10 Webs of Change? The Transformation of Online Social Networks and Communication Infrastructures from a Technological Point of View

Tobias Amft and Kalman Graffi

Free speech is mankind's most valuable achievement. If not censored, it allows people all over the world to express their feelings, their thoughts and, most valuably, their knowledge. In the recent past, the internet has become the dominant communication channel by which information and data is exchanged. At any given moment, billions of bits and bytes are traveling around the earth at the speed of light. People are able to form groups and meet in virtual reality even when scattered around the globe. However, as technology has improved, authorities have increasingly felt the urge to monitor, censor or even prohibit communication via the internet, as the vast network allows information and ideologies to spread extraordinarily rapidly.[1]

From a computer scientist's point of view, the Egyptian upheavals were technologically the most interesting of the Arab uprisings. The Egyptian government managed to shut down the country's internet access (nearly) completely, with the intention of hindering the revolts' growth. Paradoxically, this decision may have even intensified the revolt, as it led to an effective communications blackout for more than 80 million people. As explained in Eaton (2013), participants in the demonstrations of January 25, 2011, mainly used Facebook (>85%) to organize and plan activities related to the revolts, as well as to inform Egyptians and the outside world about the ongoing events. Other internet-based services such as Twitter, Flickr and YouTube were used in a similar manner around that time (Mansour 2012). On January 25, 2011, the Egyptian government decided to block all access to Twitter, and the prohibition on Facebook followed one day later (Dainotti et al. 2011). Internet access more broadly was entirely shut down during the night of Thursday, January 27, with the block lasting

1 See the contribution by Carola Richter and Hanan Badr in this volume for a communication studies' perspective on these phenomena.

through Friday, January 28. The Egyptian government instructed internet providers to shut down their services (Cowie 2011 a). On February 2, Egypt returned to the internet (Cowie 2011 b). According to Dainotti et al. (2011), Libya carried out a similar procedure around two weeks later, on February 18. While activists had previously suspected that their digital communications were being spied on, these steps indicated that even their connectivity itself was in danger.

In this article, we review the technology and infrastructure used for online social communication, and discuss the technological weaknesses that allow these networks to be spied on, censored and blocked, thus hindering the dissemination of information. We present the current state of technological developments within the computer science field, particularly focusing on tools for secure, anonymous and untraceable communication. We offer an evaluation of the degree to which the Arab uprisings affected academic thinking in the field of computer science, especially regarding topics such as privacy, anonymity, and security in networking and communications. We provide a brief overview of recent changes in academic thinking. Finally, we analyze and explain recent advancements in technology, and predict possible future trends in the areas of privacy, surveillance and censorship.

Computer science fields affected by the Arab uprisings

In the following section, we describe how internet services can be — and have been — blocked, and how the internet as a communication platform can be shut down by governments at will.

Researchers in computer science reflect on current events and sometimes include them in their research activities as case studies. Here, it is worthwhile discussing which fields in the computer science research sphere have been affected by the Arab uprisings. According to the German Research Association's (DFG) classification system, the field of computer science is clustered into eight subject areas, the most prominent being "theoretical computer science", "software engineering and programming languages" and "computer architecture and embedded systems".

These three subject areas investigate the basic foundational elements of computer science, including theory as well as the engineering aspects of software and hardware. The theoretical aspects of computer science are highly abstract and analytical, and often involve the simplification of prac-

tical experience. The hardware-related subject area, which relates to computer architecture and embedded systems, aims to accelerate and improve hardware solutions over long-time scales. Software engineering and programming languages offer tools to fully harness the potential of the hardware, and to support ongoing trends such as parallelization, distributed computing, and device and technology-specific programming. These subject areas are therefore comparatively minimally affected by current events or singular use cases.

One further subject area is "information systems, process and knowledge management". This focuses on the application and integration of IT solutions in business processes, and focuses on long-term application scenarios. It is based on the assumption that computer science plays a vital role in business processes, and often also acts as an enabler or cost-saving measure for specific business cases.

Two subject areas that have attracted increasing interest in recent years, and which are relevant to the events of the Arab uprisings, are "massively parallel and data intensive systems" and "interactive and intelligent systems, image and language processing, computer graphics and visualization". Both of these fields are related to the identification, processing and interpretation of large amounts of data. This trend is known as "big data". Processing digital information, either from advertisements, metadata, social networks or communications, allows customers to be clustered, revenues to be increased thanks to improved advertising and recommendations, and the future behavior of customers to be predicted. The same concept of deep data analysis can be used to observe communication patterns on the internet, identify discussion and communication topics, and initiate reactions to them. For instance, the communications may be reported to a third party or blocked. Thanks to advancements in the area of data-intensive systems and data processing, more and more information can be obtained from a steadily growing amount of data sources. Thus, advancements in this field contributed to the surveillance of internet users in the Arab world during the Arab uprisings, as well as worldwide.

The two remaining subject areas comprise trends that support the flow of information and counteract surveillance and the control of communication. These are "security and dependability", and "operating, communication, database and distributed systems". The subject area of "security and dependability" aims at providing solutions to support the security goals of confidentiality, integrity, and authentication, as well as availability and privacy. Thus, progress in this field directly affects what data can be ob-

tained from users against their will. Secure communication over the internet — that is, communication that is confidential and anonymous — would allow internet users to exchange their ideas freely. However, secure communication still leaves traces that allow for the identification and blocking of this communication.

Here, the subject area of "operating, communication, database and distributed systems" provides various solutions with which to overcome these threats. Specifically, in this article we elaborate on what research questions were identified in response to connectivity interruptions and observable communication trails during the Arab uprisings. In the field of communication and distributed systems, various approaches have emerged to obfuscate communication trails, to support anonymous communication, to hide communication patterns and even to avoid the internet in digital communication. Combined with security considerations, these novel distributed platforms promise to support digital communication that cannot be spied on, blocked or censored. In the following section, we describe the main principles and building blocks of the internet before presenting and discussing the advancements in computer science, specifically in the area of secure communications, that have been initiated thanks to observations made during and after the Arab uprisings.

A brief description of the internet

Before we describe the internet itself, we will first explain basic concepts of its technology. According to Kurose and Keith (2007), the internet is a computer network which connects billions of devices, such as PCs and smartphones, which we denote as hosts. Communication links and packet switches are used to interconnect those hosts physically. From another point of view, the internet is a complex infrastructure that offers various services. In order to combine the physical devices and to guarantee specific services, rules are needed that bring the internet's components to life.

Those rules, or more precisely protocols, define a communication structure that is followed by two or more devices (hosts and packet switches) in a network in order to exchange information. More specifically, protocols define actions and corresponding reactions that are performed upon events in the network — for example, upon the sending or receiving of a message. Access to the internet is typically granted by an organization we denote as an internet service provider (ISP).

Two important protocols have to be discussed here in order to understand the delivery of data via the internet: the Internet Protocol (IP) and the Transmission Control Protocol (TCP). The Internet Protocol assigns addresses to computers in a network in order to enable data delivery, in the form of data packets, from a given source host to an arbitrary destination host.

Unfortunately, the Internet Protocol itself gives no guarantee that the packets traversing the internet will reach their destinations reliably. The purpose of the Transmission Control Protocol, which is often used in combination with the IP, is twofold. One purpose of the TCP is to secure the reliable delivery of packets between two communication hosts. Reliability in this context means that all packets are guaranteed to reach their destination and the order of data is preserved during delivery. For this reason, the TCP comprises different techniques that control the traversal through a network. The second purpose of the TCP is to identify and separate different applications running on a single host. For example, a user may be streaming music from an internet radio station while simultaneously retrieving the latest news from an online magazine, thus engaging in two different applications at the same time. Since the internet today consists of billions of connected devices, the task of finding the device associated with a given internet address is not an easy task. Rules have to be defined and followed in order to enable data to flow efficiently from a source computer to the correct destination. For a proper explanation, we here introduce the terms *forwarding* and *routing*. By *forwarding*, we mean the process that takes place when a single computer hands over incoming packets to another computer. *Routing* describes the whole process of finding a path from a given source computer to a desired destination, using a set of potential intermediary nodes that forward data packets to their final goal. Algorithms and rules that specify a forwarding strategy for participating devices are termed routing algorithms or routing protocols. A device that decides how to forward a given packet, on the other hand, is usually called a router.

The internet, which has become one of the most complex infrastructures humanity has ever created, today consists of many different devices, routers and routing protocols that in combination yield the great variety of services we use every day. Despite its complexity, the internet is made up of multiple smaller networks that are controlled and managed by different organizations, typically internet service providers, so that a certain hierarchy is formed. The parts of the internet managed by different organiza-

tions are called autonomous systems. One indispensable protocol that connects all existing autonomous systems is the Border Gateway Protocol. One of the several tasks of this protocol is to announce an autonomous system's existence to other autonomous systems on the internet. Furthermore, the Border Gateway Protocol ensures that all autonomous systems on the internet know how to route messages to a specific autonomous system.

Technical possibilities of censoring communication on the internet

The Arab uprisings and the resulting blockade of the internet in Egypt and Libya prove that the surveillance and censorship of internet traffic are desirable goals for certain governments. During the Arab uprisings, these were elements of state campaigns to oppress certain groups of interest such as activists, insofar as the technology available at that time permitted. Technically, we can differentiate between two main types of attacks on the internet or network traffic in general. Passive attacks on network traffic allow an adversary to monitor communication without any interference that could be detected by a participant. As the word "passive" suggests, adversaries in this case do no more than "listen" to the forwarded data packets without changing their content. Active attacks, on the other hand, allow an adversary to read, manipulate, delete or even block the content of network traffic. Since secret surveillance of communication did not play a major role during the Arab uprisings (passive attacks alone are not sufficient to block a whole country's internet access), we will focus on active attacks on network traffic in the following discussion. These attacks share the common feature that they are at least partially noticeable to internet users. By "partially noticeable", we refer to the fact that the content of censored websites might be blocked. However, a user may only notice the absence of such content if she or he can compare a non-blocked version of the site as a reference. Next, we will present some commonly used techniques in active network attacks.

Search engine censorship

As a constantly growing system, the internet contains more than 46 billion sites, according to estimates from de Kunder (2015) in August 2015. How-

ever, the number of websites any given person visits with any frequency is very small in comparison to the overall size of the internet. Much like a search catalog in an enormous library, a web search engine is a system, usually accessed via a web browser, that enables a user to search the World Wide Web for a given search term.

Normally, a search engine returns a sorted list of popular websites that contain the search term in any form. According to NetMarketShare (marketshare.hitslink.com), the most extensively used search engine is Google, with a market share of 70.2% in July 2015, followed by Bing (10.3%), Yahoo (9.5%) and Baidu (7.1%).

Search engine censorship is probably the simplest form of blocking access to websites. The normal procedure of a search engine is to start with a list of known websites, called seeds, and to follow all newly found hyperlinks in a recursive manner; this activity is called web crawling. All websites found by the web crawler are stored by the search engine provider in a database for later use. When a user initiates a search query, the search engine compares its index database with the given keyword(s) in order to identify matches between the search term and stored websites. A service provider may return all or no matching results to the user, and may filter some results out.

One example of the exclusion of search results in Germany and France is given in Zittrain and Edelman (2002). The authors studied internet filtering initiated by governments with the aim of restricting access to websites deemed illegal under local laws, for example those that offered anti-Semitic, Nazi-related or radical Islamic content. However, since the technique of search engine censorship is simple, bypassing this mechanism is also uncomplicated. A website that is well known to a person or a sympathizing group can be accessed directly without the use of a web search engine. Alternatively, other search engines can be used. Sometimes the use of a proxy server can help to circumvent local restrictions. We provide more details on proxy servers in the section on proxy routing.

Deep packet inspection

Actively hindering people from accessing specific sites on the internet is more costly than simply monitoring network traffic. The well-targeted filtering and surveillance of information traversing the internet requires access to the internet's infrastructure in order to carry out the attack. Dis-

carding arbitrary packets or randomly distorting the global functionality of any service is no real benefit to an attacker, as this happens on a small scale in the network in any case. Large projects designed to engage in packet filtering (or any other similar projects) are only effective if they pursue a specific goal, with their intervention placed at the right location or advertised to the right group of people, thus ensuring they are on the main routes of the targeted data flow. Furthermore, potential attackers must have access to the parts of the network in which interventions are worthwhile. We take a closer look at how packets can be filtered and discarded in a network using the example of Tunisia, a country in which filtering and deep-packet inspection were present long before the Arab uprisings emerged (Wagner 2012).

In order to investigate packets in depth, a government must be capable of intervening in network traffic at specific, critical internet locations. For example, the Tunisian government had to engage in direct manipulation of the border gateway routers that run the Border Gateway Protocol.

At this point, we have to remember that the Border Gateway Protocol enables routing (the forwarding of packets) between different autonomous systems. The border gateway routers are best suited to monitoring connections between the national network, the Tunisian part of the internet, with the other networks and other parts of the internet. Among routers located at the border with other countries, selected internet gateways inside Tunisia are interesting targets for an attack. Internet gateways are typically locations or addresses in a network that offer access to the internet as a service to all participants in the network. In Ben Ali's Tunisia, the Tunisian Internet Agency (ATI) provided the gateway that served all Tunisian ISPs (OpenNet Initiative 2009). Since this agency was subject to the influence of the Ben Ali regime, it was the institution that intercepted network traffic.

At these gateways, it is theoretically possible to investigate packets that traverse the internet. Thus, packet filtering can be done very easily. Whenever an unencrypted packet traverses a gateway under surveillance, firewall-like programs search for specific keywords deemed suspicious by an inquisitive government in the passing data stream.

The work of Clayton, Murdoch & Watson (2006) describes in detail how TCP connections associated with specific keywords can be terminated by an attacker. As one example, China forces suspicious connections to close by answering queries with special TCP packets. In much the same manner as a normal firewall, which allows desired packets to be forward-

ed while dropping undesired packets, any government — for instance, those in Tunisia or Egypt — is capable of controlling the forwarding mechanism of packets entering its national network. The government can decide whether to forward, observe or drop messages. If we take Tunisia as an example, the Tunisian Internet Agency was created in 1996 with the goal of controlling national network traffic, and was instructed to start the process of internet censorship in the country in 1997 (Wagner 2012).[2]

However, deep packet inspection techniques operate more subtly and unobtrusively than we might think. A normal user might blame lost content on technical problems that seem to originate with the browser or the internet service provider. Even trickier is when TCP connections are properly closed by the attacker, and the user receives nothing more than a notification that a technical problem has occurred. In such scenarios, it is not clear whether some third person blocked access to a service, or the service itself failed due to technical problems. Moreover, the Tunisian government, like others, already had the capability to analyze and filter specific URLs and emails under Zine El Abidine Ben Ali. A telecommunications law passed in 1998 even allowed the Tunisian authorities to examine the content of personal email messages (OpenNet Initiative 2009). This goal can be accomplished with commercial filtering software that scans various websites or messages on the internet and searches them for specific keywords. Whenever those keywords are found on a website, queries to the website are detected with packet-filtering methods and blocked. Email messages that are not encrypted can be manipulated or censored after detection. This technique is often combined with IP address blocking. Well-known websites or web servers on the internet can be identified through their IP addresses. With the use of IP address blocking, connections to known addresses on the network are directly blocked. From a technical point of view, this kind of attack is a simple firewall setting that blocks the traffic to or from a specific IP address or whole address blocks.

2 See the contribution by Sarhan Dhouib in this volume on surveillance methods in Ben Ali's Tunisia that go beyond computer networks.

Disconnection of networks

As noted above, the internet has grown to become a system connecting billions of devices. We have already discussed the Border Gateway Protocol, whose goal is to connect different autonomous systems and announce their existence to each other. In other words, the linkages between all the different autonomous systems form the internet as we know it. The Border Gateway Protocol — or rather, the routing entries in a border gateway router — are necessary for packets to find their way from their starting point to an arbitrary target on the internet.

In 2011, during the uprisings, the Egyptian government exploited the nature of the Border Gateway Protocol in order to stop some messages from leaving the country. Technically, the Egyptian government simply deleted the Border Gateway Protocol entries in the border gateway routers that connect Egypt to neighboring countries. After this had been done, packets addressed to any target outside Egypt were no longer able to find a path forward toward their destinations. Packets that reached a border gateway router responsible for the forwarding of the packet across national borders were simply lost, since border gateway routers without routing entries normally do not know how to forward incoming packets.

A more drastic method would be to disconnect border gateway routers from the physical network, or even to cut the cables connecting different devices. The drawback to this method is mainly the increased material costs. In any case, the deletion of routing entries at border gateway routers is enough to fulfil this purpose.

Solutions for combatting surveillance and censorship in general

While techniques for surveillance and censorship are numerous, so are techniques and technologies that allow these mechanisms to be bypassed. As long as there are multiple autonomous systems present on the internet, or at least multiple devices that do not belong to one organization, there will be a way to communicate unreservedly and freely. Here, we present an assorted collection of techniques that can be used to avoid both censorship driven by active attacks and surveillance carried out through passive network observation. These solutions originate from the computer science subject areas of “security and dependability” and “operating, communication, database and distributed systems”.

Encryption

The wish to hide confidential information from prying eyes leads to the oldest known tool for thwarting surveillance: encryption. One of the first encryption algorithms known from historical records is the Caesar Cipher, invented by Julius Caesar, in which letters are simply shifted by a known number of positions in the alphabet. Subsequently, only those people who are privy to this secret are able to reconstruct the original plain text. Hence, communication partners always have to share a common secret, usually denoted as a key, to be able to encrypt and decrypt data. Encryption has remained a commonly used method for transferring information in an unreadable form to the present day. However, procedures have become increasingly advanced. Simple methods like the Caesar Cipher suffer from small key sets; today, smart algorithms are able to reconstruct the unencrypted plain text even without prior knowledge of the secret used to encrypt the information.

By contrast, modern encryption algorithms rely on more complex methods to translate plain text into cipher text. In theory, the reconstruction of the encrypted text would require an attacker to guess the correct key out of a very large pool of possible combinations. When a sufficiently large key is used, discovering it — and thus gaining access to the original message — would require billions of years of analysis using current hardware and software. Encryption in general can only be used to protect the content of communication from being seen by unauthorized persons — a property termed confidentiality. However, such methods are not enough alone to provide anonymity, privacy and security. Even with an encrypted message, attackers could still determine the identities of the communicating partners, and hinder them from exchanging further messages or initiating further actions online.

Proxy routing

Anonymity on the internet is usually implemented through proxy routing. The main goal of this technique is to prevent the true sender, receiver, or sender and receiver simultaneously from being identified by other participants in a network. This goal is achieved by forwarding messages to one or multiple relaying participants (proxies) in the network before they are sent on to a specified destination. Optionally, messages are often encrypt-

ed. The strategy of routing messages via additional participants is necessary in order to conceal the full path a message is traveling, and thus also the origin and sometimes the final destination of a message as well.

The best known example in this field is the Tor project (torproject.org), which allows its users to contact (web) servers without revealing their own IP addresses or locations. Using Tor, requests for a website are routed through an encrypted connection and between several Tor servers before they reach the destination web server. The last participant in the message forwarding chain, called the exit node, makes the connection to the web server and requests the desired website. The website data is then passed all the way back to the initial requester. Although Tor is designed to provide a certain level of anonymity by concealing the user's address, the system is helpless against the manipulation or censorship of websites or other information on the destination server. However, the proxy routing method has the additional potential capability of allowing one to circumvent regional search engine restrictions, for example. If a proxy is used to forward messages and queries, a search engine will believe the request has originated at a location near the proxy. If the proxy is located in a region in which no restrictions are imposed on search results, it will be able to forward those results back to the original requester without any limitations, assuming the proxy itself is not malicious.

Decentralization of service provisioning

The Arab uprisings were characterized by the strong use of social media tools and familiar internet platforms, such as Facebook, Twitter and YouTube, to organize demonstrations, share informational content or simply criticize the government. Social media was also used to communicate with countries outside the Middle East and North African (MENA) region, and to exchange information with people living in other countries involved in the Arab uprisings (Howard et al. 2011). According to the Institute of World Economy and International Relations (IMEMO), information was disseminated more quickly over Facebook than over the Arab TV channel Al-Jazeera (Stepanova 2011).

As a response to the revolutionary movements in North Africa, the Egyptian government instructed mobile phone operators and internet service providers to suspend their services. As a result, users were cut off from most parts of the internet. Several governments had done this before;

for example, Nepal cut off internet access entirely in 2005, as did Myanmar two years later in 2007 (Richtel 2011). The cases of Nepal, Myanmar and Egypt are rare examples that could be repeated any time, virtually anywhere. They show clearly that governments of countries with simple internet infrastructures are capable of stopping national internet traffic almost entirely. In such cases, most internet services and therefore social media tools are not reachable as the providers' servers are mostly located in the United States, as is the case for Twitter, Facebook, YouTube and Yahoo.

Another problem arises with traditional client-server approaches: a lack of privacy and trust. Centralized servers constitute a single point of service provisioning, with all users acting as (passive) clients that simply use the service. These servers represent single points of failure, making it easy to intercept and manipulate the information they provide. The recent revelations regarding the US National Security Agency (NSA) surveillance programs offer evidence that major internet services such as Facebook, Yahoo and Twitter, all of which are based on this client-server architecture, are well suited to being spied on. Edward Snowden revealed how the NSA uses its PRISM program to investigate packets traversing the internet in 2013. The essential basis for this to happen is that almost all information about the users of these services is gathered centrally at the providers' servers. The providers are able to censor content and opinions, read private and confidential messages, modify or market user data, or shut off internet services in oppressive countries that want to reduce communication on specific topics, as was the case during the Arab uprisings. Although the majority of users remain unaware of the risks of using centralized online social networks, and ignore the possibility of their communications being manipulated or intercepted, for some users in the world it is crucial — or even vital — to have the opportunity to communicate and organize with friends in a secure, confidential and anonymous way.

Distributed social networks, on the other hand, work to alleviate the security and censorship risks posed by centralized online social networking sites. Two significant trends have emerged in the area of distributed social networking: private-server approaches and peer-to-peer (P2P) approaches. Under private-server approaches, users set up private web servers and connect them to create a distributed social network. With this approach, central storage points are eliminated, and control over the data being exchanged remains with the users or their friends. However, the risk of data misuse and censorship remains, as any of the participating web servers

may be compromised or shut down. Diaspora (diasporafoundation.org) is one prominent example of the private-server approach. This project was initiated in 2010 by four New York University (NYU) students who wanted to create a Facebook-like network based on a decentralized structure in which control over user content would remain with the users themselves.

In contrast to the centralized server architecture, peer-to-peer-based online social networks, such as LibreSocial (libresocial.com), formerly known as LifeSocial (Graffi et al. 2010), began gaining prominence a few years ago. All participants in a peer-to-peer network essentially share equal rights and duties. User-related information is distributed among and hosted by all network participants in a decentralized manner, without the need for dedicated servers. The peer-to-peer architecture therefore enables data sharing or information dissemination even though the information is never stored on a central server. Users are expected to be active in the network only temporarily, and the functioning of the network does not rely on the assumption of any permanently online servers. While these research projects are quickly advancing, they have not yet yielded concrete final results.

Darknets: Anonymous communication with the help of peer-to-peer networks

Darknets are defined by Biddle et al. (2003) as content distribution networks in which resources and infrastructure are provided by their users, in a manner similar to peer-to-peer networks. Thus, content is introduced by network participants and is exchanged directly between users who are in contact with each other. In darknets, each node can be contacted only by a highly restricted set of trusted individuals. Strangers are not allowed to establish contact, as this would allow them to observe communication patterns and gather information that might be misused, such as what files were queried or served. Another characteristic of darknets is that single hosts cannot be found using regular internet tools, since they are connected to other members of the network in an arbitrary fashion without being registered in a search engine or any other central server. The advantages of private P2P networks, another term for darknets introduced by Rogers and Bhatti (2007), center on the high degree of anonymity and privacy provided. While the actions of people using regular social communication applications can be observed and traced back to individuals, users in private

peer-to-peer networks communicate only with contacts that are assumed not to be tracing them. Security can be further enhanced through the use of encrypted communication between nodes.

The last few years have seen a growing need for anonymous communication. Three primary kinds of anonymous peer-to-peer networks have formed as a response. In the first category, communication paths inside the network are hidden from potential observers. One common approach to providing anonymity in these networks is to use multi-hop relaying. Under this model, individual nodes simply forward chunks of data without knowing the identity of the originator or the destination node. When a query is sent out, it leaves a trail that is used to send the requested data item in reverse, hop by hop, along the same path traveled by the initial request. In addition, communication is encrypted in order to provide confidentiality.

The second category is made up of group-based networks, in which all users in the network are assumed to be trusted. The network's users only remain anonymous to entities outside the network but not to those inside the network. These networks can only be trusted as much as each of their participating members. From a technical perspective, every individual member of the group is considered to be trustworthy, and communications are encrypted with a group key, thus preventing entities outside the network from gaining insight into interactions within the network.

Finally, in the third category of friend-to-friend networks, connections are established only with selected trusted friends, each of whom acts as trusted proxy routers for traffic from their other friends. While in group-based approaches, the whole group of participants is considered trustworthy and the goal is to preserve users' anonymity to potential outside attackers, in friend-to-friend peer-to-peer networks, only a few friends are trusted, while the other members in the broader network are not trusted. A simple approach to forming a friend-to-friend network is to connect only to trusted friends, thereby establishing an unstructured peer-to-peer network.

The use of encryption to hide message content, proxies to prevent communications from being traced to the senders or recipients, and decentralization to create self-operated and self-organizing communication networks are the primary viable ways of engaging in secure and private communication online. These approaches are typically less user-friendly than the more common centralized communication tools used widely on the internet. Encryption keys have to be managed, proxies operated, and complex protocols and the effects of these communications have to be con-

trolled. However, since the technical security challenges of these solutions have for the most part been solved, the research community's focus is shifting toward creating more user-friendly versions of the tools.

Influence of the Arab uprisings on the computer science field

A sharp change in thinking within the field of academic computer science after the uprisings cannot be ascertained directly. Only selected subject areas within the academic computer science field have been affected by, or have themselves affected, the events of the Arab uprisings. Research on big data analysis has enabled communication patterns and topics in large networks to be identified, thus allowing surveillance-minded authorities to track down activists and limit the free flow of information. However, research in the area of security and communication systems reacted to the events by creating a set of solutions that will enable secure communications in the future. Although the immense communications collapse during the revolutionary protests in the Middle East and North Africa cannot be seen as having triggered a new era of technological thinking, the Arab uprisings do offer an illuminating example of small changes in the way the internet is being used today.

The Snowden affair in 2013, also known as the NSA scandal or the PRISM affair, probably had more impact on people in Europe and the United States than the Arab uprisings did. Following Snowden's revelations, people realized they had been systematically monitored by a foreign agency and government. The threat of surveillance thus moved closer. The way people regarded their privacy changed drastically. However, the technology used for communication purposes online still utilizes well-known architecture.

One explanation for the fact that mainstream computer science trends have not changed due to single incidents such as the Arab uprisings is that the political revolutions did not lead to a technical revolution. No surprising new technologies or systems emerged after the uprisings in North Africa. All the software and systems used or shut down during the Arab uprisings had been developed long before the civil riots began. In this case, a technical evolution seemed to precede the political revolution.

Social media and communication tools played a peculiar role during the Arab demonstrations. Many articles since have analyzed the use of social media platforms such as Facebook and Twitter at that time, but few have

analyzed the technology behind those systems. Without going too deeply into detail, we can say that social media platforms are mostly based on technologies that had already been widely used for many years before the uprisings in the Middle East and North Africa took place. The most significant change in these systems has come as access to online social media has become easier and simpler over time. In contrast to decades past, smartphones, tablets and computers, combined with cheap and easy-to-use communication platforms, rule the internet today. Using the internet no longer requires special knowledge. Anyone able to read and write can post his or her thoughts online in a few seconds.

The protests and demonstrations during the Arab uprisings were not driven by social-media platforms themselves, but rather by their users. However, inexpensive and easy-to-use platforms such as Facebook, Twitter, Google and YouTube are gaining increasing popularity among internet users. Those systems are open to all, and the more they are used, the more they become interesting to other users who want to express themselves.

In the previous chapter, we introduced techniques of engaging in secure and anonymous internet communication that are not provided by most online social networks today. We know from interviews with people in the Middle East and North Africa that state surveillance and censorship had begun years before the Arab uprisings started. To avoid being spied on by the government and being arrested for distributing censored content, some people in the region used secure communication tools that utilized some of the methods described above.

One of our anonymous interview partners described problems with tools such as Textsecure or Signal, which provide secure communication on smartphones, as follows:

> "I am a technologist, the problem is not with us; the problem is for the real people. They need easy-to-use solutions. And they come at times when things are urgent; they need solutions that work easily and out of the box. Although Textsecure is easy to use for us, it is difficult to use for others. I have written guides and manuals before, but there are many different challenges and situations; thus they are not always reusable" (interview by the authors).

Thus, it is evident that although technical solutions for avoiding security risks and massive censorship do exist, most people lack the knowledge that would allow them to use these techniques properly. Researchers are aware of this problem, and creating user-friendly expressions of these scientific solutions is becoming an increasingly important goal.

The Arab uprisings illustrate that specific circumstances at a specific time and place may drive the use and popularity of social media tools. However, it is always the people using social platforms to express their feelings, post pictures and share emotions who define the platforms — not the other way round. The Arab uprisings may ultimately serve as an important catalyst that drives the development of free internet, free communication, and use of the tools necessary for these goals in the Middle East and North Africa. From a scientific point of view, however, the events in the MENA region have had comparatively little influence on academic research within the computer science field. Indeed, it can be observed that the use of technology and social media in the MENA region has been only a small part of a bigger process that might affect computer science and the natural sciences as a whole. An ever-increasing number of people around the world are affected by technology and find pleasure in its use. However, most users prefer tools that are easy to use, even if they are insecure. This ongoing change in the cost, usability and design of technical devices might ultimately produce research focusing on the interactions between complex technology and human beings.

Even outside the academic research sphere, there are many community-driven projects that focus on the challenge of creating communication systems resistant to surveillance. Many of these projects share source codes and ideas in an open fashion, with the aim of being fully transparent to all users and developers, and thus exposing potential mistakes and security issues before they become problematic. The more people inspect a project's source code, the more likely it is that security problems or vulnerabilities that compromise privacy will be detected and avoided. Similarly, an open-source project model makes it less likely that malicious code will be included, since users can inspect the code before its execution.

In the future, computer scientists will be more aware of the implications of their work. Therefore, computer science as an academic discipline might become increasingly interested in understanding changes in social media platforms and their underlying technologies. In general, all natural science fields might diverge into different areas of new expertise that overlap with existing fields. The reason is that various fields are growing at different rates, and the technology being used is becoming increasingly complex and implications have to be considered much earlier.

Although the uprisings in North Africa have had only a small impact within the computer-science field itself, they have helped stimulate and extend existing research efforts, primarily in the areas of security and

communications. The effort to facilitate secure and private communication is a long-time area of research that is today being expanded thanks to real-life use and demands for better technology exposed by the MENA events. However, other technological areas have also been affected. For example, an article written by Kelev Leeraru (2011) describes how computational analysis could have been used to forecast the region's revolutions. Big data and computational analysis are up-and-coming research fields, in which the Arab uprisings could play an important role as a case study used to teach new self-learning analysis methods and machine-learning algorithms, with the aim of producing better predictions about political unrest in the future.

Instead of changing technology itself, political unrest such as the Arab uprisings changes the way technology is used both by civilian populations and political agencies and governments. The Arab uprisings clearly demonstrated that most regimes lacked and continue to lack broad knowledge about the internet and its underlying technology. Governments still have to learn about the relatively new media, and how to use the internet for their strategic purposes. Shutting down communications within a whole country and cutting off millions of people from the internet does not give the impression that the Egyptian government was prepared for such heavy use of modern communication platforms by its citizens. On the contrary, it seems that the governments in the region shut down all communication paths on the internet in an act of panic following the perception that they were quickly losing control of the situation.

The commercialization of the internet represents another immense problem that will likely persist. As long as large parts of the internet are maintained by organizations or companies subject to a given regime's control, it is likely that internet service providers will continue to be forced to block content or internet access. Current research trends such as peer-to-peer networks or darknets are still rarely used in practice. The distributed data structures offered by decentralized services offer privacy and efficiency advantages, but suffer on the other hand from a lack of central technical control, thus presenting challenges with regard to including new participants and maintaining technical quality levels. Similarly, the decentralized nature of peer-to-peer networks seems to frighten many companies and internet service providers from putting effort into their further development. In other words, most companies are not interested in maintaining systems that cannot be controlled, since their business models demand an emphasis on usability and practicability. However, the open-source community is

working to address these drawbacks, in many cases without commercial exploitation as a primary goal. Nevertheless, financing these communities' work can be a challenge, a factor that once again returns us to the issue of commerce.

Conclusion

The techniques and systems for combatting surveillance and censorship that are described in this article were not developed out of an urgent necessity. Techniques and systems such as encryption, the Tor project and LibreSocial, as well as all the attacks we have described, were developed before the Arab uprisings began. Neither the methods used to block internet access, nor the solutions used to evade such blocks evolved during the uprisings. Rather, these events have been used within academia to highlight the relevance of previous research work in the context of new political events.

Complete national internet shutdowns had taken place before, in Myanmar in 2007 and in Nepal in 2005. Years after the events in the MENA region, other countries continue to block and monitor specific services on the internet. Turkish internet service providers, for example, still frequently block access to Twitter, Facebook and other social networks. On July 22, 2015, following a suicide attack in Suruc, Turkish ISPs blocked local access to the Twitter social-networking service.

Technology most directly affects the people using it. The truth is that all regions in the world are connected through the internet, and ideas find a way to flow even around blocks and censorship. Ideas might carry the spark of revolution as they help people imagine different, potentially better realities. As former Google CEO Eric Schmidt said in an interview with Jerome Taylor (2010): "The internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had." While information flows can be blocked, speakers punished and information falsified for a certain amount of time, technology progresses nevertheless, and new forms of secure communication will be developed. In the end, information will flow.

References

Biddle, Peter & England, Paul & Peinado, Marcus & Willman, Bryan (2003): The Darknet and the Future of Content Protection. In Feigenbaum, Joan (ed.): Digital Rights Management. Washington, DC: Springer, 344–365.

Clayton, Richard & Murdoch, Steven J. & Watson, Robert N.M. (2006): Ignoring the Great Firewall of China. In Danezis, George & Golle, Philippe (eds.): Privacy Enhancing Technologies. Cambridge: Springer, 20–35.

Cowie, Jim (2011 a): Egypt Leaves the Internet. In DynResearch: http://research.dyn.com/2011/01/egypt-leaves-the-internet/

Cowie, Jim (2011 b): Egypt Returns to the Internet. In DynResearch: http://research.dyn.com/2011/02/egypt-returns-to-the-internet/

Dainotti, Alberto & Squarcella, Claudio & Aben, Emile & Claffy, Kimberly C. & Chiesa, Marco & Russo, Michele & Pescapé, Antonio (2011): Analysis of country-wide internet outages caused by censorship. Proceedings of the 2011 ACM SIGCOMM Internet Measurement Conference, 1–18.

de Kunder, Maurice (2015): The size of the World Wide Web (The Internet). In WorldWideWebSize.com: http://www.worldwidewebsize.com/

Eaton, Tim (2013): Internet Activism and the Egyptian Uprisings: Transforming Online Dissent into the Offline World. In Westminster Papers in Communication and Culture 9(2), 3–23.

Graffi, Kalman & Gross, Christian & Mukherjee, Patrick & Kovacevic, Aleksandra & Steinmetz, Ralf (2010): LifeSocial.KOM: A P2P-Based Platform for Secure Online Social Networks. In Proceedings of the 10th IEEE International Conference on Peer-to-Peer Computing (P2P).

Howard, Philip N. & Duffy, Aiden & Freelon, Deen & Hussain, Muzammil & Mari, Will & Mazaid, Marwa (2011): Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring?. In Project on Information Technology and Political Islam: https://www.library.cornell.edu/colldev/mideast/Role%20of%20Social%20Media%20During%20the%20Arab%20Spring.pdf

Kurose, Jim & Ross, Keith (2007): Computer Networking: A Top-Down Approach (4th Edition). Boston, MA: Pearson.

Leeraru, Kelev (2011): Culturomics 2.0: Forecasting large-scale human behavior using global news media tone in time and space. In First Monday: http://journals.uic.edu/ojs/index.php/fm/article/view/3663/3040

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

OpenNet Initiative (2009): Internet Filtering in Tunisia. In OpenNet Initiative: https://opennet.net/research/profiles/tunisia

Richtel, Matt (2011): Egypt Cuts Off Most Internet and Cell Service. In The New York Times, 29 January: http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html

Rogers, Michael & Bhatti, Saleem (2007): How to Disappear Completely: A Survey of Private Peer-to-Peer Networks. In Proceedings of the International Workshop on Sustaining Privacy in Autonomous Collaborative Environments (SPACE).

Stepanova, Ekaterina (2011): The Role of Information Communication Technologies in the 'Arab Spring'. In PONARS Eurasia 159, 1–6.

Taylor, Jerome (2010): Google chief: My fears for Generation Facebook. In Independent, 17 August: http://www.independent.co.uk/lifestyle/gadgets-and-tech/news/google-chief-my-fears-for-generation-facebook-2055390.html

Wagner, Ben (2012): Push-button-autocracy in Tunisia: Analysing the role of Internet infrastructure, institutions and international markets in creating a Tunisian censorship regime. In Telecommunications Policy 36(6), 484–492.

Zittrain, Jonathan & Edelman, Benjamin (2002): Localized Google search result exclusions. In Localized Google search result exclusions: http://cyber.law.harvard.edu/filtering/google/