: http://ssrn.com/abstract=1903351.

[46] Blake Hounshell. The revolution will be tweeted. *Foreign policy*, 187:20–21, 2011.

[47] Philip N Howard, Sheetal D Agarwal, and Muzammil M Hussain. When do states disconnect their digital networks? regime responses to the political uses of social media. *The Communication Review*, 14(3):216–232, 2011.

[48] Philip N Howard, Aiden Duffy, Deen Freelon, Muzammil Hussain, Will Mari, and Marwa Mazaid. Opening closed regimes: what was the role of social media during the Arab spring? 2011.

[49] Phillip Howard. The Arab Spring's cascading effects. http://www.psmag.com/politics/the-cascading-effects-of-the-arab-spring-28575/, 23 February 2011. Pacific Standard, retrieved 2 July 2013.

[50] Muzammil M Hussain and Philip N Howard. Democracy's Fourth Wave? Information Technologies and the Fuzzy Causes of the Arab Spring. March 27 2012. Available at SSRN: http://ssrn.com/abstract=2029711.

[51] George (ed.) Joffé. *North Africa's Arab Spring*. Routledge, 2012.

[52] Seth G Jones. The Mirage of the Arab Spring. *Foreign Affairs*, 92(1):55–63, 2013.

[53] A.M. Kaplan and M. Haenlein. Users of the world, unite! The challenges and opportunities of Social Media. *Business horizons*, 53(1):59–68, 2010.

[54] Alexander Kazamias. The 'Anger Revolutions' in the Middle East: an answer to decades of failed reform. *Journal of Balkan and Near Eastern Studies*, 13(2):143–156, 2011.

[55] Roula Khalaf. Nahda party reflects a divided Tunisia. http://www.ft.com/cms/s/0/37efc52e-76a3-11e2-8569-00144feabdc0.html#axzz2ahluAMkz, February 2013. Financial Times, retrieved 11 July 2013.

[56] Michel Kilo. Syria... the road to where? *Contemporary Arab Affairs*, 4(4):431–444, 2011.

[57] Kalliopi Kyriakopoulou. Authoritarian states and internet social media: Instruments of democratisation or instruments of control? *Human Affairs*, 21(1):18–26, 2011.

[58] Madelene Lindström and Kristina Zetterlund. Setting the Stage for the Military Intervention in Libya: Decisions Made and Their Implications for the EU and NATO. Technical report, FOI, the Swedish Defence Research Agency, 2012. FOI-R--3498--SE.

[59] Fredrik Lindvall and David Forssman. Internationella insatser i Libyen 2011. Technical report, FOI, the Swedish Defence Research Agency, 2012. FOI-R--3447--SE.

[60] Maria Lipman and Nikolai Petrov. Obshchestvo i grazhdane v 2008–2010 gg.[Society and Citizens 2008–2010]. Technical report, Carnegie Moscow Center, 2010. Carnegie Moscow Center Working Papers No. 3.

[61] Alexis Madrigal. The inside story of how Facebook responded to Tunisian hacks. http://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044/, 24 January 2011. The Atlantic, retrieved 2 July 2013.

[62] Essam Mansour. The role of social networking sites (SNSs) in the January 25th Revolution in Egypt. *Library Review*, 61(2):128–159, 2012.

[63] James McNeive. Frustration. In G.J. David Jr. and T.R. McKeldin III, editors, *Ideas as weapons: influence and perception in modern warfare*. Potomac Books, Inc., 2009.

[64] Evgeny Morozov. *The Net Delusion: How not to liberate the world*. Penguin, 2011.

[65] San Murugesan. Understanding web 2.0. *IT professional*, 9(4):34–41, 2007.

[66] Mohamed Nanabhay and Roxane Farmanfarmaian. From spectacle to spectacular: How physical space, social media and mainstream broadcast amplified the public sphere in Egypt's 'Revolution'. *The Journal of North African Studies*, 16(4):573–603, 2011.

[67] Keith Oliver. Are we outsmarting ourselves? In GJ David Jr and TR McKeldin III, editors, *Ideas as weapons: influence and perception in modern warfare*. Potomac Books, Inc., 2009.

[68] Anthony A Olorunnisola and Brandie L Martin. Influences of media on social movements: Problematizing hyperbolic inferences about impacts. *Telematics and Informatics*, 30(3):275–288, 2013.

[69] Open Net Initiative. OpenNet Initiative Syria Profile 2009. https://opennet.net/research/profiles/syria, 7 August 2009. Retrieved 2 July 2013.

[70] Internet enemies report 2012. Reporters Without Borders, March 2012.

[71] Dan Roberts. US says it will arm Syrian rebels following chemical weapons tests. http://www.guardian.co.uk/world/2013/jun/13/syria-chemical-weapons-us-confirm, June 2013. The Guardian, retrieved 3 July 2013.

[72] Hal Roberts, David Larochelle, Rob Faris, and John Palfrey. Mapping local internet control. In *Computer Communications Workshop (Hyannis, CA, 2011), IEEE*, 2011.

[73] Yasmine Ryan. Tunisia's bitter cyberwar. http://www.aljazeera.com/indepth/features/2011/01/20111614145839362.html, 6 January 2011. Al Jazeera English, retrieved 2 July 2013.

[74] Nivien Saleh. Egypt's digital activism and the Dictator's Dilemma: An evaluation. *Telecommunications Policy*, 36(6):476–483, 2012.

[75] Sarah Cook Sanja Kelly and Mai Truong (eds.). *Freedom on the net 2012: a global assessment of internet and digital media*. Freedom House, 2012.

[76] John Scott-Railton. Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution. Technical report, United States Naval War College, Center on Irregular Warfare and Armed Groups, 2012. CIWAG case study series 2013, ed. Richard Crowell, Marc Genest, and Andrea Dew.

[77] Shaked Spier. Collective Action 2.0: The Impact of ICT-Based Social Media on Collective Action–Difference in Degree or Difference in Kind? 2011. Available at SSRN: http://ssrn.com/abstract=1979312.

[78] Madeline Storck. *The Role of Social Media in Political Mobilisation: a Case Study of the January 2011 Egyptian Uprising*. PhD thesis, December 2011.

[79] Strategic policy issues. *Strategic Survey*, 111(1):97–138, 2011.

[80] Besiki Stvilia, Michael B Twidale, Linda C Smith, and Les Gasser. Information quality work organization in Wikipedia. *Journal of the American society for information science and technology*, 59(6):983–1001, 2008.

[81] Bogdan Szajkowski. Social Media Tools and the Arab Revolts. *Alternatif Politika/Alternative Politics*, 3(2):420–432, 2011.

[82] The International Federation for Human Rights. The Emergency Law in Egypt. http://www.fidh.org/the-emergency-law-in-egypt, 3 February 2011. Retrieved 2 July 2013.

[83] The Tor Project, Inc. Tor anonymity online. https://www.torproject.org/. Retrieved 2 July 2013.

[84] Official Records of the Security Council 6498th Meeting. United Nations, New York: 17 March 2011, S/PV.6498.

FOI, Swedish Defence Research Agency, is a mainly assignment-funded agency under the Ministry of Defence. The core activities are research, method and technology development, as well as studies conducted in the interests of Swedish defence and the safety and security of society. The organisation employs approximately 1000 personnel of whom about 800 are scientists. This makes FOI Sweden's largest research institute. FOI gives its customers access to leading-edge expertise in a large number of fields such as security policy studies, defence and security related analyses, the assessment of various types of threat, systems for control and management of crises, protection against and management of hazardous substances, IT security and the potential offered by new sensors.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone: +46 8 555 030 00
Fax: +46 8 555 031 00

www.foi.se